PACNOG

DRAFT AGENDA
Internet and IPv6 Infrastructure Security
4-8 December 2017, Nuku'alofa, Tonga

FINAL AGENDA

4 Dec 2017 (Day-1)

0800-0900	**REGISTRATION**
0900-1230	PacNOG 21 Conference Plenary Facilitators to present an update to PacNOG conference (TBA).
1230-1400	**LUNCH BREAK**
1400-1430	Opening Session: Welcome Address Group Photograph
1430-1530	Session 1: Where we are 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.
1530-1600	**COFFEE BREAK**
1600-1700	Session 2: Recap – Internet fundamentals Objective: To recap fundamental technical information on the Internet Infrastructure
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.

5 Dec 2017 (Day-2)

0900-1030	Session 3: Recap – IPv6 Protocol Objective: To recap fundamental technical information about IPv6, introduction to the protocol and the relevant standards.
1030-1100	**COFFEE BREAK**

1100-1230	Session 4: 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.
1230-1400	LUNCH BREAK
1400-1530	Session 5: Hands on Lab Work: Deploying 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 lab work to practice implementation of the Internet infrastructure security measures.
1530-1600	COFFEE BREAK
1600-1700	Session 6: Roles of ICT Policy maker and regulator in Internet and IPv6 Security Objective: To develop an understanding of what role the ICT policy maker and regulator should play to promote Internet security in general and IPv6 infrastructure security in particular.
1700-1730	Quiz
6 Dec 2017 (Day-3)	
0900-1030	Session 7: Internet Infrastructure Security Introduction Objective: Introduction to the main network security issues that infrastructure operators of any infrastructure need to be aware of. This includes discussion on confidentiality, integrity, AAA, vulnerabilities, packet flooding, Internet worms, DDOS attacks and Botnets
1030-1100	COFFEE BREAK
1100-1230	Session 8: IPv6 Security Introduction Objective: Introduction to the similarities and differences between IPv4 and IPv6 when it comes to network infrastructure security. This includes discussion about ICMPv6, multicast, extension headers, fragmentation headers, and reconnaissance on IPv6 networks.
1230-1400	LUNCH BREAK
1400-1530	Session 9: Hands on Lab Work: 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, Secure Shell (SSH), threats against interior routing protocol, Access Control Lists (ACLs) Best Current Practice (BCP) and Quality of Service (QoS) threats will be included.
1530-1600	COFFEE BREAK
1600-1700	Session 10: IPv6 Transition Technologies Objective: To recap the currently deployed IPv6 transition technologies, analysing their advantages and disadvantages.

1700-1730	Quiz
7 Dec 2017 (Day-4)	
0900-1030	Session 11: Securing the IPv6 Transition Mechanisms Objective: To look at each transition technology presented during the previous session and discuss techniques around securing them, their advantages and disadvantages as far as security is concerned, and the security implications while transiting to IPv6.
1030-1100	COFFEE BREAK
1100-1230	Session 12: Hands on Lab Work: IPv6 Internet Routing Security Objective: Introduction to how to protect IPv6 networks. This includes some theoretical explanation on Ingress and Egress filtering, route origination and RPKI, followed by a demonstration of filtering IPv6 traffic, filtering on allocated addressing and bogon addresses.
1230-1400	LUNCH BREAK
1400-1445	Session 13: IPv6 Security Monitoring IPv6 network security.
1445-1530	Session 14: IPv6 Firewalls Objective: To review Firewalls, and how to filter unallocated IPv6 address space, handle IPv6 headers, blocking ports and services, etc.
1530-1600	COFFEE BREAK
1600-1700	Session 15: Hands on Lab Work: Securing OSPF & BGP Routing Protocols Objective: Introduction to securing OSPF and BGP Routing Protocols, including neighbour authentication, bogon filtering, route origination.
1700-1730	Quiz
8 Dec 2017 (Day-5)	
0900-1030	Session 16: IPv6 on Mobile Networks: The Technology Objective: To look at how IPv6 is deployed on Mobile (3G and 4G) networks globally, the change to the infrastructure, and the benefits for the end-user.
1030-1100	COFFEE BREAK
1100-1230	Session 17: 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 18: 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.
1530-1600	COFFEE BREAK
1600-1700	Session 19: 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 presentation.
1700-1730	Summary and closing