NO	CODE	NAME	COMPANY	TITLE OF TUTORIAL	BIODATA OF SPEAKER	ABSTRACT OF TUTORIAL
1	MTA:ISP Security: Deploying and Using Sinkholes	Danny McPherson	Arbor Networks	ISP Security: Deploying and Using Sinkholes [1/2 Day Tutorial]	Danny McPherson is currently a member of the Architecture and Development groups at Arbor Networks. Prior to Arbor he was Director of Emerging Technology at Amber Networks (acquired by Nokia). He has held technical leadership positions with Qwest, Genuity & WCI and still maintains consultancy roles with several service providers. Danny currently chairs the IETF's PWE3 Working Group and is a member of several IETF directorates and IRTF research groups. He is a common contributor within the Routing, Operations and Internet Areas of the IETF, and is also active within PPVPN & MPLS related work. He has authored a number of RFCs, books and other documents related to IS-IS, BGP, OSPF, Network Security, IP addressing and several other areas. He is an active contributor to NANOG and the operator community in general, serves on the MPLScon advisory board, and commonly contributes to several other standards organizations and activities.	This tutorial will explain how to build a sinkhole, using generalized examples from ISP deployments around the world. Configuration using JUNOS and IOS will be used to demonstrate the various ways trigger routers and target routers in the sinkholes are safely, scalably, and efficiently configured. Architectural considerations relating to network topology and placement of sinkholes in the ISP's network will be covered, along with anycast deployment options. A multitude of tools that can be placed inside the sinkhole will also be discussed. These include a variety of freeware, shareware, home-built, and commercial tools - covering the diversity available to ISPs of any size. This tutorial is recommended to ISP engineers of all experience levels. The source materials are derived from live operational deployments, which can be modified and applied to any large IP transport network.
2	MTA;Mitigating D/DOS Attacks	Seo Boon Ng	Cisco	Various technique in mitigating D/DOS attacks [1/2 Day Tutorial]	There will be two instructors: Ng Seo Boon - Network Consulting Engineer from Cisco System. Primary job responsiblity is to work with large ISP in North Asia. Helping in their running of their network and mitigating D/DOS attacks. Network design and such. Have spoke on this topic in Apricot2003. Nick Satsia - Network Consulting Engineer from Cisco System. Have extensive working experience with ISP in Korea, Malaysia and Australia. Perform network design and review for customers.	half to 1 day session on various D/DOS mitigation technique base on Barry Green's security bootcamp presentation. There will be hands-on lab training on various technique namely; - using ACLs - using Netflow - remote trigger blackhole - sinkhole - Various steps to response to different type of attacks.
3	MTA:Source Specific Multicast and Nextgen Media Distribution Technologies	Mark Ian Williams	Juniper	Source Specific Multicast and Nextgen Media Distribution Technologies [1/2 Day Tutorial]	Mark Ian Williams is currently responsible for Research and Education business development for Juniper Networks in Asia Pacific. In this role Mark works with leading academic organisations in development of new advanced network technology and applications, including IPv6, MPLS and multicast. Prior to this role Mark has held a number of senior technical positions, most recently with Nortel Networks based in Beijing. Mark is an active participants in conference and workshops, and a previous presenter at many such events	Half-day tutorial: Source Specific Multicast and Nextgen Media Distribution Technologies. Multicast Introduction (75 mins) - sparse mode and dense mode, RPF trees, etc. - multicast routing - PIM SM, DVMRP, MOSPF - IGMP v1, v2, v3, IGMP snooping, IGMP proxy, IGMP relay - Inter-AS multicast routing - MSDP and MBGP - Multicast and MPLS - Multicast and IPv6 PIM-SSM (10-20 mins) Multicast-Based Media Distribution (60-90 mins) - why distribution on metros does not work with broadcast trees - why ASM multicast techniques are problematic - The value of SSM techniques (security, increased channel space, simplifies inter-AS) - overview of available products and technologies.
4	MTF:Advance Routing & Traffic Control in Linux	Kishor Panth	Kathmandu College of Management	Advance Routing & Traffic Control in Linux [Full Day Tutorial]	I,Kishor Panth, after having studied Post Diploma In Computer Application from One of the reputed institute Government Polytechnic Panaji - Goa, India after my studies of MECHANICAL ENGINEERING from the same institute Government Polytechnic Panaji - Goa, India. I worked as "Trainee Programmer" at M/S. Phil Systems Ltd. Goa from 14th December 98 to 16th April 99. This company is into Export Oriented Software Development. I worked as "Senior Marketing Officer (Software & Peripheral)" at Infotech Solution Margao, Goa, India from 2nd June 99 to 29th June 2000. PRESENTLY: Presently working at Kathmandu College of Management. (www.kcm.edu.np).Cisco Systems Regional Academy in Nepal for CCNA. As System Administrator, Main Contact & Instructor for Cisco Networking Academy Program Main responsibilities are, conducting CCNA classes, administration of Windows NT, Win2k & Linux server. Maintenance, troubleshooting in Campus LAN, WAN. (Dedicated Point to Point Lease connection via Telco Copper from Local ISP to the Campus Building) And over all upgrading of the PC's and the different software used in the lab Working in npix (Nepal Internet Exchange)(www.npi	The Topic will cover the following titles 1. Introduction to iproute 2. Rules - routing policy database 3. GRE and other tunnels 4. Internet 5. Multicast routing 6. Queueing Disciplines for Bandwidth Management 7. Load sharing over multiple interfaces 8. Dynamic routing - OSPF and BGP
5	MTF;BGP Introduction and Deployment for Service	Philip Smith	Cisco	BGP Introduction and Deployment for Service Providers [Full Day Tutorial]	Philip Smith has been with Cisco Systems since 1998. He is part of the Internet Architectures Group under CTO Consulting Engineering. His role includes working with many ISPs in the Asia Pacific region, specifically in network design, configuration, scaling and training. Prior to joining Cisco, he spent five years at PIPEX (now part of UUNET's global ISP business), the UK's first commercial Internet Service Provider. He was one of the first engineers working in the commercial Internet in the UK, and played a key role in building the modern Internet in Europe.	This tutorial introduces service providers to BGP, including IBGP, eBGP and common attributes. It will then introduce some more advanced features of BGP, and look at the various scaling techniques available, when to use BGP instead of an IGP, and examine policy options available through the use of local preference, MED and communities. The second half of the tutorial will then cover multihoming techniques, providing example strategies for configuring multiple connections to neighbouring ISPs, and finishing with a case study using many of the techniques covered in the tutorial.
6	MTF;Creating & Managing CSIRTs	Mark Zajicek	Software Engineering Institute (SEI) at Carnegie Mellon University	Creating and Managing Computer Security Incident Response Teams (CSIRTs) [Full Day Tutorial]	Mark Zajicek is a member of the technical staff at the Software Engineering Institute (SEI) at Carnegie Mellon University (Pittsburgh PA, USA). Zajicek's current work is focused on helping other organizations to build their own computer security incident response teams (CSIRTs). As a member of the CERT® CSIRT Development Team , he is responsible for providing guidance to new and existing CSIRTs, worldwide. He has co-developed a variety of documents and training materials, and is an instructor for a suite of courses that provide training for CSIRT managers and technical staff. Previously, Zajicek was the Daily Operations team leader for the CERT Coordination Center (CERT/CC), after having joined the CERT/CC's incident handling staff in 1992. Prior to joining the CERT/CC, he was a user consultant for the Computing Facilities group at the SEI. Zajicek also helped support the CERT/CC during its initial start-up in 1988. Zajicek holds a Bachelor of Science in Electrical Engineering and Biomedical Engineering from Carnegie Mellon University.	A full-day tutorial devoted to issues and topics relevant to creating and managing an effective CSIRT. The tutorial will provide; - an introduction to the purpose and structure of CSIRTs; - insight into the type of work that CSIRT managers and staff may be expected to handle; - an overview of the incident handling process and the nature of incident response activities; - best practices in creating and managing a CSIRT. Intended Audience; This tutorial is designed to provide managers and other interested staff with an overview of the issues involved in creating and operating a CSIRT. Individuals who may be tasked with creating a CSIRT; - chief information officers (CIOs) - chief security officers (CSOs) - CSIRT managers - project leaders - project team members - system and network administrators - existing security staff - other upper management - human resources

NO	CODE	NAME	COMPANY	TITLE OF TUTORIAL	BIODATA OF SPEAKER	ABSTRACT OF TUTORIAL
7	MTF: IRR Tutorial	Miwa Fujii& Andy Linton	APNIC	MTF: IRR Training [Full Day Tutorial]	Miwa Fujii& Andy Linton	The APNIC Routing Registry is fully integrated in the existing APNIC Whois Database and it is available to all APNIC members. This tutorial provides opportunities for participants to learn features of Routing Registry, basics of Routing Policy Specification Language (RPSL), how to express routing policies using RPSL and how to extract routing policies from the APNIC Routing Registry using RtConfig tool. There will be some hands on demonstration on the use of RtConfig. Topics covered are: - APNIC database recap - What is IRR o Why use an IRR? o APNIC database and the IRR o Using the Routing Registry o Benefit of using IRR - RPSL o RR objects review o Using RPSL in practice o IRR queries o Address prefix operator o AS-path regular expressions o Action specification o Syntax of policy actions and filters - RtConfig o IRRToolSet options o RtConfig command o Case studies o Using RtConfig command - The rest of the IRRToolSet This tutorial is aimed at people who are already familiar with the APNIC Whois Database and want to learn more about the APNIC Routing Registry. A basic understanding of BGP routing and the APNIC Whois Database is assumed.
8	MTF:Internet Bandwidth Management & Web Caching wi	Gihan Dias	ICT Agency	Internet Bandwidth Management and Web Caching with SQUID [Full Day Tutorial]	Dr. Dias graduated from the University of Moratuwa in Electronics and Telecom. Engineering 1985 and was awarded a doctorate in Electrical Engineering and Computer Science from the University of California in 1992. Since 1992, he has been a Senior Lecturer in the Dept. of Computer Science and Engineering, University of Moratuwa, and served as the Head of the Dept. from 1997 to 1999. He was instrumental in setting up and maintaining the academic Internet in Sri Lanka (LEARN), and was its Technical Manager till 2003. He is Currently the Programme Director, IT Human Resource Development of the Information and Communication Technology Agency of Sri Lanka. He has assisted a number of Internet service providers in setting up their networks, and was a consultant for several universities, government, and private sector organisations in the areas of networking, software, information systems, and security. His research focus in the area of bandwidth-constrained networking, i.e., how to effectively use the Internet when bandwidth is at a premium	The high cost of Internet bandwidth, both international and national, continues to be a major constraint for users and service providers in this region. Optimising the use of the available bandwidth while providing a good service to users is a prime concern of network managers. Since much Internet traffic is due to web access, web caching is a widely used solution. However, other types of traffic, such as multimedia and voice, are also important. Network traffic can be categorised as real-time, on-line, and off-line, and this tutorial will show how to deal with each of these types of traffic to make the most of your Internet connections. We will also show how differentiated levels of service can be provided to different groups of users. We will introduce caching systems and the Squid cache in particular. Participants will learn how Squid can be configured to optimise performance. We will show how to use Squid as a bandwidth manager, and the setting up of a set of inter-connected caches.
9	MTF:Metro Ethernet: The First/Last Mile Technology	Lim Wong	Cisco	Metro Ethernet: The First/Last Mile Technology [Full Day Tutorial]	I have been in IT and telecom industry for 17 years. I spent the last 8 years with Cisco Systems serving as network consultant for the Enterprise and Service Provider field of operations. I have been engaged in many large enterprise and service provider metro network designs, and also assisted with numerous complex network deployments. Prior to Cisco, I worked for Hughes Aircraft Company for nine years and have held many positions within the company's IT organization. I was the chief architect for the company's multi-protocol router based network and had managed the network for over six years. While at Hughes, I gained extensive experience in designing large scalable enterprise network. I graduated from Loyola Marymount University with a Bachelor of Science in Electrical Engineering. I was awarded with a two-year fellowship from Hughes Aircraft Company to pursue higher education; I received my Master of Science in Computer Science from UCLA.	Metro Network, with Ethernet as the last mile access technology, can deliver a variety of broadband services to the home and businesses. This tutorial discusses the architectural options for delivering high quality video, voice, and Internet services to the home; and how VPN services can be offered with tight Service Level Agreement to the businesses. What Metro technology, security and Quality of Service mechanism are needed to offer these services? Topics to be covered • Metro architecture • SDH, xDSL, CWDM & DWDM overview • MPLS switching concept, EoMPLS, MPLS/VPN • Metro Services ☐ Broadband Internet Access ☐ L2 VPN ☐ L3 VPN ☐ Multicast Video • Metro Ethernet Network Security • QoS and SLA
10	MTF:Practical Deployment for MPLS-VPN Networks	Monique Morrow	Cisco	Practical Deployment Guidelines for MPLS-VPN Networks [Full Day Tutorial]	Monique Morrow is currently CTO Consulting Engineer at Cisco Systems, Inc. She has 20 years experience in IP internetworking that includes design, implementation of complex customer projects and service development for service providers. Monique has been involved in developing managed Network Services like Remote Access and LAN Switching in a Service Provider environment. Monique has worked for both enterprise and service provider companies in the United States and in Europe. Monique led the Engineering Project team for one of the first European MPLS-VPN deployments in 1999 for a European service provider. Monique has been a speaker in the following conferences: MPLS Congress-Paris, 2000; MPLSCon 2000, London; MPLS Japan, 2002; APRICOT, Taipei, Taiwan, 2003; MPLScon 2003; Supercomm 2003, and has spoken in several Cisco Networker Conferences.Monique is co-author of the book Designing IP-Based Services: Solutions for Vendors and Service Providers (Morgan-Kaufmann, 2002). Monique has been a technical reviewer for the book, International QoS Architectures and Mechanisms, Zheng Wang (Morgan-Kaufmann, 2001); she has contributed a chapter on MPLS in	This tutorial explores the practical aspects of planning and deploying an MPLS-VPN network. It is assumed that the participant possesses a basic knowledge of MPLS principles and operations. The tutorial will address planning and deployment of BGP-VPNs (intranet;extranet topologies); explore inter-Autonmous Systemens (Inter-AS) and Carrier Supporting Carriers (CsC) implementation guidelines and discuss MPLS-VPN security issues associated with such deployments. The instructors will further highlight CoS/QoS mechanisms in conjunction with Diff-Serv Traffic engineering; finally, the instructors will highlight MPLS OAM developments for operational consideration.
11	MTP: Developments in MPLS technology	Andrew Coward	Juniper	Developments in MPLS technology and deployments [1/2 Day Tutorial]	Andrew Coward serves as the Vice President of Technical Operations, Asia Pacific for Juniper Networks. He is responsible for pre-sales and engineering support services to customers in Asia Pacific. Prior to Juniper, Andrew co launched the Asia Pacific operation of Unisphere Networks in May 1999. He led a team of system engineers to provide dedicated pre-sales and architectural design services, and support engineering services to customers through out the region. Andrew has been living in Asia Pacific for the past seven years, working with service providers in the region on IP access technologies, first with Bay Networks and later with Nortel, where he designed and planned some of the largest IP networks in Asia Pacific. Andrew started his career in government as an IP network engineer and progressed to role of Network Manager responsible for a 70-site United Kingdom wide network. Later, with Xylogics Ltd, he was responsible for delivery of the first dial internet access networks in North Asia. Andrew is currently based in Tokyo.	MPLS Tutorial - 1 day Developments in MPLS technology and deployments This workshop is designed to provide a background, history, update and insight into the important developments with MPLS related protocols. Topics covered include a technologies, implementations and case studies for the following: MPLS L2 & L3 VPNs MPLS Traffic Engineering GMPLS ATM & TDM migration Models for Carrier Interconnect, peering and billing This session is suitable for attendees interested in the actual implementation of MPLS services and how each service can be layered into
12	MTP:Network Security Steps to Secure Carrier	Wayne Chan	Juniper	Network Security - Essential steps to secure carrier scale networks [1/2 Day Tutorial]	Wayne Chan has more than six years experience in the networking and information technology. In his role as product manager in Asia Pacific for Juniper Networks, he is responsible for the industry-leading M and T-series routing platforms. He also has hands-on skill in JUNOS operating system, and experience in network design	Explain and discuss the essential steps to secure the network infrastructure from various attacks with the underlying architecture and applications of a routing device in a carrier scale network.
13	MTP:Packet Voice Backbone Network Design	Matthew Kolon	Juniper	Packet Voice Backbone Network Design [1/2 Day Tutorial]	Matt Kolon is a Senior Solutions Manager for Juniper Networks, focusing particularly on VoIP and high availability. Prior to coming to Juniper he was a Senior Member of Technical Staff for Hill Associates, a telecom training and consulting firm, and a consultant in private practice in New York City. He is a regular speaker at networking conferences and trade shows, including APRICOT, NANOG, CENIC, and SuperComm. Matt is an author of two books, "IP Telephony (McGraw-Hill, 1999) and "Juniper Networks Routers: The Complete Reference" (McGraw-Hill, 2002), and has published a number of technical and non-technical articles in industry journals and elsewhere.	It's a half day tutorial on BFD is a new multivendor draft protocol that allows for the detection of forwarding path failures in extremely short times, and thereby improves enormously the convergence characteristics of standard IP routing protocols like ISIS and OSPF. BFD allows routing protocols to detect failures and begin repairs must faster than the hello timers historically used by these protocols, but doesn't demand any changes to the protocols themselves. This presentation will introduce the concepts behind, operation of, and uses for the BFD protocol.