

<b>Course Name:</b>	Securing Your Wireless Networks
<b>Duration:</b>	1 Day
<b>Medium of Instruction:</b>	Cantonese (with handout in English)
<b>Award of Certificate:</b>	Certificate of Attendance

### **Nature and Objectives:**

The rapid development of wireless technologies and industry standards enables organizations to strengthen their communication and enhance the applications of IT at reduced costs. Wireless technologies provide unique benefits of quick, flexible and inexpensive deployment and modification. However, it also creates concerns in deployment, management and security. Even if you are experienced with traditional / wired networks, you need to take a step back and survey the technology, the facility where the network will be installed, and the equipment that is available before you jump in and start building wireless networks. The course provides participants with comprehensive information to design, implement and manage wireless networks.

### **Who Should Attend:**

Professionals responsible for making decision to invest, design, implement and administer of wireless networks.

### **Course Outline:**

#### **OVERVIEW OF RADIO COMMUNICATION**

- Evolution of Radio Communications
- Radio Frequency technology
- 802.11 protocol series
- Cellular Telephony and 3G network
- Advantages of the Wi-Fi Networks

#### **WIRELESS NETWORK FUNDAMENTALS**

- Wireless Communication Basics
- 802.11 Protocol Stack
- WLAN components

#### **WIRELESS NETWORKS IMPLEMENTATION**

- Wireless Network Architecture
- Ad-Hoc wireless LAN, Infrastructure Mode and Wireless Bridge
- Preparing for Operational Support of a Wireless LAN
- Wi-Fi channels and Frequency reuse
- RF Antenna characteristics
- MIMO (Multiple-In, Multiple-Out) Smart Antenna

#### **WIRELESS SECURITY**

- Assessing WLAN vulnerabilities
  - Types of Attacks
  - Peer attacks and Information Theft.
  - Susceptibility of wireless-enabled laptops
  - WAR driving

#### **WIRELESS SECURITY**

- Security weaknesses of and attacks to wireless LANs
  - RF Jamming and Data Flooding (DoS)
  - Rogue Hardware and Default Settings for WLAN equipment
  - Malicious and inadvertent interference
  - Intercepting Wi-Fi traffic
  - Forcing client de-authentication
- Wireless Devices Security
  - Wireless Gateway Security
  - Wireless Station Security
- Wireless LAN Assessment

#### **PROTECTING DATA AND ACCESS CONTROLS**

- Wired Equivalent Privacy (WEP)
  - Cryptography in Wireless Network
  - RC4, AES, RSA
- Security protocols for Wireless LANs
  - Wi-Fi Protected Access 802.11i (WPA/WPA2)
  - Temporal Key Integrity Protocol (TKIP)
  - 802.1x, Extensible Authentication Protocol (EAP)
- Enterprise Wireless network.
  - Deployment of Wireless Access Points
  - VPN technologies in Legacy Wireless Networks