|  |  |  |
| --- | --- | --- |
|  | **ITU ASP CoE Program on****IPv6 Infrastructure Security** 22-26 June, 2015 Bangkok, Thailand | **mict_logo** |

**Supported by**

** **

**Draft Agenda**

|  |
| --- |
| **22 June (Day-1)****IPv6 Infrastructure Security Workshop for Telecom Service Providers** |
| 0830-0900 | **REGISTRATION** |
| 0900-0930 | **Opening Session:** Welcome Address1. ITU
2. APNIC
3. MICT, Thailand
 |
| 0930 - 1000 | **Session 1: Where are we now: IPv6 deployment update** Objective: To provide an overview of IPv6, the need for migration and the current IPv6 deployment status in the world, and technical trend.  |
| 1000 - 1030 | **Session 2:  Recap – Internet fundamentals** Objective: To recap fundamental technical information on the Internet by focusing on mechanism of IP peering |
| 1030-11:00 | **COFFEE BREAK** |
| 1100-1230 | **Session 3: Recap – IPv6 Protocol**Objective: To recap fundamental technical information about IPv6, introducing the protocol and the relevant standards. |
| 1230-1400 | **LUNCH BREAK** |
| 1400-1530 | **Session 4: Hands-on lab on IPv4 and IPv6 Dual Stack network**Objective: Constructing IPv4 and IPv6 dual stack router based network infrastructure which will be used for other hands-on workshops to practice implementation of the Internet infrastructure security measures. |
| 1530-1600 | **COFFEE BREAK** |
| 1600-1700 | **Session 5: Roles of Policy maker and regulator in IPv6 migration**Objective: To develop an understanding of what role the policy maker and regulator should play to promote IPv6 migration, including any policy and regulatory incentives.  |
| 1700-1730 | **Recap:** To summarise the topics learned during the first day, and have a quick quiz to introduce participants to the exam questions during the workshop. |

|  |
| --- |
| **23 June (Day-2)** |
| **IPv6 Infrastructure Security Workshop: Building IPv6 Infrastructure Network Security I** |
| 0900-1030 | **Session 6: Recap - About IPv6 Addresses**Objective: To explain IPv6 addressing, how it works, the differences from IPv4, and introduce how a well designed address plan can assist with network security and integrity planning. |
| 1030-1100 | **COFFEE BREAK** |
| 1100-1230 | **Session 7: IPv6 Security Introduction**Objective: Introduction to the main similarities and differences between IPv4 and IPv6 when it comes to network infrastructure security. Presentation also introduces the main network security issues which operators of any infrastructure needs to be aware of. This includes discussion about ICMPv6, multicast, extension headers, fragmentation headers, and reconnaissance on IPv6 networks. |
| 1230-1400 | **LUNCH BREAK** |
| 1400-1530 | **Session 8: Hands-on lab on IPv4 and IPv6 Dual Stack network (cont’d)**Objective: Constructing IPv4 and IPv6 dual stack network which will be used for other hands-on workshops to practice implementation of the Internet infrastructure security measures. |
| 1530-1600 | **COFFEE BREAK** |
| 1600 –1700 | **Session 9:** **Exercise on IPv6 addressing design to enhance network security** Objective: To learn how to construct a scalable address plan in IPv6. With a new protocol and vast address space, constructing a scalable and usable address plan is a very important component of enhancing the security of an IPv6 network infrastructure. |
| 1700-1730 | **Examination 1** |

|  |
| --- |
| **24 June (Day-3)** |
| **IPv6 Infrastructure Security Workshop: Building IPv6 Infrastructure Network Security II** |
| 0900-1030 | **Session 10:** **Hardening IPv6 network devices**Objective: To review issues that face network devices and the threats that target the network infrastructure, and to learn services that you should disable on a router to avoid vulnerabilities. Topics such as disabling unnecessary services, IPv6 device management, threats against interior routing protocol, Access Control Lists (ACLs) Best Current Practice (BCP) and Quality of Service (QoS) threats will be included. |
| 1030-1100 | **COFFEE BREAK** |
| 1100-1230 | **Session 11: IPv6 Transition Technologies**Objective: To recap the currently deployed IPv6 transition technologies, analyzing their advantages and disadvantages.**Session 12: Securing the transition mechanisms**Objective: To look at each transition technology presented during the previous session and discuss about securing them, their advantages and disadvantages as far as security is concerned, and look at general security implications during transition to IPv6. |
| 1230-1400 | **LUNCH BREAK** |
| 1400-1530 | **Session 13: Hands-on lab on IPv6 infrastructure security** Objective: To learn look at infrastructure device security and access. Participants are divided into 14 small teams and each team will configure one router.Participants will be requested to implement infrastructure security coding into their routers. Keep logs of their operations into a presentation file to present it at the end of the workshop to be examined by instructors. |
| 1530-1600 | **COFFEE BREAK** |
| 1600 - 1700 | **Session 14: Hands-on lab on IPv6 infrastructure security (cont)** Objective: Continuing the lab work, now looking at IPv6 Traffic Filtering. |
| 1700-1730 | **Examination 2** |

|  |
| --- |
| **25 June (Day-4)** |
| Applying knowledge to develop a plan for implementing IPv6 security  |
| 0900-1030 | **Session 15: IPsec and SSL virtual private networks**Objective: To review encryption technologies such as IPsec and Secure Socket Layer (SSL) that can be used to protect Virtual Private Networks (VPN). Host to Host IPsec communication and Site to Site IPsec VPN will be reviewed along with multipoint IPsec VPN examples. |
| 1030-1100 | **COFFEE BREAK** |
| 1100-1230 | **Session 16: Security monitoring**Objective: To review tools and techniques to monitor IPv6 networks. To learn monitoring of tunnels and performing forensics of possible IPv6 security events through reviewing configuration and testing of IPv6 intrusion prevention systems.  |
| 1230-1400 | **LUNCH BREAK** |
| 1400-1530 | **Session 17: Hands-on lab on IPv6 infrastructure security**Objective: Continuing the lab work, now looking at Routing Protocol security.Participants will be requested to implement infrastructure security coding into their routers. Keep logs of their operations into a presentation file to present it at the end of the workshop to be examined by instructors. |
| 15:30 – 16:00 | **COFFEE BREAK** |
| 1600-1700 | **Session 18: Hands-on lab on IPv6 infrastructure security**Objective: Continuing the lab work, now looking at IPv6 NetFlow. |
| 1700-1730 | **Examination 3** |

|  |
| --- |
| **26 June (Day-5)** |
| Applying knowledge to develop a plan for implementing IPv6 security  |
| 0900-1030 | **Session 19: Hands-on lab on IPv6 infrastructure security**Objective: Continuing the lab work, now other Security Monitoring Tools and IPv6 Network Management.Participants will be requested to implement infrastructure security coding into their routers. Keep logs of their operations into a presentation file to present it at the end of the workshop to be examined by instructors. |
| 1030-1100 | **COFFEE BREAK** |
| 1100-1230 | **Session 20: Working Group exercise** Objective: To summarize learning of the workshop capturing important element of learning that can be used to inform your colleagues who could not participate in this workshop. Participants will present their choices of router configurations that they applied to mitigate security vulnerabilities and logic behind of such implementation. Each team will be asked to present it in a 10 minute presentation. |
| 1230-1400 | **LUNCH BREAK** |
| 1400-1530 | **Session 21: Presentation by participants + evaluation** Objective: To present the learning in front of other participants and instructors. There will be a short QA session at the end of your presentation. |
| 15:30 – 16:00 | **COFFEE BREAK** |
| 1530-1600 | **Summary and closing** |

Target audience: Engineering professionals dealing with deployment of IPv6 in their networks and / or IP network’s security issues.