ISP and NSP Security Workshop

APRICOT 2013

Welcome!

- Welcome to the 2013 Network Security workshop!
- Five days of hands-on learning!
- Material was developed over many years, from many people, from many experiences
- Help network operators understand security architecture and operations

Introductions

- Your instructors:
  - Alastair JOHNSON (alastair.johnson@alcatel-lucent.com)
    - Senior Product Line Manager, Service Routing Business Unit, Core Networks Division, Alcatel-Lucent USA
  - Daniel GRIGGS (daniel@pch.net)
    - Senior OpsDev, Packet Clearing House, New Zealand
  - Ram KRISHNA (ramkrishna@subisu.net.np)
    - Senior Network Engineer – L3 R&D Subisu Cablenet, Nepal

Introductions

- Yourselves!
  - What's your name?
  - Where are you from?
  - Where do you work? What do you do there?
  - What's your ASN?
  - What's your background and skill-level?
  - What do you want to get out of this workshop?

Free Use

- This slide deck can be used by any operator to help empower their teams, teach their staff, or work with their customers.
- It is part of the next generation of **APRICOT Security Curriculum ....** providing tools that can improve the quality of the Internet.
- Materials will be available after the workshop

Goal

- Provide security core techniques/task that any SP can do to improve their resistance to security issues.
- These core techniques can be done on any core routing vendor's equipment.
- Each of these techniques have proven to make a difference.

Credits

In no particular order…

- Barry Raveendran Green
- Merike Kaeo
- Damien Holloway
- Jonny Martin
- Peter Losher
- Gaurab Raj Upadhaya
- Mark Tinka
- Philip Smith
- Michael Jager
- Yusuf Bhaiji

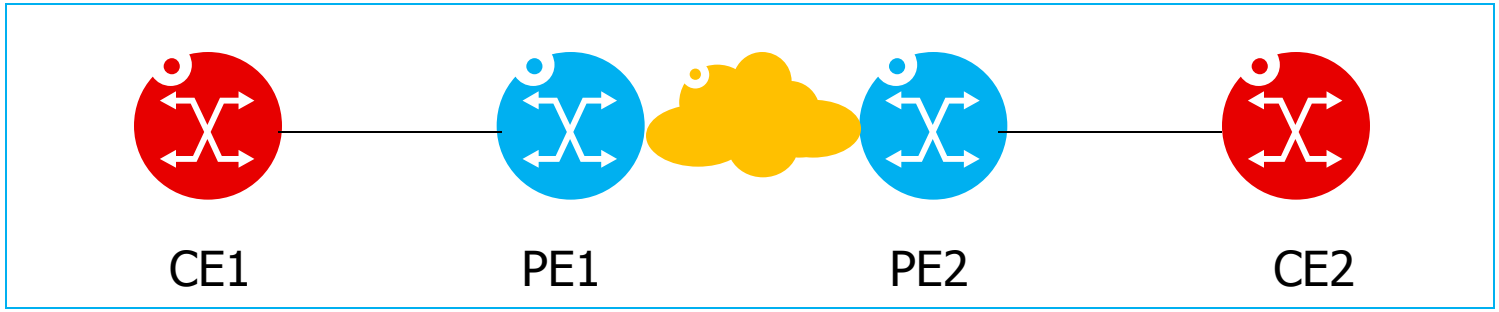
… and many others…

Class Structure

- Theoretical
  - Lecture driven by instructors
- Practical
  - Hands-on in the lab
  - By yourselves in a group of four
    - You need to be seated in the same place each day
  - Instructors will support you in the lab
- Relaxed, informal environment
  - Please share experiences and ask questions!

Class Structure

- 8 pods
- 4 routers per pod
- 4 participants per pod
- Addressing and access details will be shared this afternoon
- Virtualized environment, reconfigurable – more on that later



Agenda

- Day 1/2:
  - Securing the Infrastructure
- Day 3:
  - Gain visibility
- Day 4:
  - MPLS / L3VPN Security
- Day 5:
  - Managed security services
  - L2 security
- Conclusions

Housekeeping

- WiFi password: apricot2013
- Class hours
  - 9am to 5pm, Tuesday through Saturday
- Break times in the mezzanine area
  - Morning tea: 10:30-11:00
  - Lunch: 12:30-13:30
  - Afternoon tea: 15:00-15:30
- Health and Safety

Housekeeping

- There will be a daily quiz
- Regular pop quizzes!
- Test at the end of the workshop
- Keep listening and thinking!
- No matter how small something may seem
  - ***It will come up!***

Tuesday agenda

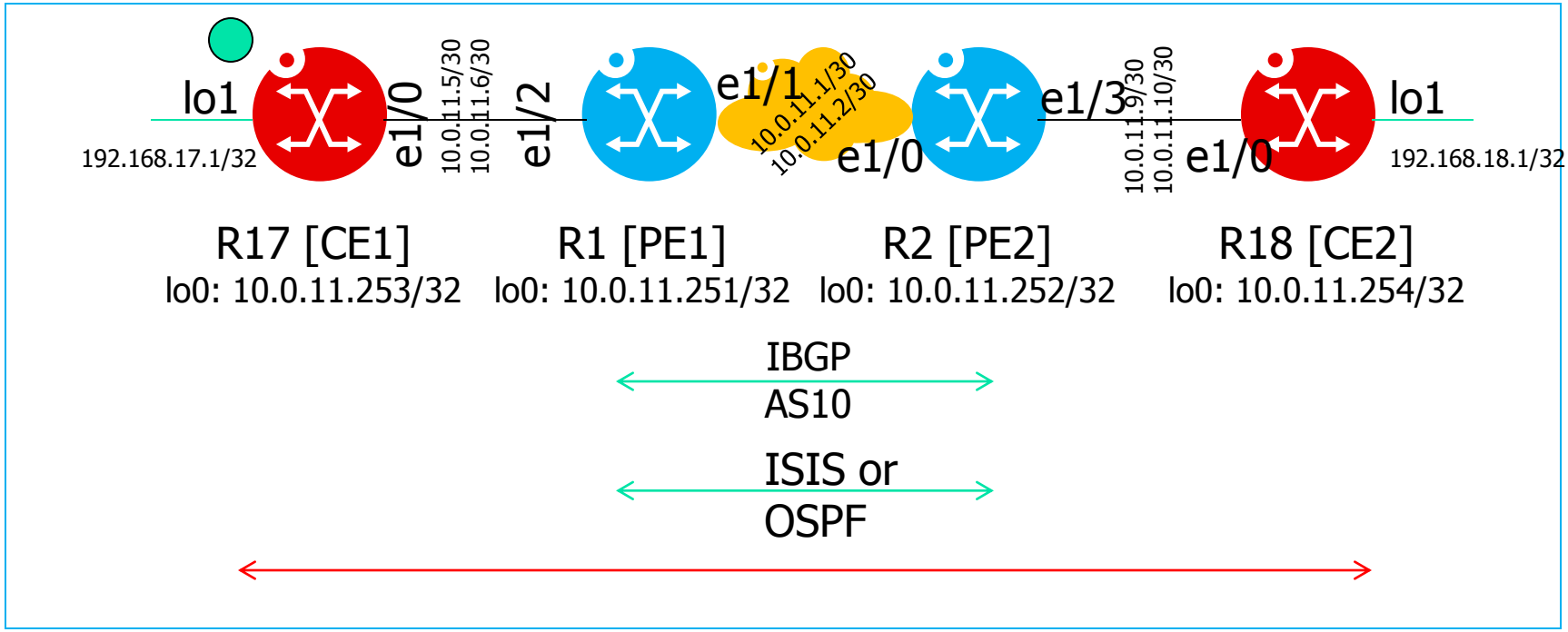
09:00	**Open**
09:00-9:30	Introduction
09:30-10:30	Core security
10:30-11:00	*Break*
11:00-12:30	Infrastructure security
13:00-14:00	*Lunch*
14:00-15:30	Lab introduction
15:30-16:00	*Break*
16:00-17:00	Lab
17:00	**Close**

RECAP AND WRAPUP

Day 1 Wrap-up

- Network security history
- Network security theory
  - Infrastructure security
  - Physical security
  - Logical security
  - "Social security"
- Cisco command introduction
- Lab introduction
  - *Save your configs!*

We built a lab!



A look at security incidents

- Operation Aurora
  - http://en.wikipedia.org/wiki/Operation_Aurora
- Facebook
  - Firedrill: http://arstechnica.com/security/2013/02/at-facebook-zero-day-exploits-backdoor-code-bring-war-games-drill-to-life/
  - Facebook computers compromised by zero-day exploit: http://arstechnica.com/security/2013/02/facebook-computers-compromised-by-zero-day-java-exploit/
- Arbor Networks Worldwide Infrastructure Security Report
  - http://www.arbornetworks.com/research/infrastructure-security-report
  - www.nanog.org/meetings/nanog57/presentations/Tuesday/tues.general.sockrider.2012_infra_sec_report.1.pdf

Quiz

1. Why is social networking important for network security?
2. What platform are we using in the lab?
3. When should you use telnet?
4. What other protocols might you use to manage a router?
5. Where does PCH mean?
6. What is a worm?
7. How long would a router with no password last on the Internet?
8. What does '`no ip domain-lookup`' do?
9. How many phases of incident response are there?
10. What are some ways to identify a security incident in process?
11. Why does iBGP use loopback addresses?
12. What does '`aaa security new-model`' do? Why would it be a good idea?
13. Does Daniel take sugar in his coffee?

Wednesday agenda

- Recap
- Edge protection
- Packet filtering
- Securing Routing infrastructure
- Remote Triggered Blackhole (RTBH)
- Sinkholes
- Source Address Validation