OSI 7層結構, Open System Interconnect, 系統開放互連, 網路標準化的結構

1. 應用層 🡪 為應用程序提供服務

經過以上一跳一跳路由器的中繼, 终點主機的各層協議頭, 源主機的二進制流送到終端主機, 數據是文字,圖片,音樂,影片, 就由應用層協議來最終解釋

Protocol: DHCP(v6), DNS, FTP, Gopher, HTTP(SPDY, HTTP/2), IMAP4, IRC, NNTP, XMPP, POP3, SIP, SMTP, SNMP, SSH, TELNET, RPC, RTCP, RTP, RTSP, SDP, SOAP, GTP, STUN, NTP, SSDP

|  |  |
| --- | --- |
| Protocol | Description |
| DHCP(v6)  https://upload.wikimedia.org/wikipedia/commons/thumb/2/28/DHCP_session_en.svg/800px-DHCP_session_en.svg.png | Dynamic Host Configuration Protocol, 動態主機設定協定, 是一個局域網協議, 使用UDP工作, 定義為RFC 2131, v6則在RFC 3315中, DHCP主要有兩個用途:   1. 用於內部網路或網路服務供應商自動分配IP地址給用戶 2. 用於內部網路管理員作為對所有電腦作中央管理的手段   DHCP用一台或一組DHCP服務器來管理網路參數的分配, 這種方案具有容錯性, 即使在一個僅擁有少量機器的網路中, DCHP仍然是有用的, 因為一台機器可以幾乎不造成任何影響地被增加到本地網路中。  而對於一些設備如路由器和防火牆, 就不應使用DHCP, 把TFTP或SSH服務器放在同一台運行DHCP的機器上也是有用的, 目的是為了集中管理。  原理: DHCP是一種使網路管理員能夠集中管理和自動分配IP網路地址的通訊協議, 在IP網路中, 每個連接Internet的設備都需要分配唯一的地址, DHCP使網路管理員能從中心結點監控和分配IP地址, 當某台計算機移到網路中的其他位置時, 能自動收到新的IP地址。  使用的是租約概念, 可以定義租約的時間, 同時也可以為計算機分配靜態地址, 例如WEB服務器, Window NT/2000 都有DHCP服務器, 要知自已的計算器是否使用DHCP, CMD 🡪 ipconfig –all 即可 |
| DNS | Domain Name System域名系統，是互聯網的一個服務，它作為將域名和IP地址相對應的分佈式數據庫，使用TCP和UDP端口53，每一域名長度為63，總長度不超過253個字符 DNS系統中，常見的資源記錄類型有：  •主機記錄（A記錄）：RFC 1035定義，記錄是用於名稱解析的重要記錄，它將特定的主機名映射到對應主機的IP地址上。  •別名記錄（CNAME記錄）：RFC 1035定義，CNAME記錄用於將某個別名指向到某個A記錄上，這樣就不需要再為某個新名字另外創建一條新的A記錄。  •IPv6主機記錄（AAAA記錄）：RFC 3596定義，與A記錄對應，用於將特定的主機名映射到一個主機的IPv6地址。  •服務位置記錄（SRV記錄）：RFC 2782定義，用於定義提供特定服務的服務器的位置，如主機（主機名），端口（端口號）等。  •NAPTR記錄：RFC 3403定義，它提供了正則表達式方式去映射一個域名.NAPTR記錄非常著名的一個應用是用於ENUM查詢。 |
| FTP | File Transfer Protocol, 是用於網路上進文件傳輸的一套標準協議, 使用客戶/服務器模式, 文件傳輸和文件存取之間的區別在於, 前者由FTP提供, 後者由NFS等系統提供, RFC959定義。  FTP是一個8位的客戶端-服務器協議, 能操作任何類型的文件而不需要進一步處理, 就似MIME或Unicode一樣, 但是FTP有高的延時, 從開始請求到第一次接收需求數據之間的的時間, 會非常長, 而且不時就是執行一些登錄，端口為20或21兩個, 20用於客戶端和服務器之間的傳輸數據流, 端口21用於傳輸控制流。  數據流傳輸時，控制流會閑置，當控制流空置時間太多時，客戶端防火牆就會將會話置為超時，當大量數據通過防火牆時就會產生問題，同時因為會控制會話，會被防火牆斷開，產生錯誤  **FTP實現的目標**  促進文件的共享（計算機程序或數據）  鼓勵間接或者隱式的使用遠程計算機  向用戶屏蔽不同主機中各種文件存儲系統（文件系統）的細節  可靠和高效的傳輸數據  **缺點**  密碼和文件內容都使用明文傳輸，可能發生竊聽。  因為必須開放一個隨機的端口以建立連接，當防火牆存在時，客戶端很難過濾處於主動模式下的FTP流量。這個問題，通過使用被動模式的FTP，得到了很大解決。  服務器可能會被告知連接一個第三方計算機的保留端口。  此方式在需要傳輸檔案數量很多的小檔案時，效能不好 |
| Gopher | 互聯網上使用的分布型文件搜索網路協議, 不過已經幾乎沒人使用 |
| HTTP | Hyper Text Transfer Protocol是一種分佈式, 協作式和超媒體信息系統的應用層協議, HTTP/2為新一代HTTP, 已取代HTTP 1.1  HTTP是一個客戶端(用戶)和服務器端(網站)請求和應答的標準(TCP), 客戶端發起一個HTTP請求到服務器上的指定端口(80), 這個客戶端稱為用戶代理程式(UESR AGENT), 應答的服務器上存儲資源,為origin server, 中間可能有多個中間間(gateway or tunnel, etc)  http沒有規定必須要使用它或它支持的層, 所以可以在任何協議上使用, http假定下層協議提供可靠傳輸, 所以任何能提供保證的協議都可以使用  GET  向指定的資源發出「顯示」請求。使用GET方法應該只用在讀取資料，而不應當被用於產生「副作用」的操作中，例如在Web Application中。其中一個原因是GET可能會被網絡蜘蛛等隨意訪問。  HEAD  與GET方法一樣，都是向服務器發出指定資源的請求。只不過服務器將不傳回資源的本文部份。它的好處在於，使用這個方法可以在不必傳輸全部內容的情況下，就可以獲取其中「關於該資源的信息」（元信息或稱元資料）。  POST  向指定資源提交數據，請求服務器進行處理（例如提交表單或者上傳文件）。數據被包含在請求本文中。這個請求可能會建立新的資源或修改現有資源，或二者皆有。  PUT  向指定資源位置上傳其最新內容。  DELETE  請求服務器刪除Request-URI所標識的資源。  TRACE  回顯服務器收到的請求，主要用於測試或診斷。  OPTIONS  這個方法可使服務器傳回該資源所支持的所有HTTP請求方法。用'\*'來代替資源名稱，向Web服務器發送OPTIONS請求，可以測試服務器功能是否正常運作。  CONNECT  HTTP/1.1協議中預留給能夠將連接改為管道方式的代理服務器。通常用於SSL加密伺服器的連結（經由非加密的HTTP代理伺服器）。  HTTP至少應提供 GET和HEAD |
| IMAP4 | Internet Message Access Protocol, 因特網信息訪問協議, 用來從本地郵件客戶端訪問遠程服務器上的郵件, 而在的版本是IMAP4rev1, 在RFC3501 中定義, 和POP3 都是現在郵件伺服器支持的。 |
| IRC | Internet Relay Chat, 因特網中繼聊天, 是一種透過網路的即時聊天方式, 使用的端口有6667(明文), 6697(SSL加密), 是一種公開協議, 採用TCP和SSL協議, 多台IRC可擴展為IRC網路, IRC用戶透過客戶端和服務器相連, 大多數IRC不需要註冊, 而連接前需要諼定好nickname, 但客戶端一般會自動分配一個 |
| NNTP | Network News Transport Protocol(網路迎聞傳輸協議), 是一舍主要用於閱讀和張貼新聞文章到Usenet上的Internet應用協議, 協議負責新聞在服務器間的傳送, 與SMTP類似, 但不同的是只能用來讀新聞, 這個協議目前被廣泛應用 |
| XMPP | Extensible Messaging and Presence Protocol, 是一種以XML為基礎的開放式即時通訊協定, 被GOOGLE TALK (IP電話及即時通訊服務) 應用, 關鍵特色是 – 分散式的即時通訊系式, 因為基於XML的彈性, 所以可應用於多個方面  優點:  開放: 有多種實作的項目  分散: 核心協議是先建立一個stream, 沒有中央主伺器, 任何人都可以運行自己的xmpp  安全: 任何xmpp協議的伺服器都可以獨立於公眾xmpp, 而使用SASL及TLS等技術的可靠安全性, 因為XMPP內核已內建  缺點:  資源負載太重: 超過70%的XMPP協議伺服器被重複轉發  二進制資料: XMPP傳輸單一的XML文件, 因此要傳輸二進制資料, 要先將二進制Base54編碼, 更好的做法是使用其他協議, 而以xmpp溝通 |
| POP | Post Office Protocol 是tcp/ip協議中的一員, 由RFC1939定義, 本協議主要用於支持使用客戶端遠程管理在服務器上的電子郵, 提供了SSL加密的POP3為POP3S  POP支持離線處理, 具體過程是, 郵件發送到服務器上, 電子郵件客戶端調用客戶機程序連接服務器, 下載所有未讀郵件, 是一種儲存轉發服務 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. 表示層 🡪 數據格式轉化, 數據加密

表示層協議頭會把當中的應用層發給表示層

Protocol: 該層被棄用, HTTP, FTP, TELNET等協議有類似功能, 傳輸層的TLS/SSL也有類似功能

1. 會話層 🡪 建立, 管理和維護會話

會話層協議頭會把當中的表示層發給表示層

Protocol: 該層被棄用, 應用層的HTTP, RPC, SDP, RTCP等協議都有類似功能

1. 傳輸層 🡪 建立, 管理維護端到端的連接

傳輸層協議頭會把當中的會話層發給會話層

Protocol: TCP (T/TCP, FAST OPEN), UDP, DCCP, SCTP, RSVP, PPTP, TLS/SSL

1. 網路層 🡪 IP選址及路由選擇

這個協議頭包括了目的地網路地址, 用於指示所經的路由器這段二進制流的目的地, 通過查詢自己的網路地址表, 決定更靠近目的地的下一跳路由器, 一個出接口和下一跳路由器直連時, 又要考慮再增加鏈路層的協議頭, 依據不同的接口類型, 增加不同的鏈路層協議頭, 所以每經過一跳路由器, 就會變換一次特有的鏈路層協議頭, 但網路協議層不變, 直到這二進制流到達終點

Protocol: IP (v4, v6), ICMP (v6), IGMP, IS-IS, IPsec, BGP, RIP, OSPF, RARP

1. 鏈路層 🡪 提供介質訪問及鏈路管理

這個協議頭只有源主機, 端接路由器可以理解, 只要端接路由器能順利接收, 使命就算完成, 協議頭就會在二進制流消去, 到上級的網路層協議頭

Protocal: WiFi (IEEE 802.11), ARP, WiMAX (IEEE802.16), ATM, DTM, Token ring, FDDI, 以太網, 幀中繼, GRPS, EV-DO, HSPA, HDLC, PPP, PPPoE, L2TP, ISDN, SPB, STP

1. 物理層 🡪 純物理層

依據不同的物理層介質以光, 電, 電磁波的信號發送出去

Protocol: 以太網, 調制解調器, 電力線通信, 同步光網絡, G.709, 光導纖維, 同軸電纜, 雙紋線

以上七道工序產生了二進制流, 每道工序都有屬於自己的協議頭

網路安全

**機會性加密**

或伺機加密（英語：Opportunistic encryption，簡稱OE；有時也稱非認證加密、隨機加密）是一種網絡通信加密機制，即當建立通信連接時，首先嘗試請求加密，如果對方也支持加密連接，連接則開始加密，期間不進行身份驗證；如果加密請求嘗試失敗，則回退到明文通信機制。這種加密不須雙方進行事先配置，能夠抵抗被動的流量竊聽，但無法防禦中間人攻擊等主動攻擊。因此，它不能替代完整的加密方案。使用機會性加密時，用戶也不會看到任何連接安全的提示。

大多數互聯網安全協議中，開始加密通信前都會進行身份驗證，以防止中間人攻擊，從而確保通訊安全。但是，這將涉及到身份驗證與密鑰管理，且須進行事先配置，否則無法開始安全通信。這使加密變成了「有或無」的一個問題，只能在「完全安全」或「完全不安全」兩個極端選項之間選擇，沒有條件時便只能放棄加密，使用不安全的明文連接。這限制了加密連接在互聯網上的大規模應用，使被動的攻擊者也能夠竊聽大量互聯網流量。

SASL

Simple Authentication and Security Layer, 簡單認證與安全層, 是一個在網路協議中用來認證和數據加密的構架, 它把認證從程序中分離開, 理論上使用SASL的程序協議都可以使用SASL所支持的全部認證, 認證機制可支持代理認證, 讓一個用戶可以承擔另一個用戶的認證。同時, SASL提供數據安全層, 提供了數據完整驗證和數據加密。

TLS

Transport Layer Security傳輸層安全協定, 目的是為網際網路通訊提供安全及數據完整性保障, HTTPS協定加SSL加密, 成為目前的工業標準 (RFC 6176), SSL包括記錄層 (Record layer) 和傳輸層, 記錄層協議確定傳輸層數據的封裝格式, 傳輸層安全協議使用x.509認證, 之後利用非對稱加密演算來對通訊方做身份認證, 之後交換對稱金鑰, 這個會談金鑰是用來將通訊兩方交換的資料做加密, 保證兩個應用間通訊的保密和可靠性, 使客戶與服務器應用之間的通訊不被攻擊者竊聽。