

## The Bug Hunt

Jemand hat an ihrem System gefuscht! Hacker, Updates oder Kollegen hinterlassen Systeme manchmal nicht in dem Zustand, den Sie zuvor eingerichtet haben. Fehler strategisch aufzuspüren und zu beheben ist nun eine nützliche Kompetenz. In dieser Aufgabe bekommen Sie ein bereits konfiguriertes AS im Mini Internet.

### Aufgabe

Ihr Netz aus Aufgabe 2 hat sich verändert. Neben diversen validen Änderungen wurden auch Fehler eingebaut! Überprüfen Sie die Konfiguration sorgfältig, um zu lernen, wie Ihr Netz nun aufgebaut ist. Loggen Sie sich dazu auch in Ihr Netz ein und testen Sie Ihre Erwartungen. Ihre Aufgabe ist es,

1. die Fehlerzustände zu erkennen und einzugrenzen,
2. die Fehlerursachen herauszufinden,
3. die Fehlfunktionen und das Verhalten zu korrigieren.

In Ihrem Netz sollte folgendes konfiguriert sein:

- Die Host innerhalb des L2 East (L2E) können sich untereinander erreichen.
- Die Admin(A) und Student(S) Hosts sind über VLANs auf Layer 2 isoliert.
- Pakete werden über OSPF geroutet (zwischen den Hosts an den Routern sowie den Hosts in den layer 2 Netzwerken).
- Alle Hosts ( $\langle \text{asn}.100 + \langle \text{router} \rangle .0.1$ ) an den Routern können sich gegenseitig erreichen.

Testen Sie das Verhalten ihres Systems systematisch. Nutzen sie die bekannten Tools. Gegebenenfalls kann ein direkter Blick auf Pakete helfen.

#### Tools

ping, traceroute, tcpdump

### Abgabe

Beschreiben Sie in Ihrem Protokoll bitte Ihr Vorgehen beim Testen. Welche Fehler haben Sie wie gefunden? Was sind die Ursachen für diese Fehler, und wie haben Sie die Fehler behoben? Dokumentieren Sie schließlich, dass Ihr Netz den obigen Anforderungen genügt.

Nehmen wir an, Sie müssten ein Netz dieser Größe (und darüber hinaus) auf Dauer betreiben. Wie würden Sie ihre Strategie bei der Fehlersuche anpassen?