ISP and NSP Security Workshop

APRICOT 2013

Day 4

PCH Packet Clearing House

Alcatel·Lucent

SUBISU

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: 13:00-14:00
  - Afternoon tea: 15:30-16:00
- Health and Safety

Housekeeping

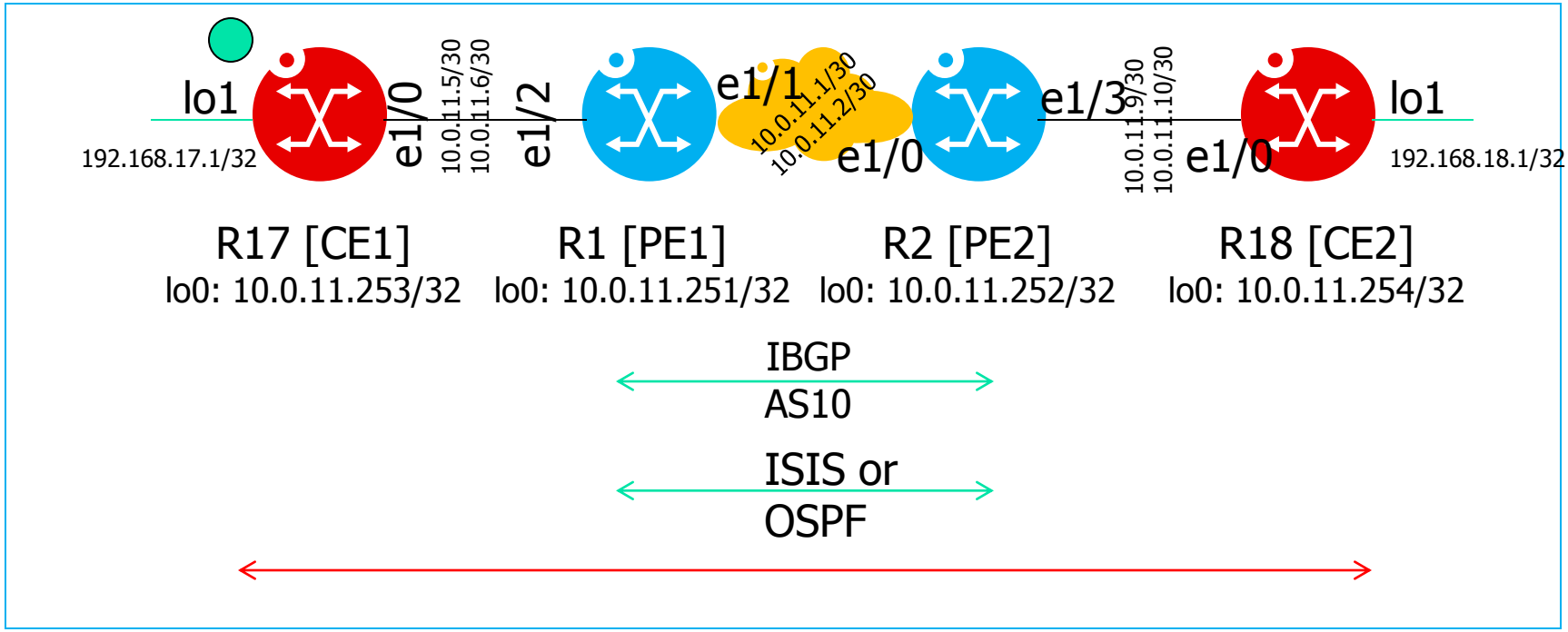
- There will be a daily quiz
- Regular pop quizzes!
- Test at the end of the workshop
- Keep listening and thinking!
- No matter how small something may seem
  - ***It will come up!***

Tuesday agenda

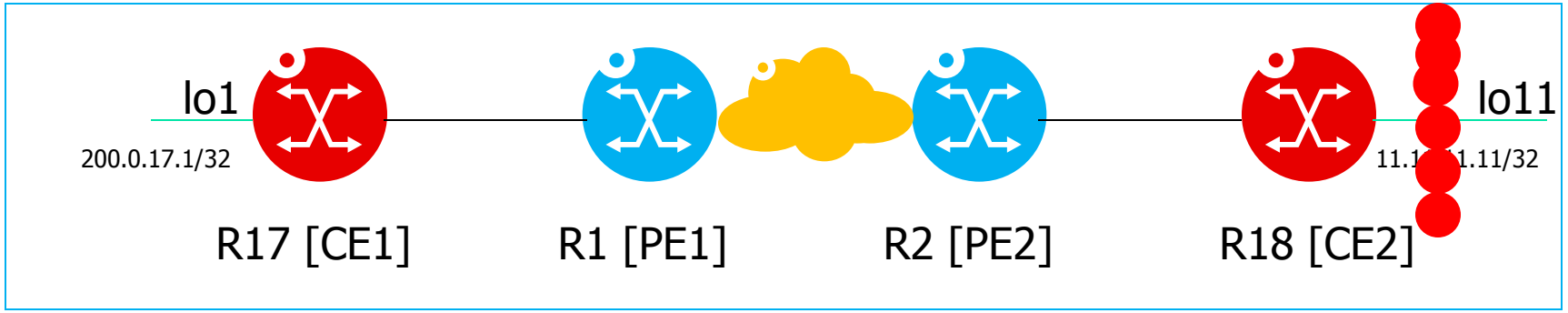
- **09:00** **Open**
- 09:00-9:05 Introduction/Recap
- 09:05-10:30 S/RTBH lab close
- *10:30-11:00* *Break*
- 11:00-12:30 MPLS configuration
- *13:00-14:00* *Lunch*
- 14:00-15:30 MPLS security
- *15:30-16:00* *Break*
- 16:00-17:00 MPLS (IPSec – if time)
- **17:00** **Close**

RECAP

We built a lab!



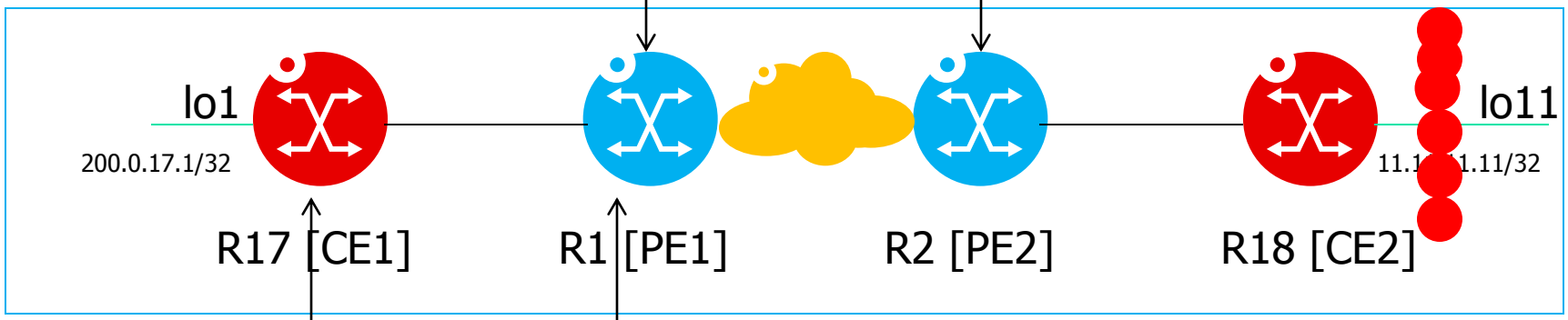
Where is S/RTBH useful?



- Host or hosts under attack in our network
- From a source, or few sources
  - Block the source, not the destination!

Where is S/RTBH useful?

1. PE routers in the network already configured for S/RTBH support
Trigger community 666:666



3. Advertised prefix has next-hop modified to 192.0.2.2 by PE router

4. 192.0.2.2 is always configured to be a null0 route
uRPF check will fail for 11.11.11.11 and traffic will drop
This is because 11.11.11.11 / null0 is an invalid source

2. Advertise S/RTBH *source* prefix to ISP network to start filtering it 11.11.11.11/32 community 666:666

Quiz and checkpoint

We've discussed a lot of techniques so far this week. What are these used for?

1. Security action plan (P-I-C-T-R-P)
2. Infrastructure ACLs
3. Management (or application) ACLs
4. Routing protocol security
    1. Prefix-lists
    2. AS-Path lists
    3. Authentication
5. RTBH
6. S/RTBH
7. Telemetry
    1. Netflow
    2. Syslog
    3. TACACS+
    4. SNMP

How comfortable do we feel about deploying these in our networks now?