London Metropolitan Network Advanced Technology Seminar
28th January 2009 at 11a.m. – 13.00 p.m.

Network Security

Examining Network Security Fundamentals
The Need for Network Security
Network Security Objectives
Basic Security Assumptions
Basic Security Requirements
Confidentiality
Integrity
Availability
Data Classification
Security Controls
Response to a Security Breach
Laws and Ethics
Laws
Ethics
Liability
Policy

Examining Network Attack Methodologies
Adversaries, Motivations, and Classes of Attack
How Hackers Think
The Principles of Defense in Depth
IP Spoofing Attacks
Confidentiality Attacks
Integrity Attacks
Availability Attacks
Best Practices to Defeat Network Attacks

Secure Network Lifecycle Management
Principles of Operations Security
Network Security Testing

Unified Communications

Benefits of Cisco Unified Communications
Cisco Unified Communications System
Cisco Unified Communications Infrastructure Layer

Call Processing Agents
Endpoints
Applications

Messaging
Cisco Auto-Attendants
Cisco Unified IP IVR
Cisco Unified Communications Mobile Solutions
Cisco Unified Presence
Cisco TelePresence

Introducing VoIP & IPT
Introducing Voice Gateways
Specifying Requirements for VoIP Calls
Understanding Codecs, Codec Complexity, and DSP Functionality

Converged Networks Quality Issues
Bandwidth
End-to-End Delay
Packet Loss
QoS Requirements
QoS Policy
QoS for Converged Networks

IPv6

Explaining the rationale for IPv6
Evaluating IPv6 features and benefits
Describing the IPv6 Header Format

IPv6 Transition Mechanisms
Implementing Dual Stack
Describing IPv6-to-IPv4 Transition Mechanisms
Other Tunneling and Transition Mechanisms
Describing IPv6-over-IPv4 Tunneling Mechanisms and IPv4 Addresses in IPv6 FormatNAT-PT

Explaining IPv6 8-4
Describing IPv6 Features
Defining IPv6 Addressing
Describing IPv6 Addressing Architecture
Defining Address Representation
IPv6 Address Types

Routing with RIPng
Examining OSPFv3
Examining Integrated IS/IS
Examining EIGRP for IPv6
Understanding BGP (BGP4+)