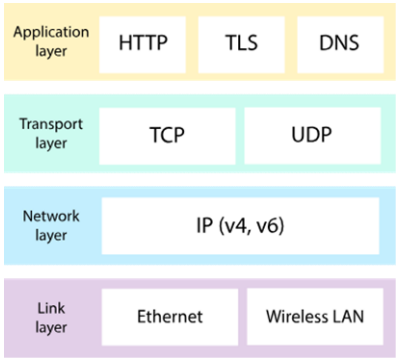


第六章 網路協定
Network Protocols

- 本章探討網路協定的目的並以最常見的TCP/IP協定為例

有效的網路通訊

- 有效的網路通訊，電腦必須傳送資料必須可信賴與有效率
- 有些協定強調信賴有些強調效能，網路協定通常會協同合作在網路通訊的不同層提供信賴與效能

協定與協定組合

- 協定
  - 通常協定(Protocol)是由規則與程序所組成，為了溝通行為或禮儀等目標
- 協定組合
  - 一組協同工作的通信協定，通常稱為協定組合或稱協定堆疊，最通見的協定組合是Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP 分層架構

Layer name	TCP/IP protocols			
Application	HTTP	FTP	DHCP	TFTP
	SMTP	POP3	DNS	SNMP
Transport	TCP		UDP	
Internetwork	ICMP	ARP	IPsec	
	IPv4 and IPv6			
Network access	Ethernet, token ring, FDDI, WAN technologies			

應用層協定(Application-Layer Protocols)

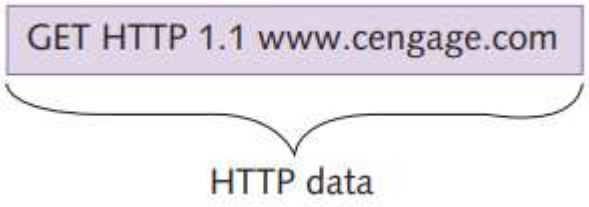
- 應用層提供網路服務給需要存取網路資源的應用程式
- 應用層處理以下的功能:
  - 讓應用程式存取網路服務
  - Client/server資料存取
  - 名稱解析
  - 動態位址配置
  - 認證/使用者登入
  - 資料格式化與轉換

應用層協定(Application-Layer Protocols)案例

- HTTP: Protocol of the World Wide Web
- E-Mail Protocols: POP3, IMAP, and SMTP
- FTP and TFTP
- Server Message Block
- Remote Desktop Protocol
- Telnet and SSH
- Simple Network Management Protocol
- Dynamic Host Configuration Protocol
- Domain Name System

HTTP: Protocol of the World Wide Web

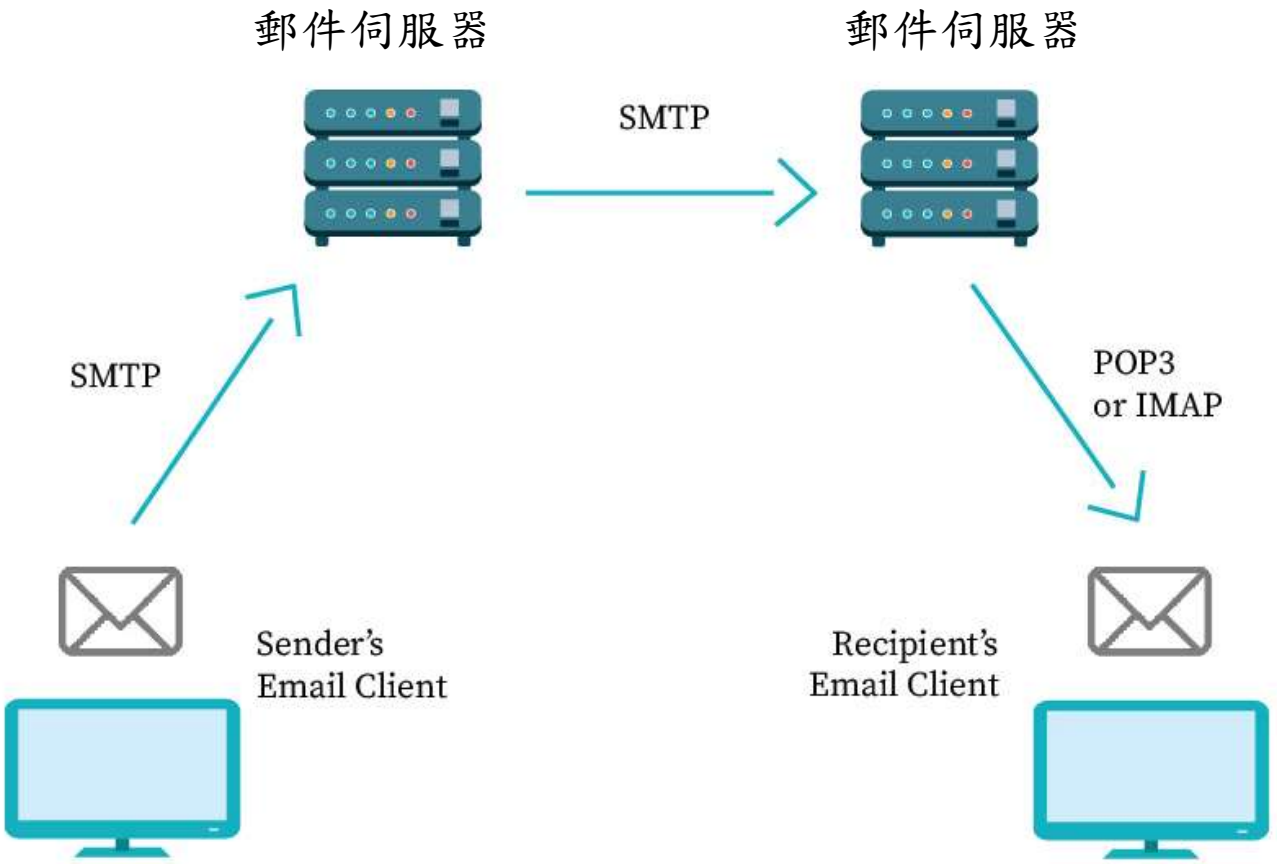
- 瀏覽器存取Web資料的協定
- 傳送HTML網頁
- HTTP也用來傳送檔案、下載顯示多媒體檔案，遞送動畫、互動網頁等
- 一個HTTP 的協定訊息可參考如下



E-Mail Protocols: POP3, IMAP, and SMTP

- Post Office Protocol version 3 (POP3)
  - E-mail用戶端使用Post Office Protocol version 3 (POP3)協定從電子郵件伺服器將進來的訊息下載到本地端的電腦，電子郵件伺服器的信件則被刪除
  - POP3 使用 TCP port 110
- Internet Message Access Protocol version 4 (IMAP4)
  - IMAP4 有一些進階的訊息控制的功能包含在本地端管理電子郵件或是留在電子郵件伺服器中,加上額外的容錯功能
  - IMAP4 可以下載郵件標頭，當訊息被選定時才下在訊息內容與附件
  - IMAP4 使用TCP port 143
- Simple Mail Transfer Protocol (SMTP)
  - SMTP 是一個在Internet 標準的寄送電子郵件的協定，通常POP3是用來下載電子郵件
  - SMTP 使用 TCP port 25
  - 以上三個電子郵件協定都是使用TCP Transport-layer protocol 確保可信賴的傳送大量電子郵件

電子郵件寄送運作流程


郵件伺服器
郵件伺服器
SMTP
SMTP
POP3
or IMAP
Sender's
Email Client
Recipient's
Email Client

FTP 與 TFTP(1/2)

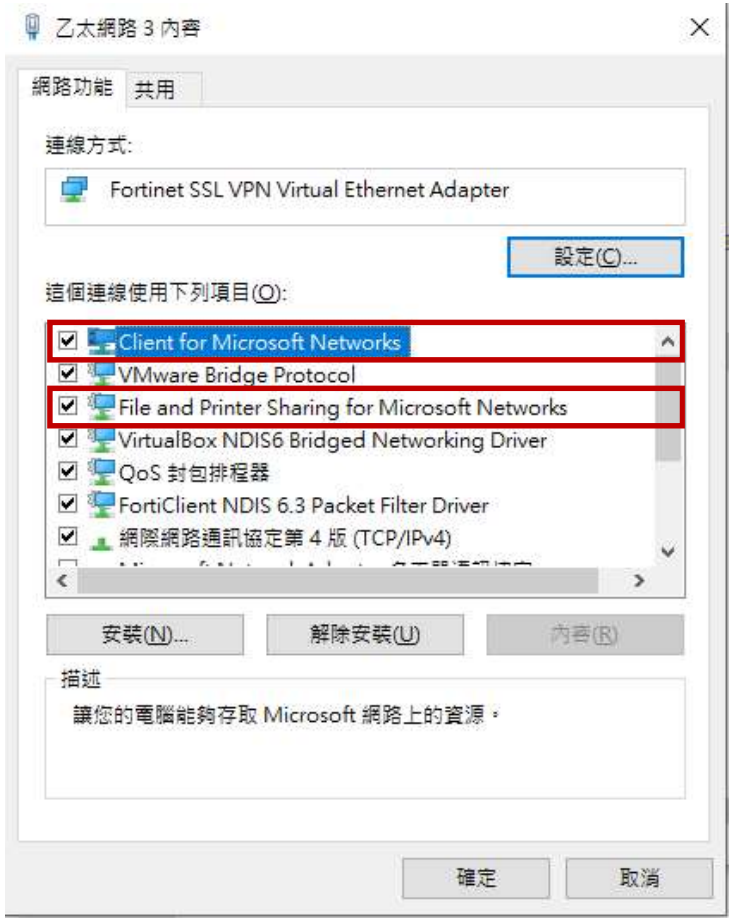
- File Transfer Protocol (FTP)
  - 檔案傳輸協定顧名思義是屬於client/server 協定 用於網路上傳送與管理檔案
  - FTP 使用 TCP ports 20 與 21，Port 21 用來送控制命令, port 20 是用來傳送檔案資料
  - FTP可用在私人網路與網際網路上來傳送檔案，他是不安全的協定，使用他傳送檔案有風險，資料或帳號密碼都沒有加密，如果包含登入資訊的封包被截取，帳號與密碼資料就會被揭露

FTP 與 TFTP(2/2)

- Trivial File Transfer Protocol (TFTP)
  - TFTP是一個簡單的檔案傳輸協定，具有很少的檔案管理功能，它使用UDP port 69，它是不可信賴對於在網際網路上傳送大檔案
  - 它的主要用途是在區域網路內傳送組態檔與韌體檔案給網路設備，諸如路由器與交換器，TFTP也會用於一些裝置，透過網路啟動作業系統並非從本身的儲存裝置
  - FTP, TFTP 是不安全的協定，少被用於網路網路上，不需要憑證，安全不是重要考慮

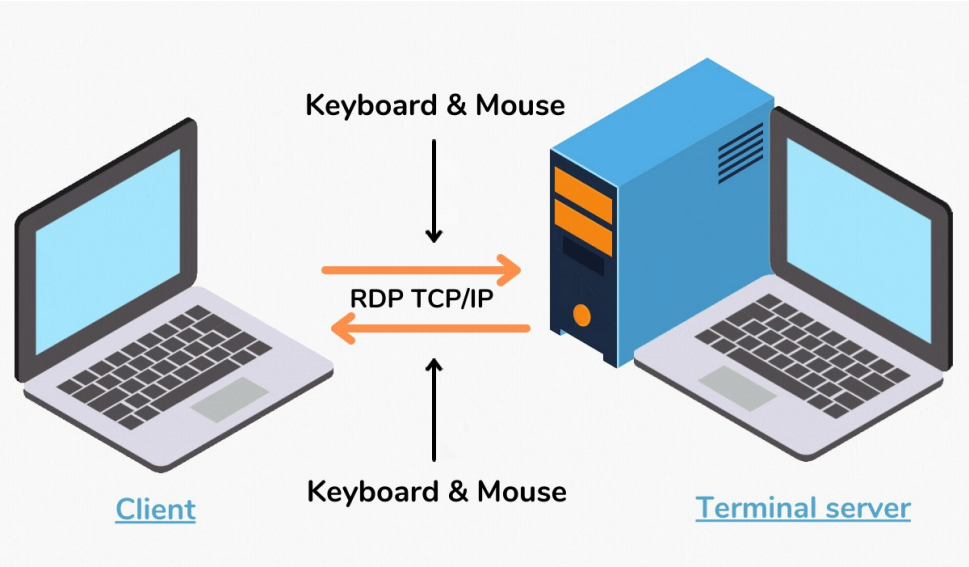
伺服器訊息區塊 (Server Message Block)

- SMB是一個協定用於Windows之間，檔案與印表機資源分享，例如在network connection's properties 中的Windows Client for Microsoft Networks 與 File and Printer Sharing for Microsoft Networks 使用SMB 協定跨網路分享檔案
- SMB 協定跨網路分享檔案SMB幾乎用於私人網路環境非網路網路上， Linux 與 Mac OS X 也支援 SMB 用他們對應SMB程式
- SMB 使用 TCP port 445



遠端桌面協定 (Remote Desktop Protocol)

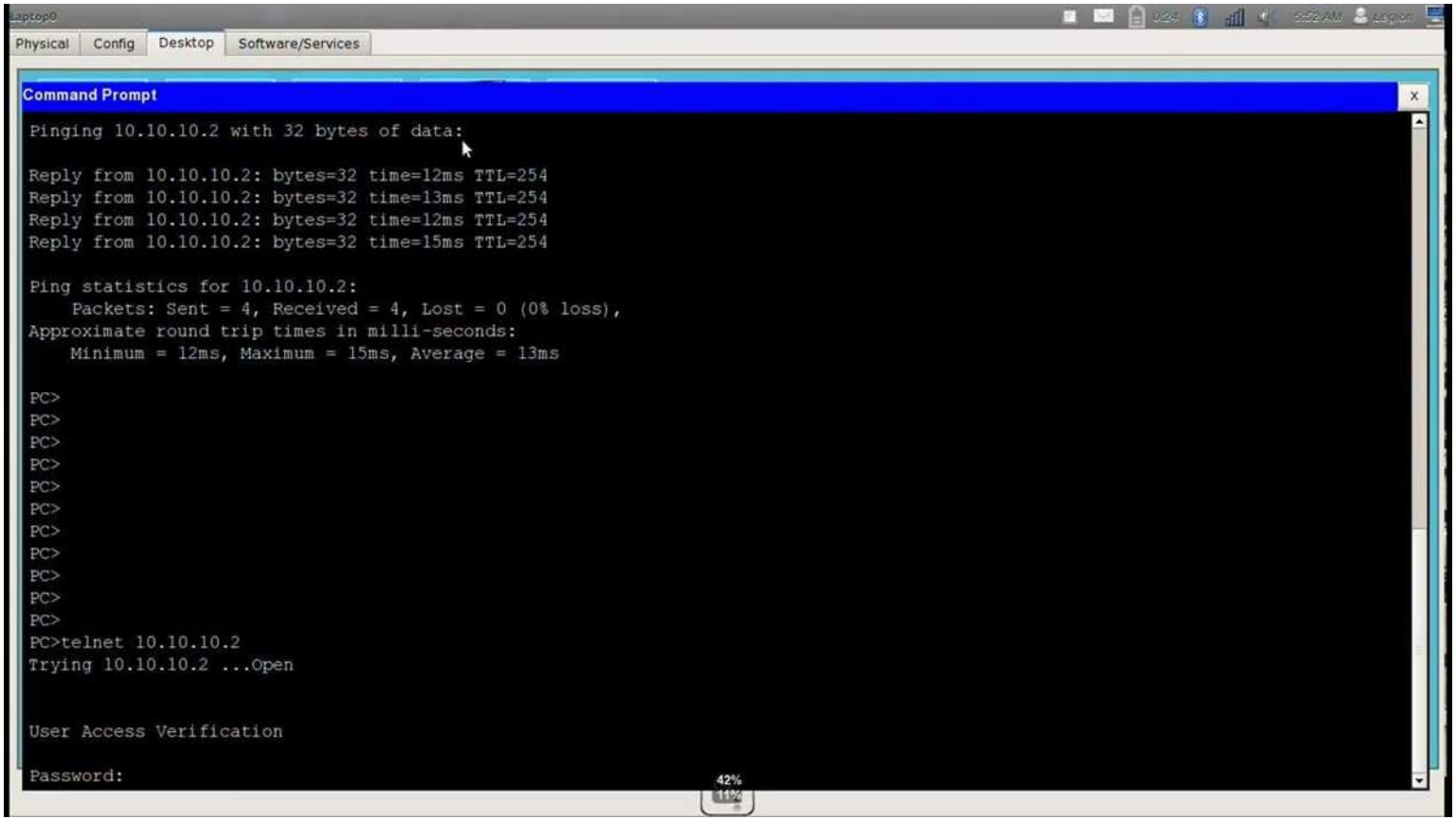
- RDP 指使用Windows graphical user interface (GUI)存取遠端的Windows電腦，使用RDP，你能夠跨網路存取另一部電腦的桌面，使用遠端的電腦宛如你正坐在該電腦螢幕前使用它的鍵盤與滑鼠，RDP可於遠端執行應用程式，網路管理者通常使用它來遠端管理Windows 工作站與伺服器
- RDP 使用TCP port 3389



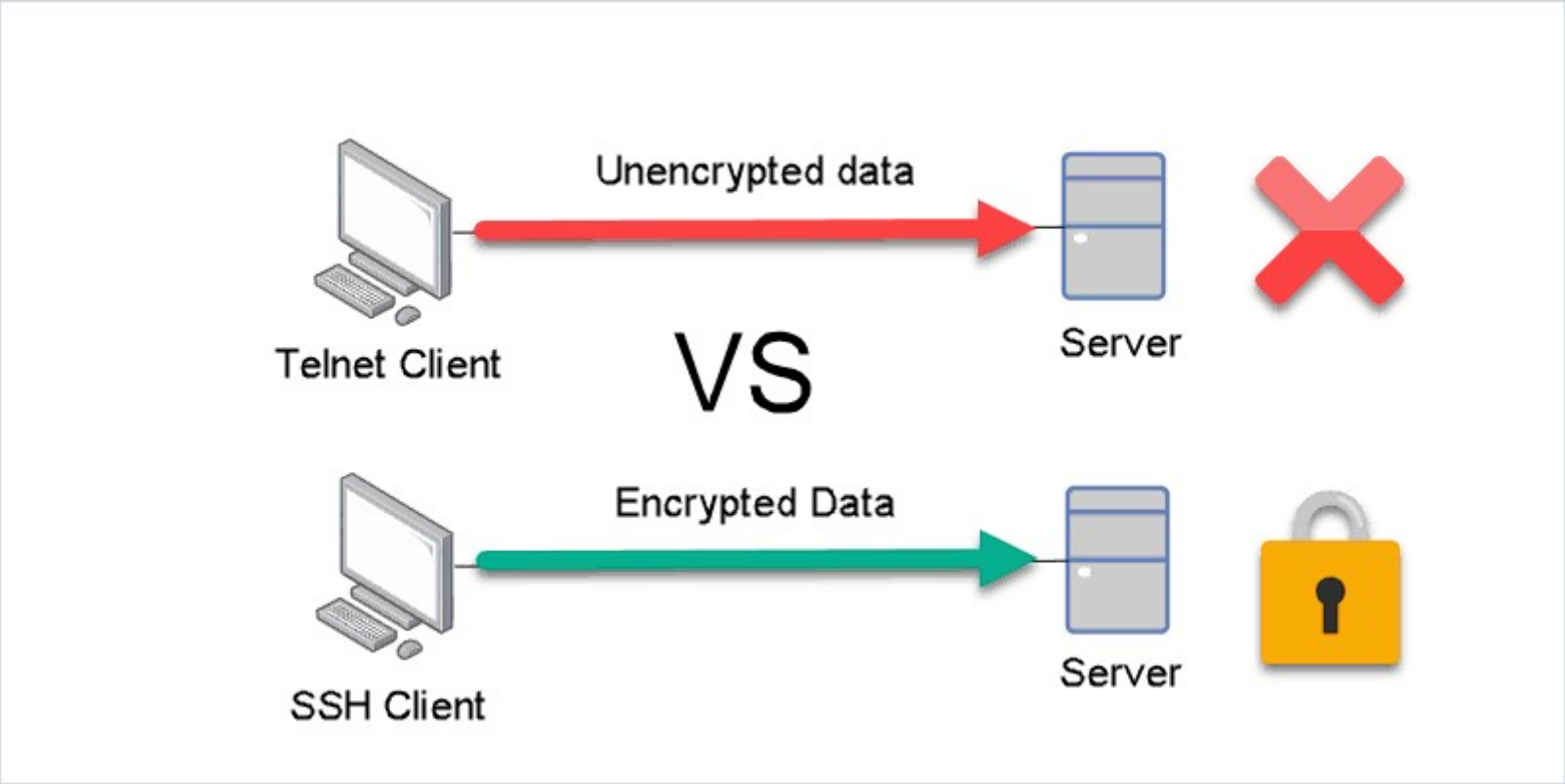
命令列介面式遠端連線(Telnet 與SSH)

- Telnet and Secure Shell (SSH)是在跨網路的環境中使用命令列介面連接網路裝置
- 網路管理者通常使用Telnet 或 SSH 連接至一個被管理的交換器或路由器，檢示其狀態或是藉由命令列介面進行組態設定的工作， Telnet 使用 TCP port 23像FTP一樣不是一個安全的協定，因此要小心使用， SSH 使用 TCP port 22 並且在client 與server兩端之間提供一個加密的管道，如果裝置兩者都有提供，應該優先選擇SSH
- Telnet vs SSH Explained
  - https://www.youtube.com/watch?v=tZop-zjYkrU

命令列使用介面 (command-line interface)

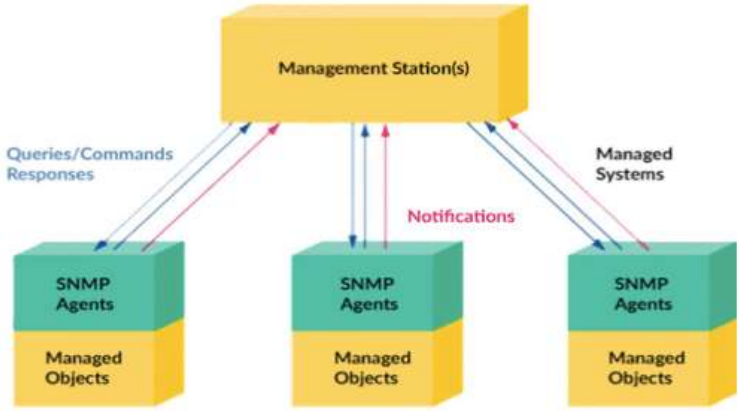


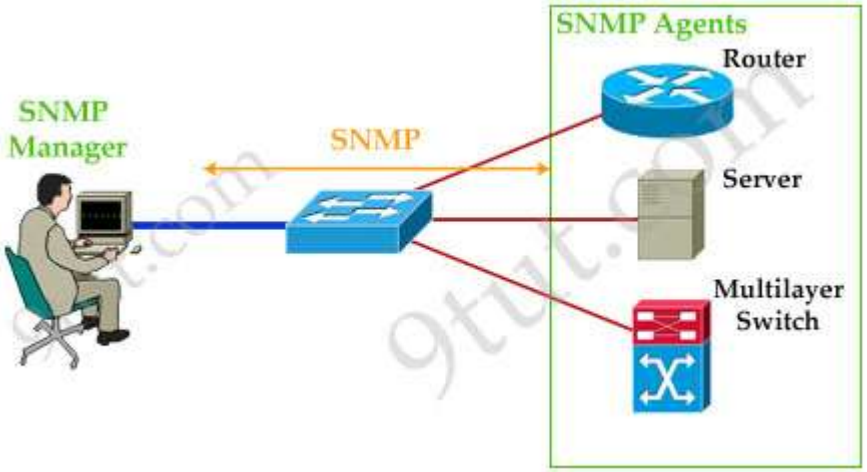
Telnet vs SSH



簡單網路管理協定(Simple Network Management Protocol)

- SNMP 是用來監督與管理網路設備並蒐集網路流量統計資料，屬於client/server 協定，須將代理程式安裝在被監控與管理的設備上， SNMP代理程式蒐集資料並傳送至網路管理工作站存放與分析
- SNMP 運作在 UDP ports 161 與162

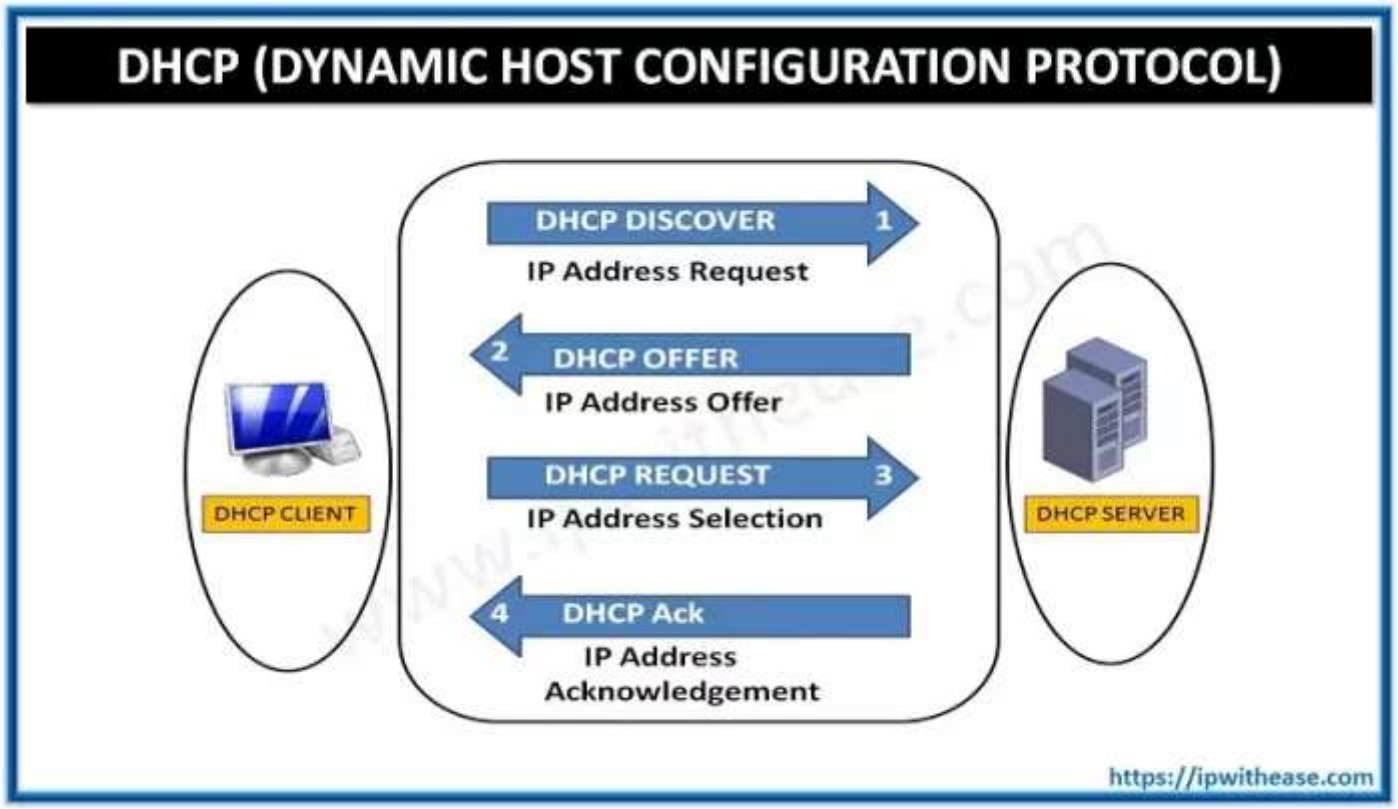




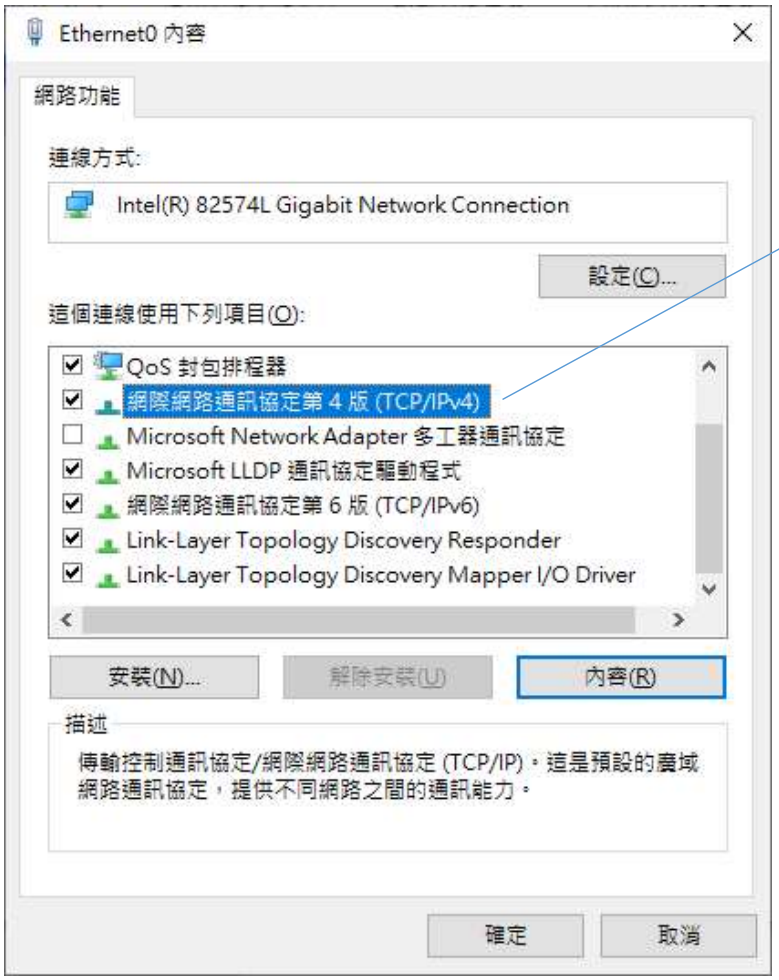
動態主機設定協定(Dynamic Host Configuration Protocol)

- 一個大型的網路使用TCP/IP的缺點包含設備的詳細組態的管理，須持續追蹤被賦予的IP，哪一部電腦使用這個IP等相關資訊，相當繁瑣
- 為了讓這個工作更容易些， DHCP被發展出來，要使用DHCP，必須設置一部DHCP伺服器，此伺服器擁有一段IP位址，及其他IP位址組態設定資訊
- 電腦必須設定為請求取得IP位址的組態，才會向DHCP伺服器請求IP ，電腦是以廣播訊息的方式向DHCP伺服器請求IP位址資訊
- 每次電腦請求一個IP，DHCP伺服器分配一個IP直到沒有IP可以用為止，電腦使用IP完畢或期限到之後，會將IP歸還給DHCP伺服器，供DHCP伺服器配置給其他電腦使用

DHCP 運作流程


DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)
DHCP DISCOVER
1
IP Address Request
2
DHCP OFFER
IP Address Offer
DHCP REQUEST
3
IP Address Selection
4
DHCP Ack
IP Address
Acknowledgement
DHCP CLIENT
DHCP SERVER
https://ipwithease.com

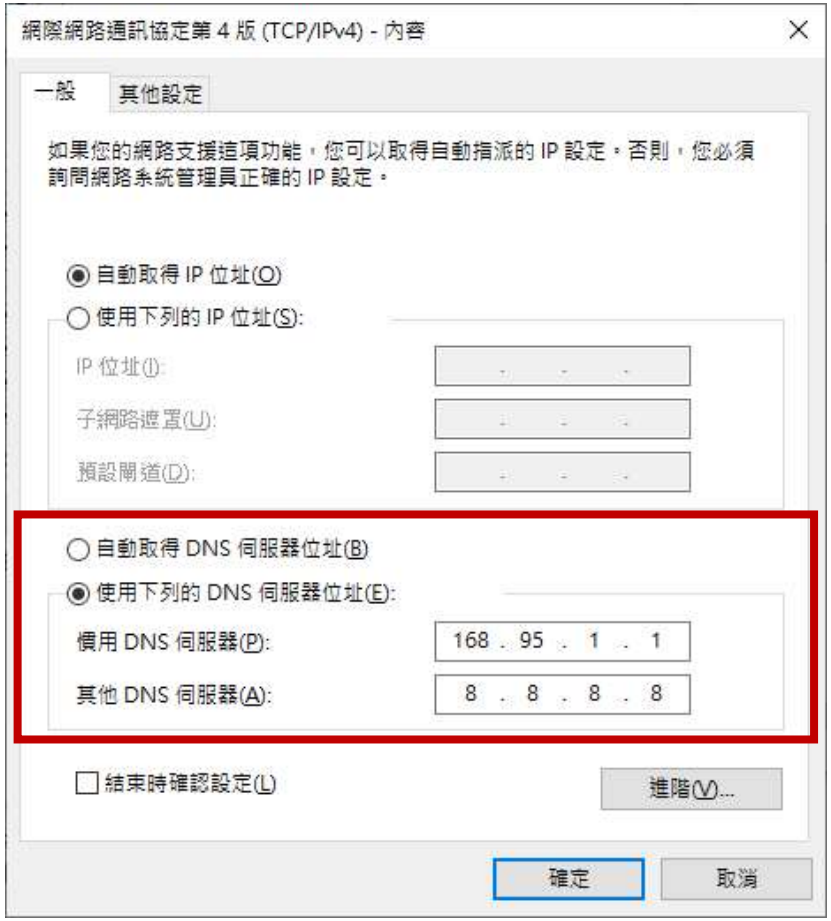
Windows電腦DHCP設定



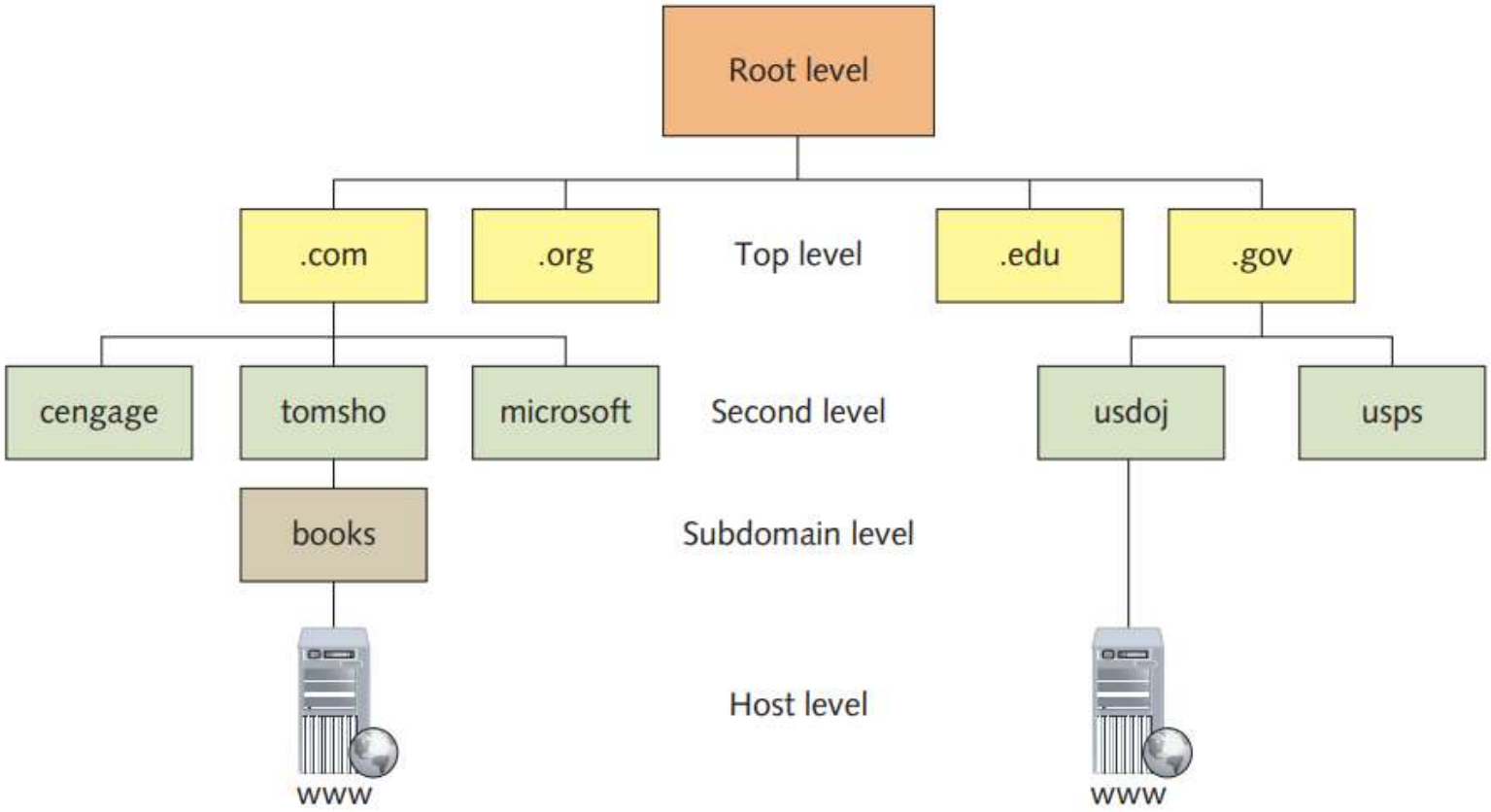
網域名稱系統(Domain Name System)

- DNS 是一個 名稱-to-位址 的解析協定，協定存有一份電腦名稱與其IP位址對應清單，使用者可以用電腦名稱例:www.uch.edu.tw(非用數值位址)，例如120.124.96.145與電腦溝通
- 當使用者在瀏覽器上輸入www.uch.edu.tw，瀏覽器會聯繫電腦上的DNS 用戶端，DNS用戶端詢問DNS伺服器(參考IP組態中DNS伺服器的設定)請求將www.uch.edu.tw 轉換成IP位址，DNS伺服器回覆www.uch.edu.tw的IP位址，使用這個IP位址，瀏覽器能夠連接到對應到的Web伺服器請求網頁

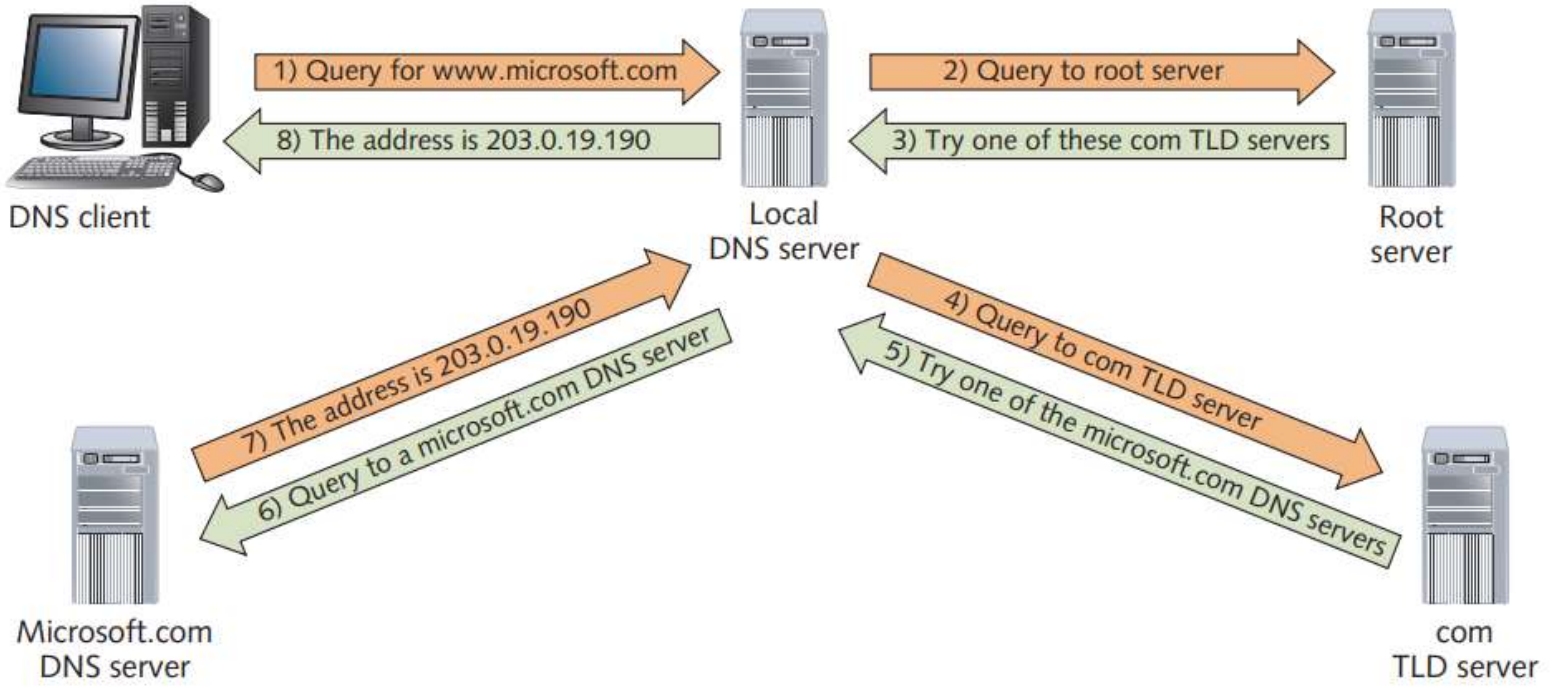
用戶端DNS伺服器位址設定



DNS的階層架構


Root level
.com
.org
Top level
.edu
.gov
cengage
tomsho
microsoft
Second level
usdoj
usps
books
Subdomain level
Host level
www
www

DNS 查詢過程經由DNS階層架構



傳輸層協定(Transport-Layer Protocols)

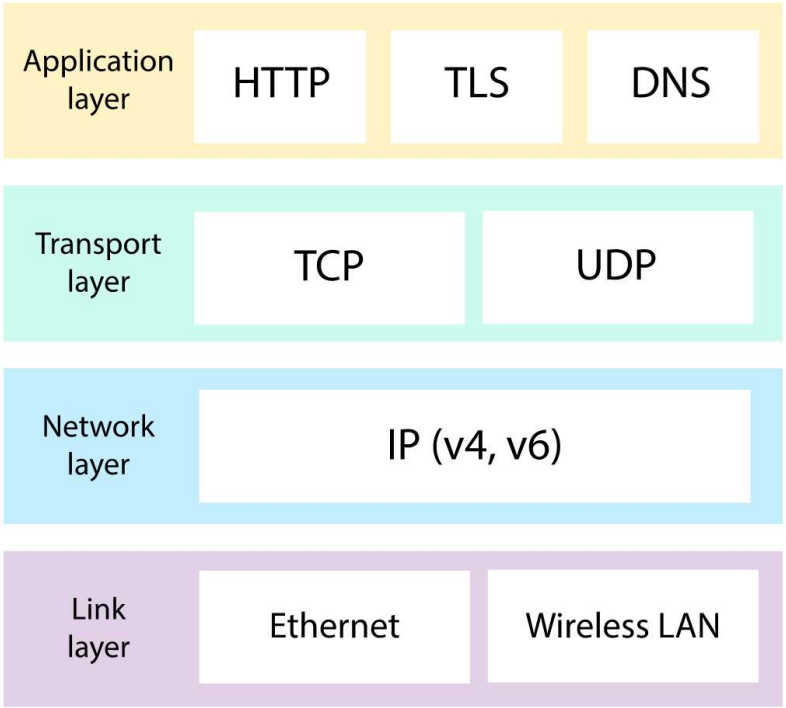
- 傳輸層協定最被應用層協定所使用，因為傳輸層協定提供表頭欄位中可用來識別應用層並且提供可信賴度與流量控制給需要傳輸大量資料的應用程式
- 以下解釋TCP/IP中傳輸層的角色，接著說明兩個協定運作此層TCP and UDP

傳輸層的角色

- 傳輸層有兩個協定，TCP(Transmission Control Protocol)是連接導向(connection oriented)，設計用於在複雜的互動網路下提供可靠(reliable)的傳輸
- UDP(User Datagram Protocol) 是非連接導向(connectionless)，設計用於小資料量下效能溝通
- 兩個協定進行下列工作
  - 運作於 segments (TCP) or datagrams (UDP)
  - 提供方法識別參與溝通的來源或目的應用程式
  - 使用checksum來保護驗證資料

兩個協定工作內容

- 處理Segments 與 Datagrams
  - TCP 處理的資料單位稱為 “segments”
  - UDP 處理的資料單位稱為“datagrams”
- 識別來源與目的的應用程式
  - 傳輸層表頭提供決定傳送資料給應用程式的資訊，TCP與UDP使用埠號(port)指出來源與目的地應用程式
- 保護資料使用Checksum
  - 為了保護資料完整性，TCP 與 UDP 提供 checksum

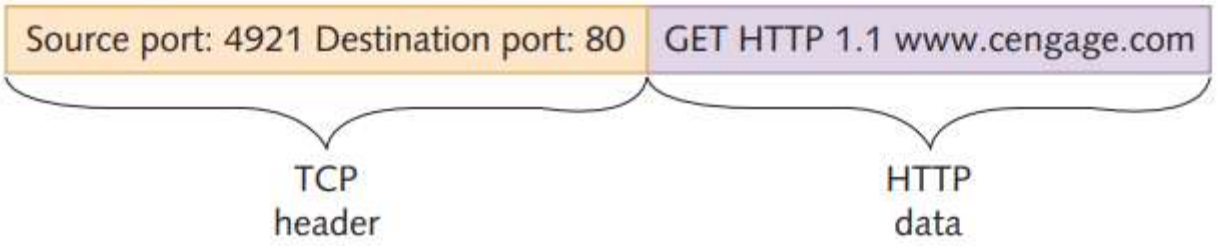


眾所周知的埠號Well-known port numbers

Application-layer protocol	Port number	Transport layer
FTP	20, 21	TCP
SSH	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	UDP
DHCP	67, 68	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP	143	TCP
SNMP	161, 162	UDP
HTTPS	443	TCP
SMB	445	TCP
RDP	3389	TCP

TCP: 可信賴傳輸傳輸層 (The Reliable Transport Layer)

- 如果應用程式需要可靠資料傳輸，應該使用TCP當作傳輸層，TCP提供可靠的傳輸具有下列特性，這些是UDP沒有的
  - 建立連接
  - 將大資料分段
  - 使用回覆確認確保流量控制，每一項特性信賴連接導向協定，TCP與目的地建立連接，資料被傳送，連接中斷



互聯網路層協定(Internetwork-Layer Protocols)

- 這一層是管理人員做的事就是網路組態設定
- IP協定就是運作在這一層，它是TCP/IP 協定組合的核心
- IP位址在此定義，路由發生在這一層，沒有路由網際網路與WWW不會存在，可見此層的重要性
- 由於路由設定與IP位址的複雜度，這一層是網路設定出錯最多的地方，在一個大型互動網路，大量的時間花在解開互動網路層的複雜性
- 互聯網路層協定有四項主要的工作
  - 定義與驗證IP位址
  - 路由封包穿越互聯網路
  - 解決從IP位址到MAC位址的對應
  - 有效的傳送封包

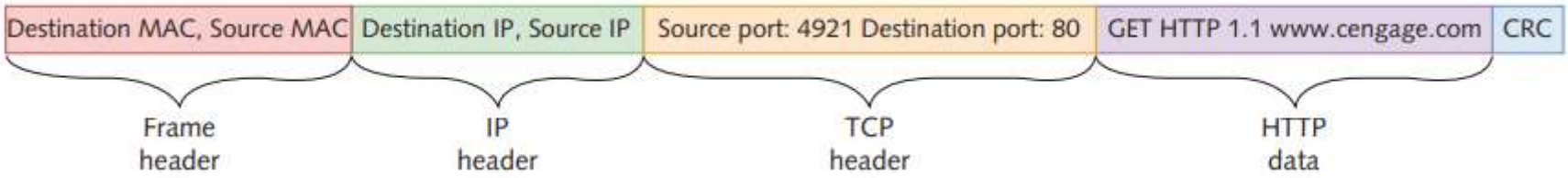
運作在互聯網路層的協定

- IPv4
  - IPv4 是最通用的IP版本，最廣為使用
- IPv6
  - 較大的位址空間IPv4 位址是 32 位元, IPv6 位址128 bits
- ARP
  - 解決logical (IP) 位址到實體(MAC)位址
- ICMP
  - 用來網路設備間傳送錯誤、狀態、控制訊息
- IPsec
  - 運作於 IPv4 確保安全的傳送封包，藉由認證與加密提供安全性

網路存取層協定(Network Access-Layer Protocols)

嚴格講，網路存取層協定並非組成TCP/IP協定組合的一部分，網路技術如Ethernet運作在此層，網路存取層是TCP/IP架構的一部分，僅是延伸互聯網路層使其有能力與網路技術溝通按網路存取層的規則
網路存取層執行的工作包含:

- 提供實體位址給網路介面
- 驗證進來的frame有正確的MAC位址
- 定義並遵循媒體存取規則
- 接收上層互聯網路層的封包(packet)並將之封裝訊框(frame)
- 解封裝收到的訊框(frames)並將封包(packet)送至互聯網路層
- 提供訊框(frame)以CRC編碼的形式
- 傳送與接收位元訊號
- 定義傳送位元資料的訊號，是電子、光脈衝或無線電?
- 定義媒體與實體網路連接時所需連接器



本章完結