行政院及所屬各機關出國報告
(出國類別：實習)

無線上網（Wireless Internet）新技術

服務機關：中華電信股份有限公司

數據通信分公司

出國人　職　稱：專員

姓　名：陳致和

出國地區：德國慕尼黑

出國期間：90年11月12日 至 90年11月24日

報告日期：91年11月

系統識別號:C09006166

公 務 出 國 報 告 提 要

頁數: 33　含附件: 否

報告名稱:

實習無線上網(Wireless Internet)新技術

主辦機關:

中華電信數據通信分公司

聯絡人／電話:

／

出國人員:

陳致和　中華電信數據通信分公司　網際網路處　專員

出國類別: 實習

出國地區: 德國

出國期間: 民國 90 年 11 月 12 日 -民國 90 年 11 月 24 日

報告日期: 民國 91 年 11 月 22 日

分類號/目: H6／電信　H6／電信

關鍵詞:　HiNet,Wireless LAN,802.11,802.1x,WiFi,VoIP,SURPASS

內容摘要: 隨著網路的普及，人們對於網路的需求日益殷切，除了頻寬的需求之外，上網的便利性也逐漸成爲人們對新世紀網路的期待。無線上網技術的出現，正好彌補了這個缺口，隨時隨地與網際網路接軌，對使用者而言所代表的是無限的便利；對服務提供者而言，則是龐大的商機。目前雖然已經出現技術較成熟、業界接受度較高的標準，也就是IEEE 802.11b標準（又稱爲WiFi），但網路科技的發展日新月異，無線網路亦然，許多新的標準及機制不斷地被制定出來。因此，我們必須先了解整個無線網路技術的發展趨勢，並就目前可行性最高的方案加以深入了解，包括其他衍生出來的議題如頻寬管理、運作模式及安全性機制等等，以期能順利導入這項新的接取技術。 本報告書共分五個單元，第一單元說明本次實習之目的。第二單元敘述實習行程及課程。第三單元敘述目前無線上網新技術服務的介紹，並著重在無線區域網路的技術，包含應用範圍、目前的標準、系統組成元件、運作模式、IEEE 802.11b的實體層與資料鏈結層及802.1x安全性機制。第四單元則敘述德國西門子公司所提出的次世代語音與網路的整合平台- SURPASS Solutions and Product Introduction。第五單元爲實習心得與結論。

本文電子檔已上傳至出國報告資訊網

摘要

隨著網路的普及，人們對於網路的需求日益殷切，除了頻寬的需求之外，上網的便利性也逐漸成為人們對新世紀網路的期待。無線上網技術的出現，正好彌補了這個缺口，隨時隨地與網際網路接軌，對使用者而言所代表的是無限的便利；對服務提供者而言，則是龐大的商機。目前雖然已經出現技術較成熟、業界接受度較高的標準，也就是 IEEE 802.11b 標準（又稱為 WiFi），但網路科技的發展日新月異，無線網路亦然，許多新的標準及機制不斷地被制定出來。因此，我們必須先了解整個無線網路技術的發展趨勢，並就目前可行性最高的方案加以深入了解，包括其他衍生出來的議題如頻寬管理、運作模式及安全性機制等等，以期能順利導入這項新的接取技術。

本報告書共分五個單元，第一單元說明本次實習之目的。第二單元敘述實習行程及課程。第三單元敘述目前無線上網新技術服務的介紹，並著重在無線區域網路的技術，包含應用範圍、目前的標準、系統組成元件、運作模式、IEEE 802.11b 的實體層與資料鏈結層及 802.1x 安全性機制。第四單元則敘述德國西門子公司所提出的次世代語音與網路的整合平台 - SURPASS Solutions and Product Introduction。第五單元為實習心得與結論。

目次：

壹、實習目的

隨著網路技術的進步與應用的普及，人們對於網路的依賴程度與日俱增，除了追求更高的頻寬之外，上網的便利性也成為人們的重要考量之一，只能在固定地點上網已經無法滿足現今許多網路的應用，Internet Everywhere（到處都能上網）的口號逐漸成為人們對於網際網路的新期待。無線上網的結果，會使得人們對於網路網路的使用率激增，除了達成全民上網的願景之外，對於網路服務提供者而言，這其中所蘊含的商機，潛力更是無可限量。因此，身為為ISP業界龍頭的HiNet很早就注意到這個現象，並在先期即積極投入研究與規劃的工作。因此本次職奉派出國實習，主要在於學習無線網際網路的新技術服務，明瞭現今無線網際網路最新技術，了解相關重要技術項目包含各組成元件、運作流程、操作模式，以及相關的安全性機制，並且就歐洲先進的電信公司德國西門子公司新的電信與數據整合技術予以了解。

貳、 實習行程及實習課程

職奉派至德國西門子公司實習『無線上網（Wireless Internet）新技術』，實習時間自民國九十年十一月十二日至九十年十一月二十五日為期十四天。本次實習課程計有：

SURPASS Solutions and Product Introduction課程研習 （4天）

Wireless Internet Access Solutions課程研習（5天）

參、 無線上網新技術

3.1 概說

無線區域網路（Wireless Local Area Network）是一種具有高度彈性的通訊網路。顧名思義，無線區域網路也就是將無線傳輸的技術，應用在原先有線的區域網路環境之中，可省去佈接實體線路所需的工程，只要在無線電波涵蓋的範圍內，使用者都可以透過支援無線區域網路的裝置，如筆記型電腦、個人數位助理（PDA）、或其他手持裝置與網路接駁。無線區域網路同時兼具了無線傳輸的便利性與區域網路的靈活性，可以用來取代或是當做有線區域網路的延伸，並適合在人潮往來頻繁的公共場所中提供上網的服務。

3.2 無線區域網路應用的範圍

由於無線區域網路易於安裝及擴充，而且涵蓋範圍可以從幾公尺到幾百公尺，因此應用的範圍很廣泛，包括：

1. 家庭：可省去佈接實體線路所需的工程，保持居家環境美觀，也可避免因線路過於龐雜而導致維護不易。
2. 校園：學生可以在校園任何地方查詢相關資訊，包括圖書館館藏、課程資訊、校園公告等等。
3. 醫院：醫生及護士可以隨時隨地查詢病人的病歷資料，省去人工調閱的繁瑣手續及等待時間。
4. 營業場所：如旅館、咖啡廳、賣場等等，可額外提供顧客其他加值服務，增加顧客上門率及營收。

5. 公共場所：如展覽場、會議廳、機場、企業辦公場所等等，提供相關在地資訊，而商務人士亦可透過無線網路，即時傳送商情資訊，以配合其業務需求。

6. 建物：大樓的舊線路淘汰，或是新增管線架設不易時，可利用無線區域網路的彈性與易於架設的優點，建構所需的網路環境。

3.3 無線區域網路相關標準

目前已經制定或正在制訂中的無線區域網路規格包括：

IEEE 802.11

這份規格在1997年由IEEE制定完成，其中定義了無線區域網路在2.4GHz頻段的運作規範。原始的IEEE 802.11標準提供1到2 Mbps的傳輸速度，採用FHSS（Frequency Hopping Spread Spectrum）、DSSS（Direct Sequence Spread Spectrum）或IR（Infrared）三種實體層技術，並確保使用同一種實體層技術的不同設備能夠相互通信。此後，許多規格都基於這個標準陸續被制定出來，並提供更高的資料傳輸速度。802.11b提供最高11 Mbps的傳輸速度；802.11a則作業於更高的5 GHz頻段，並將速度提升至54 Mbps。

IEEE 802.11b

這個由IEEE 802.11所延伸出來的規格，由IEEE於1999年制訂完成，在2.4 GHz的頻段提供5.5及11 Mbps的傳輸速度，相容於IEEE 802.11的DSSS，但採用了可以提升傳輸速度的調變技術Complementary Code Keying（CCK）。WECA（Wireless Ethernet

Compatibility Alliance）成立了測試802.11b設備互通性的實驗室，通過互通性認證的設備，就可以貼上Wi-Fi的標誌。此外，802.11b的產品也向下相容於802.11的系統。

Frequency Range	2 4 to 2 4835 GHz
Air Access.	Direct Sequence Spread Spectrum (DSSS) using Complementary Code Keying (CCK)
Data Rate	up to 11 Mbps
Compatibility.	Compatible to 802.11 DSSS 1 and 2 Mbps systems. Not compatible with 802 11 FHSS, Infared (Ir) systems or HomeRF
Operating Range	depends on installation and obstacles, up to 500 m
Applications	all LANs (wireless Ethernet)

IEEE 802.11g

同樣運作於2.4 GHz頻段，但提供高達54 Mbps的傳輸速度，更重要的是，它向下相容於Wi-Fi的產品。對於Wi-Fi產品的使用者而言，可以輕易地將系統提升至802.11g標準，延長了2.4 GHz產品的使用壽命。這份規格於2001年11月在IEEE 802會議中提出，目前是Draft Standard，其中包含必要性（mandatory）及選擇性（optional）的要件：

1. 必要性：OFDM（Orthogonal Frequency Division Multiplexing）是必要的部份，在2.4 GHz頻段中使用OFDM技術，以提升速度至54 Mbps。
2. 必要性： 必須要向下相容於同樣作業於2.4 GHz頻帶的Wi-Fi產品，因此必須提供CCK（Complementary Code Keying）。
3. 選擇性：802.11g將PBCC（Packet Binary Convolution Coding）及CCK/OFDM列為選擇性要件。CCK/OFDM表示每一個資料封包都有一個CCK編碼的前置碼（preamble）及標頭（header），以及OFDM編碼的封包內容。符合802.11g標準意味必須包含第1及2項，但可以不包括第3項。

Frequency Range	2 4 to 2 4835 GHz
Air Access.	Mandatory Complementary Code Keying (CCK) and Orthogonal Frequency Division Multiplexing (OFDM), Optional Packet Binary Convolution Coding (PBCC) and CCK/OFDM
Data Rate	up to 54 Mbps
Compatibility·	Backward compatible with 802 11b Not compatible with 802 11 FHSS, Infrared (Ir), or HomeRF

IEEE 802.11a

802.11a作業於不需申請執照即可使用的5 GHz頻段，採用OFDM技術，提供高達54 Mbps的傳輸速度。另外一個歐洲規格ETSI HiperLAN2也使用了與802.11a相似的實體層（PHY）技術。

Frequency Ranges & Power	5.15 to 5 25 GHz (50 mW), 5 25to 5 35 GHz (250 mW) and 5 725 to 5.825 GHz (1 W)
Air Access	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rates:	up to 54 Mbps
Compatibility	Not compatible with 802 11, 802 11b, HomeRF, HiperLAN/2
Operating Range	depends on installation and obstacles
Applications	Wide Area Networks and Local Area Networks (data, voice, video)

HiperLAN2

這個隸屬於ETSI Broadband Radio Access Networks（BRAN）的計劃使用了與IEEE 802.11a十分類似的技術，包括5GHz的工作頻段及OFDM技術，最大的差別在於媒體存取控制（MAC）的部份。HiperLAN2的連接方式為連接導向（connection-oriented），並採用分時多工技術（TDM），每個頻道都可根據使用的需要，而指定不同的服務等級（QoS），也因為這個特性，HiperLAN2可應用在連接WAN環境中的各個節點。

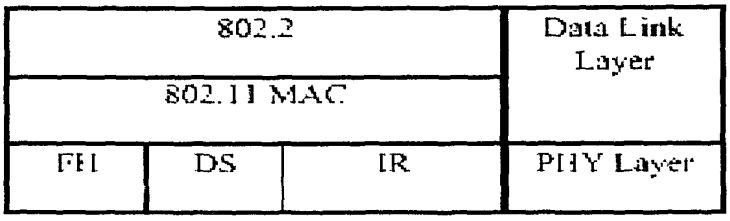
Frequency Range·	5 15 to 5 35 GHz and 5.470 to 5.725 GHz
Air Access	Orthogonal Frequency Division Multiplexing (OFDM)
Data Rates	up to 54 Mbps
Compatibility:	Not compatible to 802.11, 802 11b,802.11g, HomeRF
Operating Range	depends on installation and obstacles, 150m maximum
Applications	WAN/LAN, packetized voice, video, data

以下是一些重要無線區域網路技術標準的對照表。

	802.11	802.11b	802.11g	802.11a	Hiper LAN1	Hiper LAN2
使用頻段 (GHz)	2.4	2.4	2.4	5	5	5
資料傳輸速率 (Mbps)	2	11	54	54	24	54
傳輸距離(m)	100	100	100	30	50	30
調變技術	FHSS	DSSS	OFDM	OFDM	OFDM	OFDM
制定團體	IEEE	IEEE	IEEE	IEEE	ETSI	ETSI
規格確定時間	1997	1999	2001,11	2001		
推廣組織	WECA	WECA	WECA	WECA		

3.4 IEEE 802.11 / 802.11b標準

無線區域網路是否能廣泛的應用，取決於工業界標準的制定，以確保不同廠牌的裝置能夠互通。IEEE於1997年制定了原始的802.11標準，定義了三種實體層（PHY）及一種媒體存取層（MAC）技術（如圖所示），提供1Mbps及2Mbps的傳輸速度，並定義了一些基本的信號處理規範及其他服務。由於傳輸的速度太慢，無法適用於現今多變的網路應用環境，因此IEEE又於1999年9月制訂了802.11b規格（也就是所謂的Wi-Fi），將傳輸速率提升至11Mbps。許多廠商開始宣佈支援此一規格，使得802.11b成為目前最被工業界廣為支援規格，也同時帶動起無線區域網路的市場。



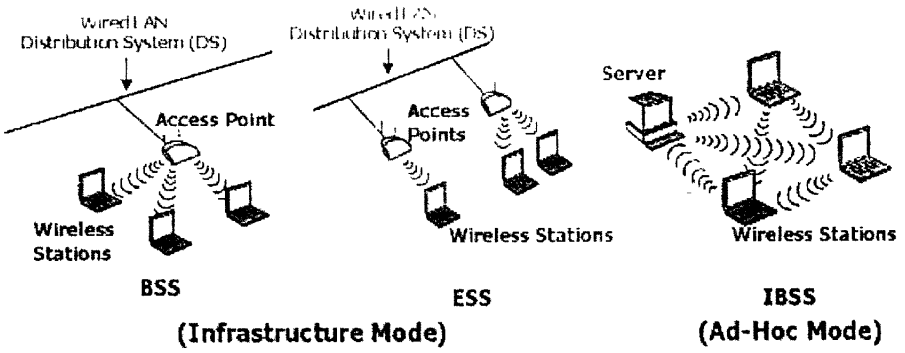
3.4.1 系統組成

一個無線區域網路包含下列兩個基本組成元件：

1. 工作站（Station）：通常指的是配備無線網卡的電腦。
2. 接取點（Access Point，AP）：橋接有線與無線網路的設備，這類設備包含了無線及有線的網路界面，並同時具有符合802.1d標準的橋接功能，扮演無線裝置的基地台的角色。

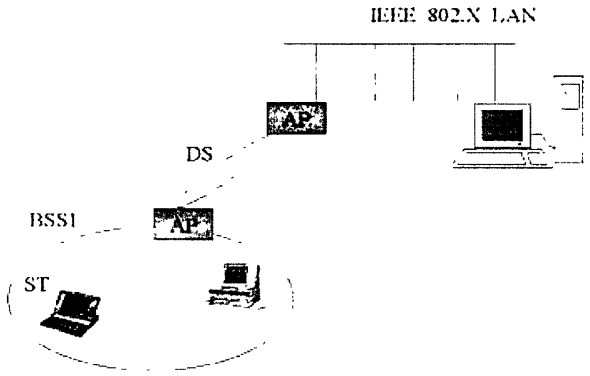
3.4.2 操作模式

分為ad hoc及Infrastructure兩種操作模式，如圖所示。



在ad hoc模式中，各個工作站之間直接互相通訊，而不透過擷取點橋接，這個工作站無線電波所及的範圍便形成了無線區域網路的基本服務區（Basic Service Set，BSS），每一個BSS，都給予一個唯一的識別碼（BSS ID），換言之每一個BSS就是一個Adhoc Network，各工作站只能藉無線媒介來收送訊息，而無法進入其他類型的網路，其結構簡單但延展性較小。這種模式又稱為獨立基本服務區（Independent Basic Service Set，IBSS）。

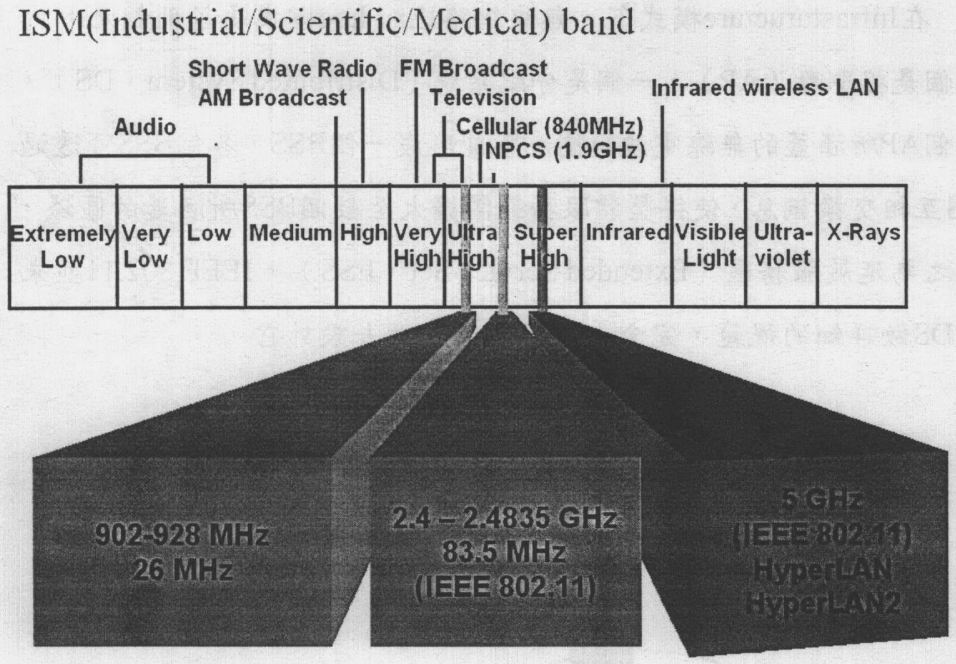
在Infrasturucture模式下，無線網路比ad hoc模式多了兩個元件，一個是接取點（AP），一個是分配系統（Distributed System，DS）。每個AP所涵蓋的無線電波範圍，各自形成一個BSS，各個BSS可透過DS互相交換訊息，使得整體服務範圍擴大至數個BSS所涵蓋的區域，稱之為延展服務區（Extended Service Set，ESS）。IEEE 802.11並未對DS做詳細的規範，完全看各家廠商怎麼去設計它。



透過Infrastructure模式，無線的網路可以與有線的網路介接，使得無線網路的應用與延展性得以發揮至最大。

3.4.3 IEEE 802.11實體層（PHY Layer）技術

802.11定義了三種實體層技術，包括兩種展頻技術（Spread-spectrum）及紅外線（Infrared）。兩種展頻技術分別為跳頻展頻（Frequency Hopping Spread Spectrum，FHSS）及直序展頻（Direct-Sequence Spread Spectrum，DSSS），但這兩種展頻技術的原理並不相同，也不能協同工作。工作頻帶則為2.4GHz ISM頻帶，如圖所示

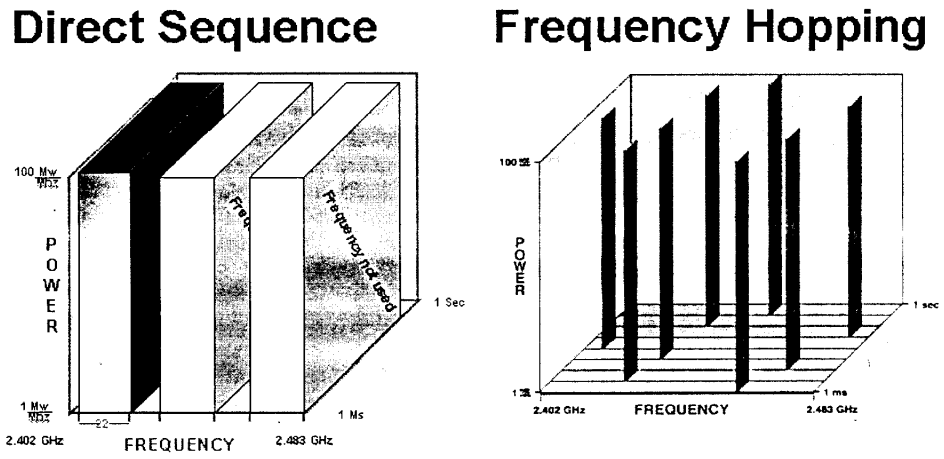


3.4.3.1 跳頻展頻（FHSS）

FHSS將2.4GHz的頻帶分成75個1MHz頻道，發送端和接收端會先協定好一組跳頻順序，接著資料就照這個跳頻順序在各頻道間傳送。每次資料的送收，都有不同的跳頻順序，所以這樣的設計可避免兩個發送端同時使用同一個頻道。FHSS的無線技術並不困難，但是最高速度被限制在2Mbps之內，這是因為FCC規定每個頻道不可超過1MHz，迫使FHSS必須將所有頻道分佈在整個2.4GHz的頻帶上，其跳頻的速度約為每30秒75個頻道，所以一個頻道最多只能使用0.4秒後，就必須跳到另一個頻道，每一次跳頻都會讓系統產生額外的負擔（Overhead）。

3.4.3.2 直序展頻（DSSS）

DSSS將2.4GHz的頻帶分為14個22MHz頻道，每個相鄰的頻道有部份相互交錯（Overlap），但其中有3個頻道不與其他頻道交錯。資料在22MHz的頻道傳送時毋需跳頻，為了解決雜訊問題，資料在傳送時會加上填充比次（chips），這些填充比次提供了檢查錯誤的機制，因此即使資料有部份遺失，在許多情況下都能自動修正，明顯降低重新傳輸的次數。



基本上，FHSS所需的功率較DSSS要低，而且成本也低，但相對地，所能提供的傳輸速率也較低。因此，DSSS會朝高速無線區域網路的方向應用，而FHSS會往低價的網路應用發展，提供SOHO及家庭應用，或週邊之無線設備連結。

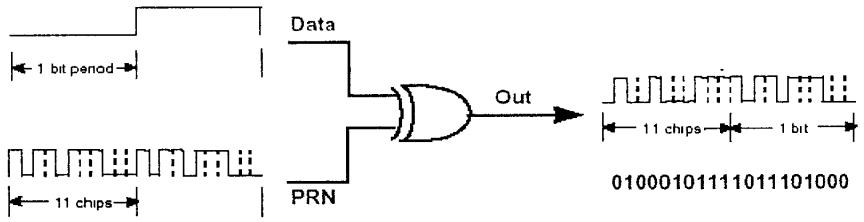
3.4.3.3 紅外線（Infrared）

其技術類似於電視遙控器，使用的頻率接近可見光，無法穿透不透明物質，有效傳輸距離較短，一般多用於室內環境。對於移動範圍較廣的空間則不適用。

3.4.3.4 IEEE 802.11b實體層（PHY Layer）加強部份

802.11b最關鍵的貢獻之一，就是針對實體層的部份加強，使得傳輸速率達到5.5Mbps及11Mbps。為了達到這個目標，採用DSSS成為唯一的選擇，這也意味著802.11b僅能向下相容於802.11的1Mbps及2Mbps DSSS模式。

原始的802.11 DSSS使用11個位元的比次（chips）來代表一個資料位元，稱之為Barker sequence（如圖所示）。這些比次被轉換為電磁波在空氣中傳遞，稱為Symbol，利用BPSK調變技術，傳輸速度可達1MSps（Million Symbols Per Second），當採用QPSK調變技術時，速度可提升至2Mbps。



11 Bit Barker Code (PRN):
1 0 1 1 1 0 1 0 0 0

為了要增加傳輸速率，必須使用更複雜的編碼技術，以提升無線頻道的使用效率，802.11b使用了CCK（Complementary Code Keying）技術。5.5Mbps每個載波可編碼4位元，11Mbps則可到8位元。各技術之不同點如下表。

Table 1. *802.11b Data Rate Specifications*

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

3.4.4 IEEE 802.11資料鏈結層（Data Link Layer）技術

資料鏈結層分為兩大部份：邏輯鍵結控制（Logical Link Control，LLC）及媒體存取控制（Media Access Control，MAC）。802.11使用與其他802系列相同的LLC及48位元定址方式，因此可以很輕易地與原先有線的網路接軌。MAC層則與802.3的概念十分相似，也就是讓共享同一傳輸媒介的多個使用者，在傳送資料之前先偵測是否有其他人正在傳送。802.11 MAC定義了兩種存取方式：Distributed Coordination Function（DCF）及Point Coordination Function（PCF）。

3.4.4.1 CSMA/CA

DCF實際上就是所謂的Carrier Sense Multiple Access with Collision Avoidance（通常被稱為CSMA/CA）。CSMA的運作方式如下：當工作站要傳送資料之前，會先偵測介質是否忙碌（也就是是否有其他的工作站正在傳送資料），如果有，也就是所謂的碰撞（Collision），則會等待一個隨機產生出來的延遲之後，才會再次偵測傳送介質是否正被使用，這個協定在傳輸介質不很忙碌時很有效率。當介質經常忙碌時，就有可能會發生因同時需要傳送資料，而使得有些工作站必須等待。在乙太網路的環境中，發送端的MAC層會偵測到碰撞情形，並延遲一段時間才會重送，這種演算法稱為Exponential Random Backoff。

這樣的碰撞偵測機制在有線區域網路中沒有問題，但不適用於無線區域網路，主要原因有二：

1. 這個碰撞偵測機制需要具備全雙功功能的無線模組，才能同時傳送及接收資訊，這會使得成本提高。

2. 在無線的環境中，我們不能保證每個工作站都能互相「聽取」對方；而且當發送端附近的傳輸介質不忙碌時，不代表接收端附近的介質亦不忙碌。

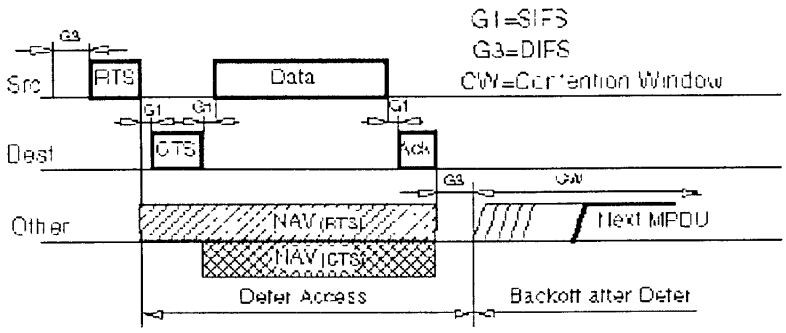
為了解決這些問題，802.11提出一套避免碰撞（Collision Avoidance）及正面回應（Positive Acknowledge）機制，其運作原理如下：

當發送端要傳送資料時，先偵測介質是否忙碌，如果忙碌則延遲發送；如果介質在一段指定的時間（稱之為Distributed Inter Frame Space，DIFS）內都無人使用時，才能傳送資料。接收端在收到封包後會檢查CRC內容，並回應一個ACK封包。當發送端收到此ACK封包時，即表示無碰撞發生。如果發送端沒有收到ACK回應，則會繼續嘗試發送同一封包，直到收到ACK回應，或是超過一定之重傳次數。

為了降低碰撞發生的頻率，802.11定義了一個Virtual Carrier Sense機制，運作方式如下：

當發送端要傳送資料時，先送出一個小控制封包，叫做RTS（Request To Send），裡面包含了發送端、接收端、及接下來封包（也就是資料及ACK封包）收送所允許的時間，如果接收端能夠接收資料（即介質沒被佔用），會回應一個CTS（Clear To Send）控制封包，裡面也會包含下次送收允許的時間。所有收到RTS/CTS的工作站會將此時間記錄在Network Allocation Vector（NAV）中，並利用這項資訊做為偵測介質狀況的依據。在這段時間內，介質會被「標示」為使用中，直到這次的送收完成為止，所以能降低碰撞發生的機率。由於RTS/CTS是小封包，因此萬一在傳送時發生碰撞，也因為遠比一般資料封包要小，所以也降低了碰撞所產生額外負擔（Overhead）。此外，802.11也允許小封包可以不透過RTS/CTS的機制來傳送，並透過每個

工作站的RTSThreshold參數加以控制。RTS/CTS的運作原理可參考下圖。



3.4.4.2 封包的分割與重組

一般有線區域網路的最大封包限制在1518位元組，也就是所謂的MTU（Maximum Transmission Unit）；但在無線區域網路中較小的MTU可能比較適合，原因如下：

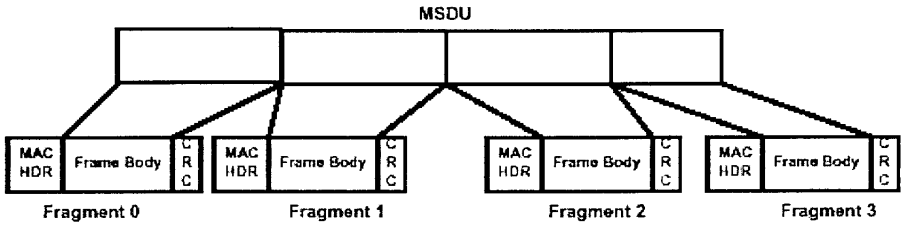
1. 因為無線環境干擾較多，位元錯誤率（Bit Error Rate，BER），通常較有線環境要高。封包越大，封包資料錯誤的機率也越高。
2. 當資料封包錯誤需要重傳時，小封包所產生的額外負擔（Overhead）也較大封包來得小。
3. 在跳頻系統下，頻道會週期性的跳躍，所以封包越小，被延遲的機率也越低。

但換個角度來看，如果發展一個不能處理1518位元組封包的無線區域網路，顯然不太合理。為了解決這個問題，802.11在MAC層加入了封包分割（Fragmentation）及重組（Re-assembly）的機制，封包在傳送端會先被分割成適當的大小，接收端收到之後再將封包重新組

合。這個機制基本上是一個「傳送/等待」的演算法，工作站在傳送新的分割之前，必須滿足以下任一條件：

1. 收到前一個分割的ACK。
2. 分割重送次數過多，整每封包都被丟棄。

下圖所顯示的是一個封包（MSDU）被切割成數個分割（MPDU）。



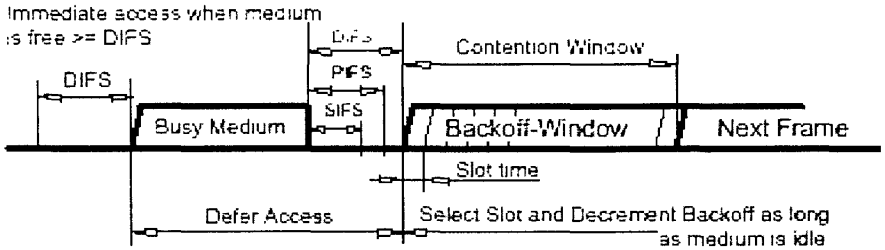
3.4.4.3 Inter Frame Space（IFS）

802.11定義四種IFS，各有不同的優先順序：

1. SIFS：Short IFS是用來區隔一次的送收（即Fragment-ACK），同時最多只能有一個工作站在這段時間內傳送資料，因此優先權最高。在802.11跳頻模式下，這個值為28 microsecond。
2. PIFS：Point Coordination IFS是用來讓AP（也就是Point Coordinator）取得傳輸媒介控制權，這個值是SIFS再加上Slot Time（定義見3.4.4.4），也就是78 microsecond。
3. DIFS：Distributed IFS是一個工作站決定要開始傳送資料前所需等待的時間，其值為PIFS再加上Slot time，也就是128 microsecond。
4. EIFS：當工作站收到無法解釋的分割時，Extended IFS被用來避免後續的碰撞問題。

3.4.4.4 Exponential Backoff演算法

所謂的Backoff是一種解決多個工作站因同時都要存取傳輸介質所引發的競爭問題，每個工作站會任選一個隨機數值N，並等待N個時槽之後才嘗試存取傳輸介質。其運作方式如圖所示。



所謂Slot time指的是從發送端偵測到碰撞後到重新再傳送資料前所等待的時間，發送端會根據當時的狀況，決定出適當的Slot time，這樣的機制可將碰撞發生的機率減為原來的一半。

Exponential Backoff指的是當發送端決定要送出資料，但卻發生碰撞時，會再等待N個slot，而這個N會隨著碰撞發生的次數做級數增加。

當下列情況之一發生時，就必須使用此演算法：

1. 當工作站在發送第一個封包時，偵測到傳輸介質正被佔用。
2. 在每次封包傳送後。
3. 在每次封包成功傳送後。

3.5 無線網路的安全機制

在建構無線網路環境時，安全性是一個很重要的課題。在無線網

路的環境中，安全性的威脅要比有線環境來得大，因為在無線環境中，入侵者可以輕易的側錄你的無線電波通訊內容，而且追查不易，很多機密的資訊會因此洩漏。

3.5.1 第一代安全性機制

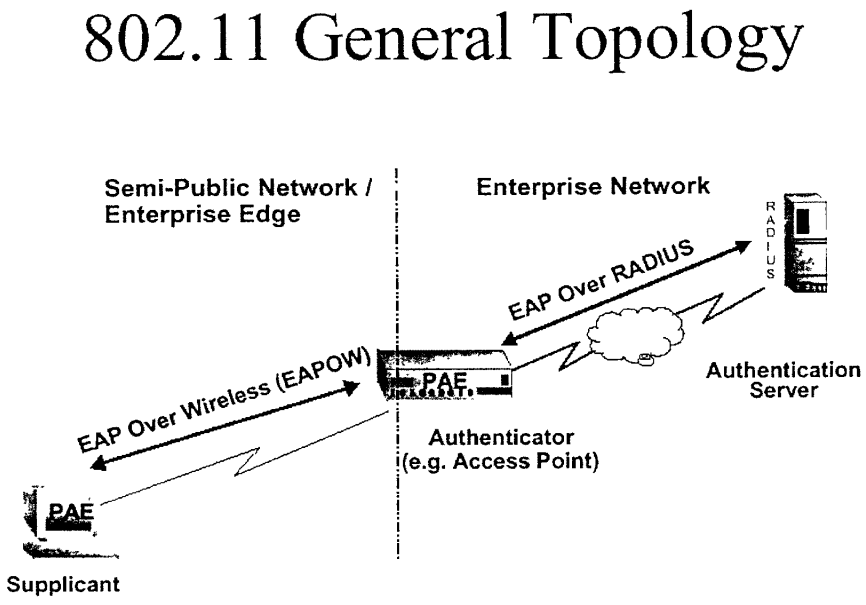
原始的802.11定義了兩種安全性機制，一個是「服務區識別碼」（Service Set Identifier，SSID），一個是WEP（Wired Equivalent Privacy）。當工作站要連接AP時，必須要設定與該AP相同的SSID才能通訊，這個方法並不安全，因為AP會廣播它的SSID出去，入侵者只要在AP附近竊聽封包，即可得知SSID的內容。WEP是透過一組相同的KEY來對傳輸資料做加解密，這個加密方式已經證明在15分鐘內即可破解。此外，有些AP還提供一種簡易的MAC位址認證機制，只有那些MAC位址有設在AP上的工作站才允許通訊，但這種認證方式除了需要大量的人工設定之外，只能做到工作站的認證，而不是使用者的認證，也就是只認證無線網路卡，而不是認證使用網路的人，而且此認證方式並不適用於在公共場合提供無線服務。因此，這些所謂的第一代基本安全防護機制並不堪用。常見的安全性漏洞包括：

1. 工作站被不明人士使用，WEP key通常存在硬碟或無線網路卡上，也可能一併被盜用，為了安全性的考量，所有使用相同key的工作站可能都要變更key。
2. 入侵者在原AP附近放置另一個AP（即所謂的Rogue Access Point），並複製相同的資訊（可經由竊聽AP封包達成），使用者在連接上AP時，並不能確認所連接上的是否為合法的AP，因此入侵者可以竊取使用者資訊。

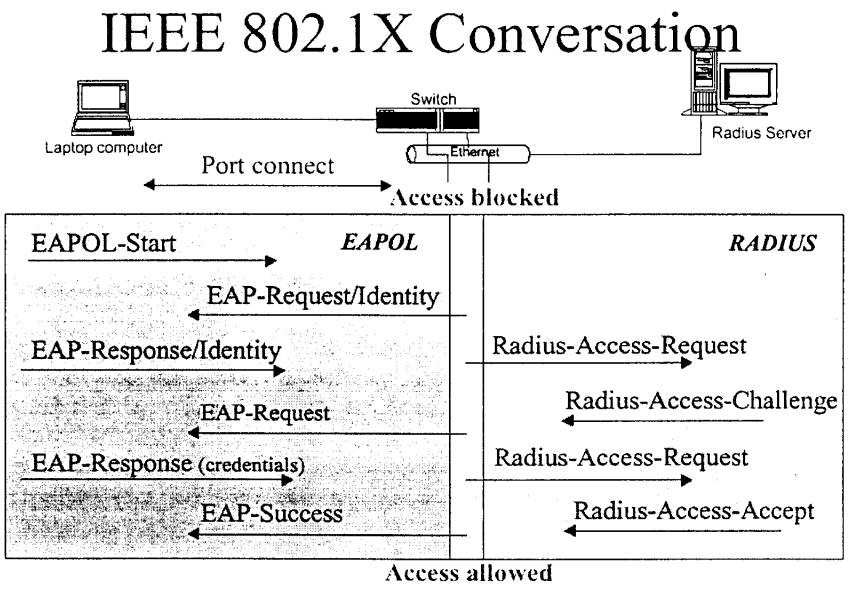
3. 入侵者可以透過封包抓取軟體，重組使用者封包，以擷取出機密的資訊。這些軟體如AirSnort、WEPCrack、NetStumbler等等，很多都可以從網路上免費下載，取得十分容易。

3.5.2 IEEE 802.1x

IEEE根據EAP(Extensible Authentication Protocol，IETF RFC 2284）為基礎架構制定出802.1x標準。主要目的是為所有IEEE 802系列技術（包括有線及無線）提供一套原本所缺乏的安全認證機制。EAP是屬於Layer 2的傳輸協定，客戶端的認證過程是發生在鏈結層（Link Layer），毋須先取得IP位址。EAP對網路設備如交換器（switch）或AP而言是透通的，因此要在此架構上開發新的認證方式時，只需在前端及後端新增功能即可，毋須更新中間的網路設備。802.1x架構如下圖所示：



典型的802.1x的運作模式如下圖所示：



3.5.3 EAP認證方式

根據EAP架構，目前已發展出許多認證方式，包括：

- EAP-MD5

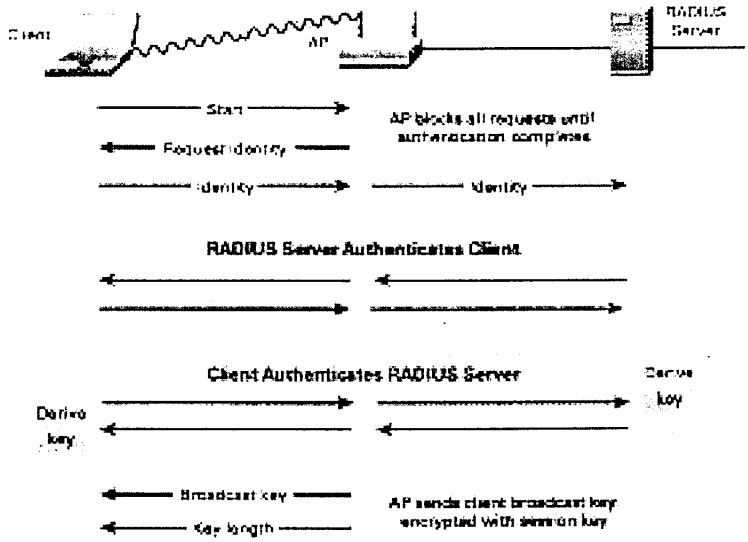
  基本是上使用者名稱/密碼的認證方式，使用者名稱由明碼傳送，認證主機在收到請求之後會送出Challenge要求客戶端送密碼，客戶端會將Challenge及密碼做MD5加密後送至認證主機，認證主機重覆上述步驟，若兩者結果相等表示認證成功。此認證方法有下列缺點：

  1. 只用一組手動設定的WEP key，並不支援動態WEP key。
  2. 容易被猜中密碼（dictionary attack）。
  3. 只提供伺服端對客戶端的認證，客戶端無法得知認證主機是否合法，即可能會暴露在Man-in-the-middle攻擊。

這是802.1x中最不安全的認證機制。

- LEAP

  Lightweight EAP由Cisco所提出，運作方式和EAP-MD5類似，但在認證過程中使用動態的session key，安全性較高，但必須使用支援LEAP的AP及認證主機。此外，LEAP還是有可能會遭到dictionary式的攻擊。運作方式可參考下圖。



- EAP-TLS

  由Microsoft所提出，其認證原理與現今HTTP-SSL類似，也就是在EAP中建立TLS（Transport Layer Security）通道來傳送認證訊息，客戶端及認證伺服器互相交換電子憑證（certificate），因此能做到相互間的認證，避免遭到man-in-the-middle攻擊。每次的認證過程都使用不同的key來加密，客戶端也可隨時發出重新認證（re-authentication）的請求來取得新的key，而不影響現有的連線，因此安全性更高。它的缺點在於必須在每個客戶端及認證主機上都要安裝電子憑證，就目前環境而言，執行上較困難。

- EAP-TTLS

  由Funk Software所提出，可看成是EAP-TLS的延伸。它同樣提供一套客戶端與認證主機相互認證的機制，但是在驗證客戶端的部份採用了較簡單的方式，客戶端不需要安裝電子憑證。它比EAP-TLS好的一點是，使用者名稱在TLS通道建立後才傳送，而不是以明碼傳送。目前唯一的缺點在於這個標準尚未獲得Internet社群普遍的認可；此外，IETF也正在制定一個類似的標準，PEAP（Protected EAP），同樣解決了EAP-TTLS所解決的許多問題。

各種EAP認證的比較可參考下表說明。

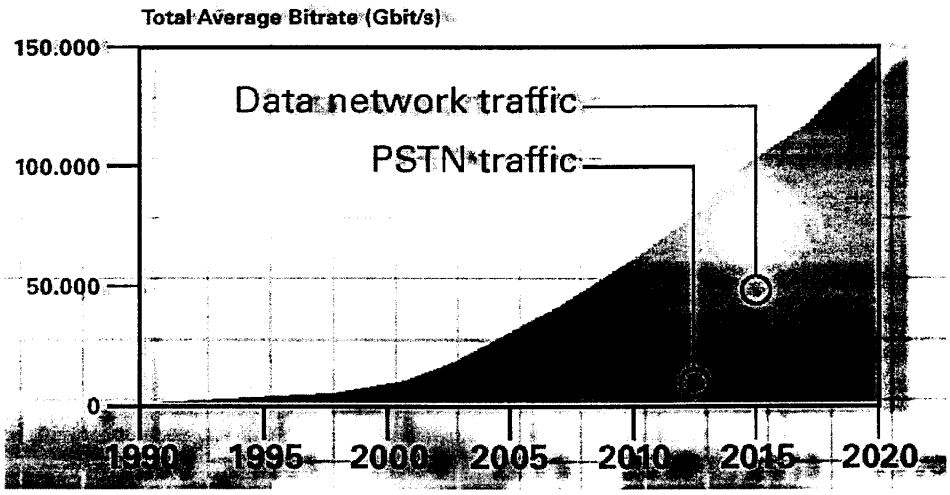
Security Methods Comparison

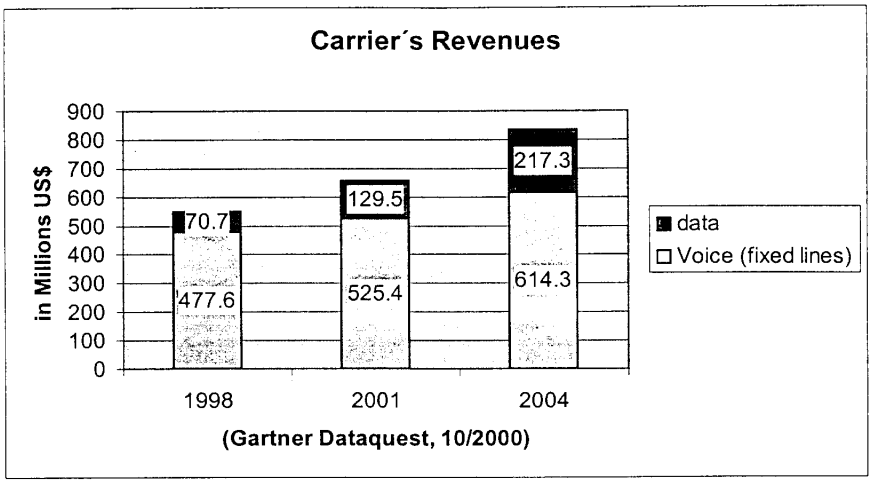
Topic	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (FUNK)
Security Solution	Standards-based	Proprietary	Standards-based	Standards-based
Certificates – Client	No	N/A	Yes	No
Certificates – Server	No	N/A	Yes	Yes
Credential Security	None	Weak	Strong	Strong
Supported Authentication Databases	Requires clear-text database	Active Directory, NT Domains	Active Directory	Act. Dir., NT Domains, Token Systems, SQL, LDAP
Dynamic Key Exchange	No	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes

肆、 SURPASS Product and Solutions Introduction

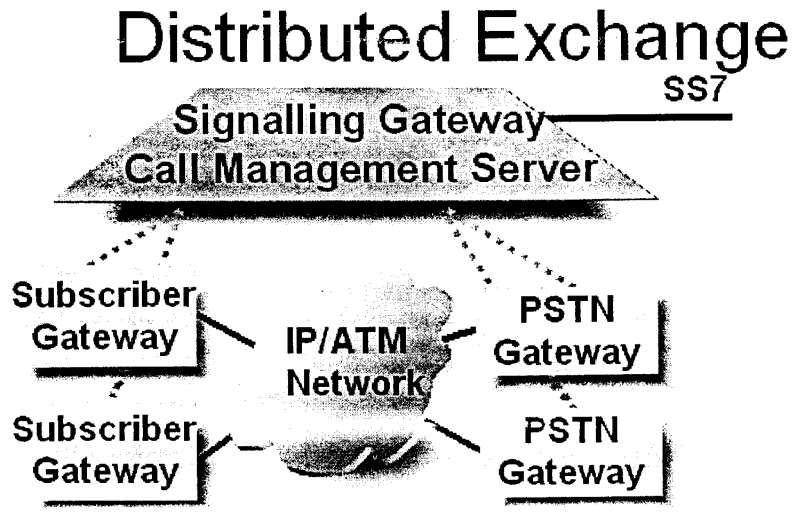
4.1 SURPASS概說

目前最大的兩個網路系統，也就是公眾交換電話網路（PSTN）及網際網路（Internet），就全球的應用而言，其流量已經達到不分軒輊的程度，但隨著以IP為基礎的應用日益廣泛，資料網路的流量終將超越電話網路（如圖所示）。即使如此，目前電信業者最主要的收入來源仍然是電話服務，且在短時間之內似乎不會有太大的轉變（如圖所示），因此能夠成功結合成本較低廉的IP網路並同時提供電話服務的業者，才有機會在市場上成功。然而，單純的電話服務也漸漸無法滿足現今多樣化的需求，電信業者所需要的，是一個可以整合電話及電腦網路的完整解決方案。





SURPASS是德國西門子公司針對於新世代網路架構所提出的統一解決方案，它其實是由許多Datacom及Telecom的產品所組成，企圖在各種異質的網路架構下，提供整體與統一的工作平台。此架構主要的特點為：以IP為基礎的骨幹網路、分散式架構、集中式管理、媒體閘道（media gateway）控制、接取閘道控制、以及開放式的標準介面，加速各類服務的提供（Service Creation）。其基本精神如下圖所示：



4.2 SURPASS組成元件

SURPASS組成元件包括：

- SURPASS hiQ：Servers and controllers
- SURPASS hiR：Resource Servers
- SURPASS hiS：Multiprotocol signaling gateways
- SURPASS hiG：Media gateway
- SURPASS hiA：Multi-service access

系統架構圖、各元件系列產品及功能如下所示：

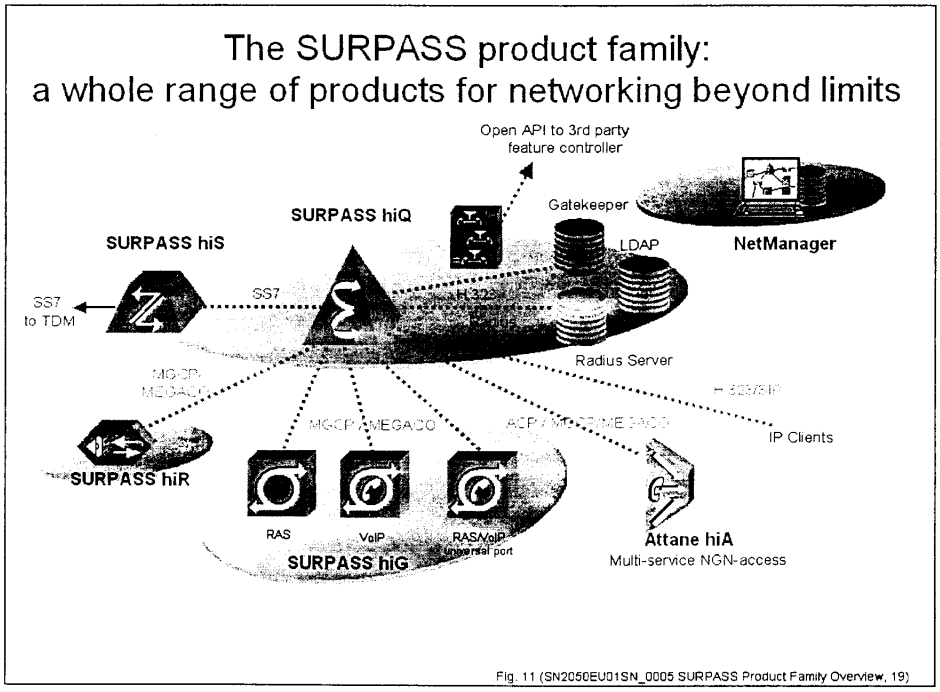


Fig. 11 (SN2050EU01SN_0005 SURPASS Product Family Overview, 19)

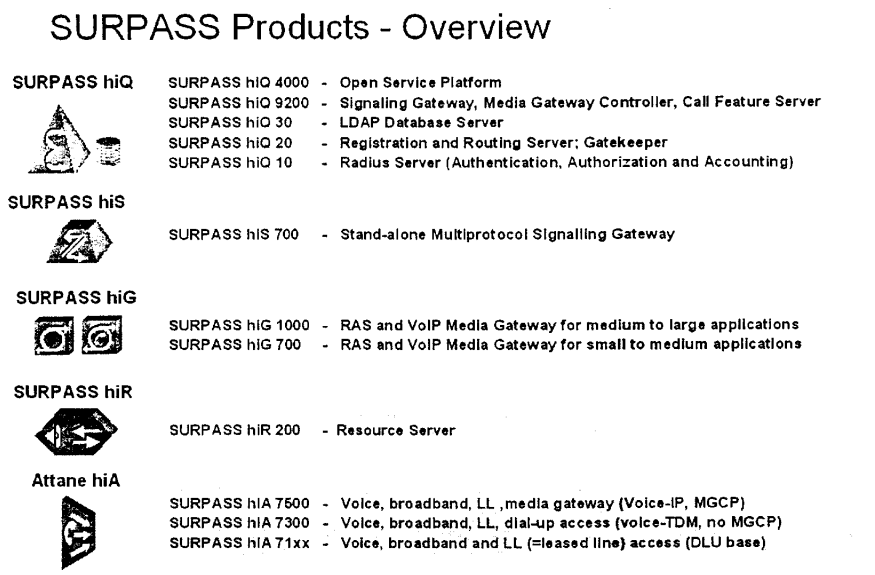
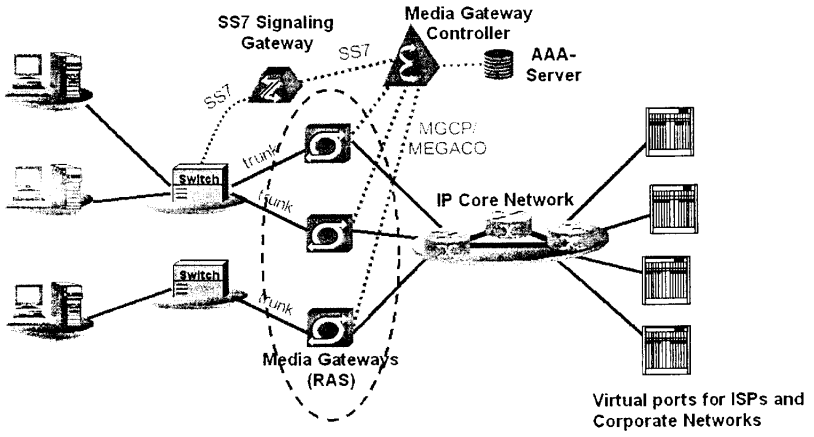


Fig. 12 (SN2050EU01SN_0005 SURPASS Product Family Overview, 19)

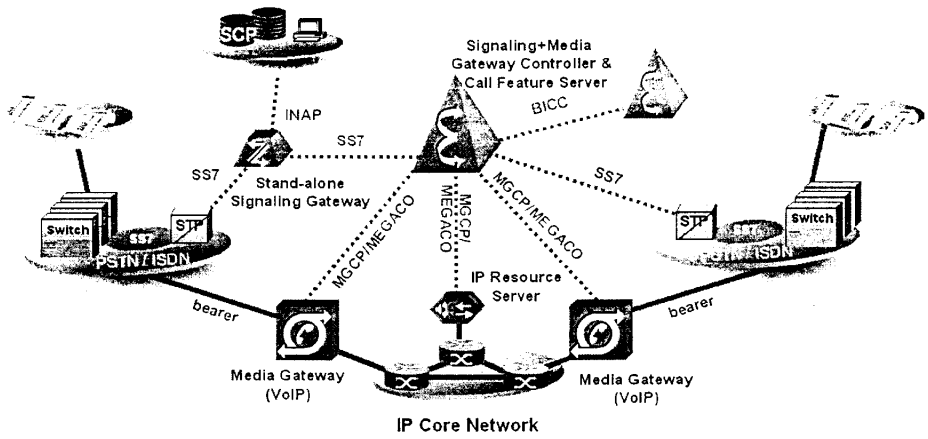
4.3 SURPASS解決方案

SURPASS所提出的解決方案，最主要包括下列幾個項目：

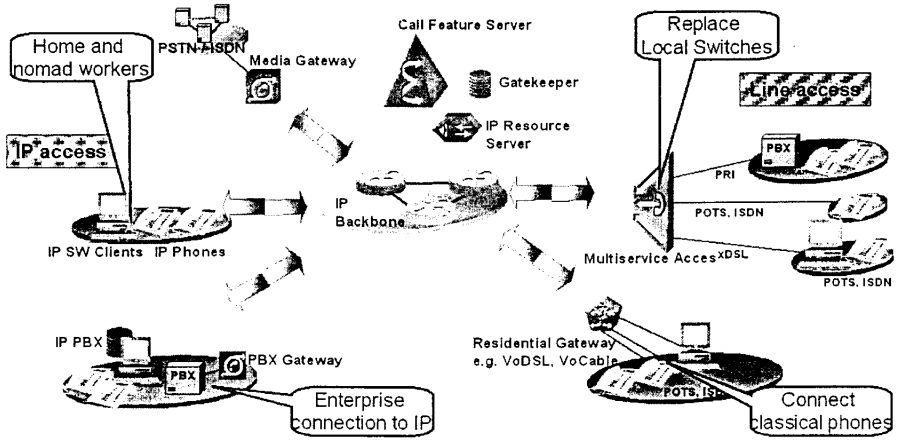
1. Carrier Class Dial-in（CCD）：透過SS7 signaling gateway及Media Gateway Controller，將RAS與PSTN之連接做有效率的管理，降低維運成本，並對整體資源做更有效率的使用。



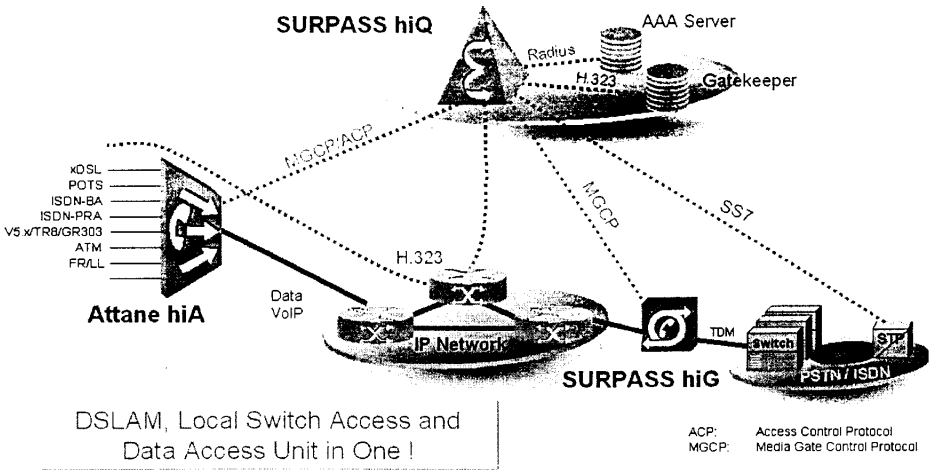
2. Virtual Trunking（VT）：經由Media Gateway Controller控制Media Gateway，將Circuit-Switch的語音資訊與Packet-Switch的語音封包作轉換，中間透過IP網路來傳送，節省維運及擴充成本。



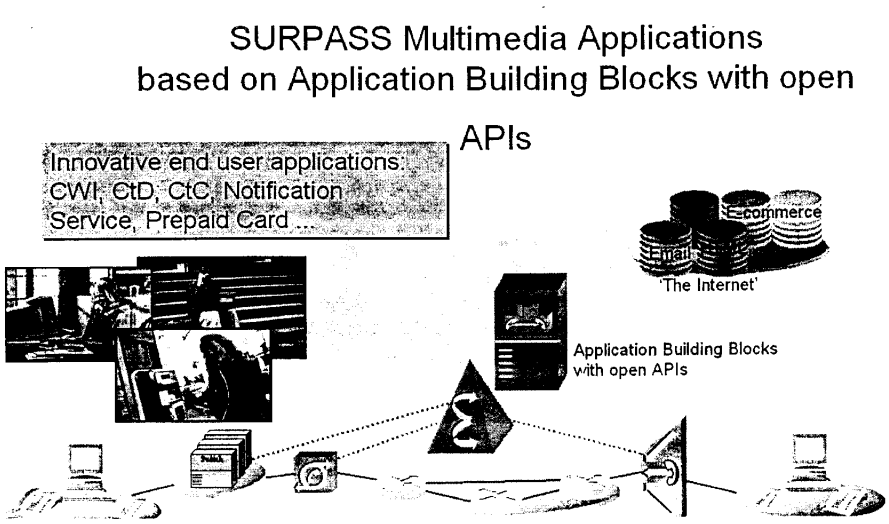
3. Next Generation Local Switch（NGLS）：擴充Local Switch功能，提供SS7與VoIP信號（H.323/SIP）、E.164與IP位址間的轉換，提供使用者透通性的網路整合功能。



4. Multi-Service Access（MSA）：透過Attane hiA提供各類接取服務，包括xDSL、POTS、ISDN、V.5x/TR8/GR303、ATM、Frame Relay、SMDS、Leased Line、Circuit Emulation。



5. Multimedia Applications（MMA）：提供開放式應用程式開發介面及建構區塊（Building Block），讓服務提供者能快速開發多媒體應用服務，包括Internet Call Waiting、Click-to-Dial、Prepaid Card等等。



4.4 結語

SURPASS提供的解決方案，最主要是將電話與電腦網路加以整合，而其目的是為了提供一個單一骨幹網路（也就是IP網路），以及多樣性的電信服務，並藉以降低建置與維運成本，進而創造出更高的營收，這將是未來電信服務的新趨勢。

伍、 實習心得與感想

隨著網路的普及化，網路科技的進步可謂一日千里，接取技術更是隨著無線網路的興起而有不同的風貌。無線網路帶給使用者的便利性，以及網路架構設計上的彈性，顯示出無線網路未來發展的潛力驚人。然而，目前無線網路的發展方興未艾，各種不同標準之間的互通性、傳輸速度仍待提升、以及安全性的考量等等，也顯示出無線網路在未來的發展上仍有很大的空間。能有機會參與這次無線上網新技術的實習，深感榮幸，經由實際了解德國西門子公司無線網路的解決方案，對今後所參與的網路系統必能有所助益。以下謹提出個人的心得與體驗，希望能對從事無線網路接取服務的相關同仁有所助益。

1. 未來無線區域網路在結合大範圍的行動通訊網路（如第三代行動電話系統）及短距離的個人無線網路（如藍芽），將可建構起一個完整的無線網路環境。我們應該密切注意這些技術的後續發展，以因應各種不同的應用及需求。

2. 對於無線上網的安全性機制而言，應捨棄EAP-MD5認證方式及靜態WEP Key編碼方式等已經證明可以在短時間內被破解的安全性機制。建議採用的認證方式包括EAP-TTLS或EAP-PEAP；以及編碼方式如TKIP（Temporal Key Integrity Protocol，WEP2）或802.11i AES（Advanced Encryption Standard），以保障無線網路使用者的隱私，消除使用者疑慮，並提高使用意願。

3. IEEE 802.11b為目前最廣為工業界支援的標準，產品線也最齊全，而802.11a/b雙模（dual-mode）及802.11a/b/g三模（triple-mode）的產品目前尚未成熟。建議公司可先推行採用

802.11b規格的無線網路服務，未來視市場需求，再將既有無線網路環境升級成支援多模的架構，以提供更高的頻寬。

4. 無線通訊是未來的趨勢，全球網路業者無不投注大量的心力在這個新興的市場上，建議公司應及早切入無線網路市場，利用身為國內最大ISP業者的優勢與資源，以永續保持業界領先的地位。