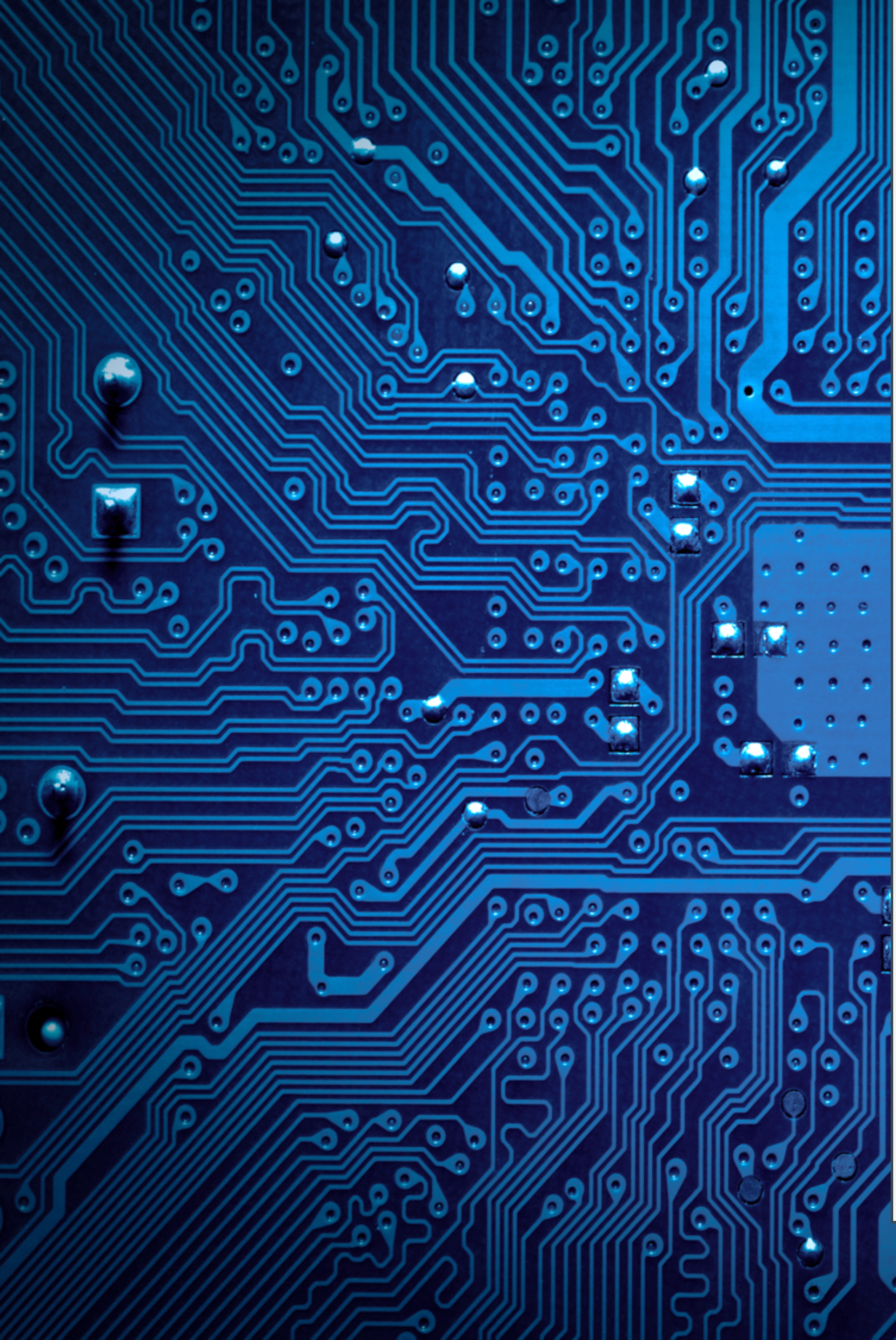
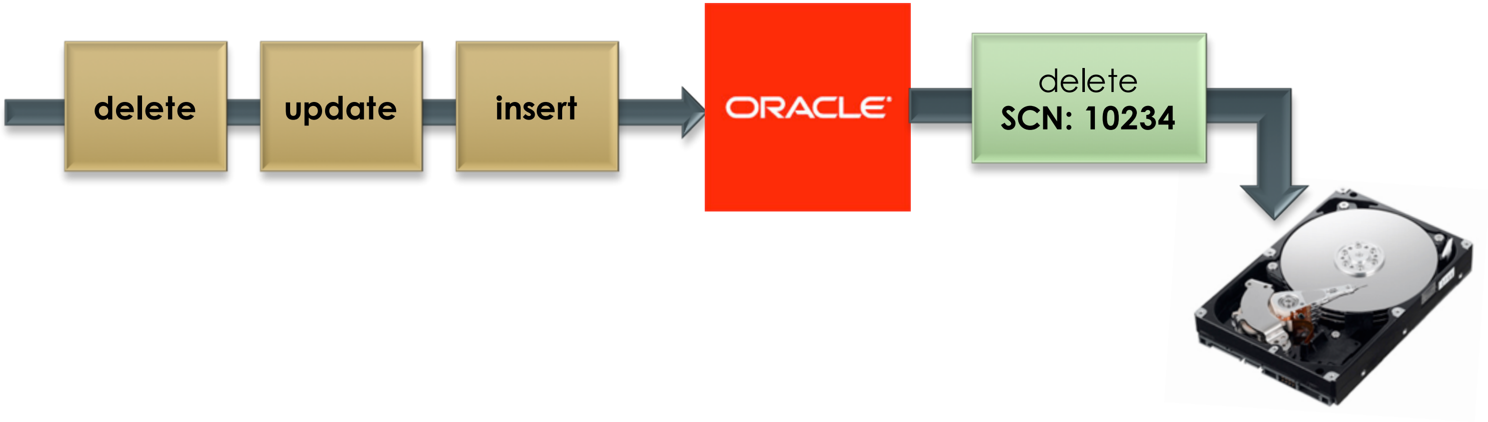


Case Study on Trust: **Oracle SCN**

ECE568 – Lecture 3.1
Courtney Gibson, P.Eng.
University of Toronto ECE

Oracle Databases

- Oracle databases keep track of actions on the database by assigning them each a unique **System Change Number (SCN)**
  - Used for recovery, synchronization and audit purposes
  - Database's "clock": must always increase



delete

update

insert

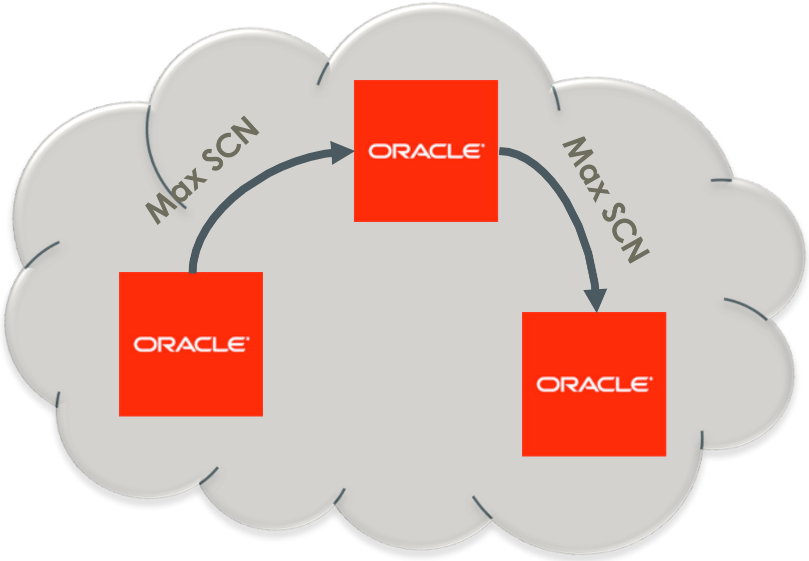
ORACLE

delete
SCN: 10234

SCN Synchronization

Clustered databases maintain consistency by synchronizing to a common SCN

- Requires every database to keep jumping to the highest SCN held by any member of the pool



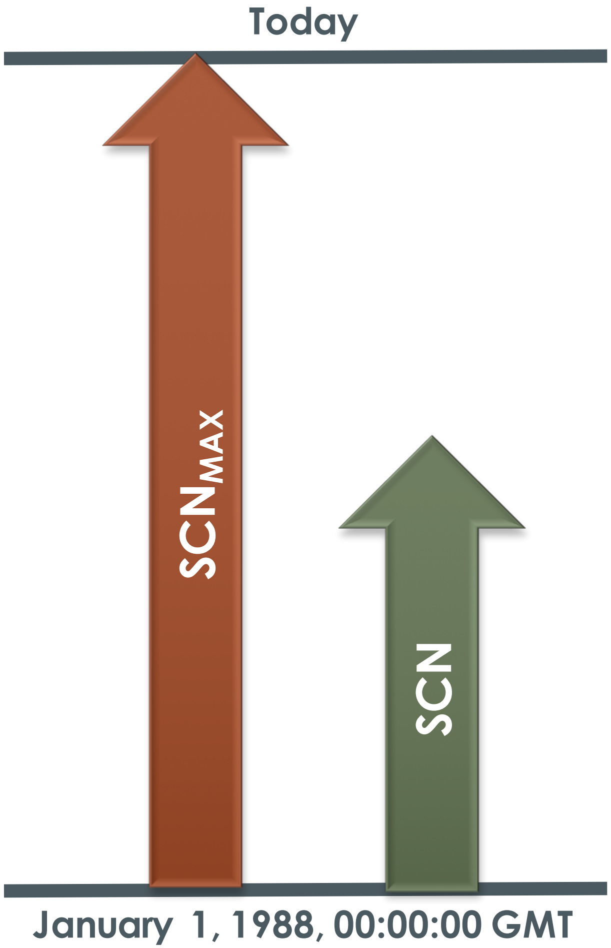
SCN: Implicit Trust

- There is a significant level of implicit trust: accepting SCN from any other database who contacts you
- Significant SCN-related security flaw, potentially enabling attackers to disable every database in a corporation's network, was recently disclosed (Jan 17, 2012)

SCN: Soft Limit

Need a way of determining if a database instance is malfunctioning

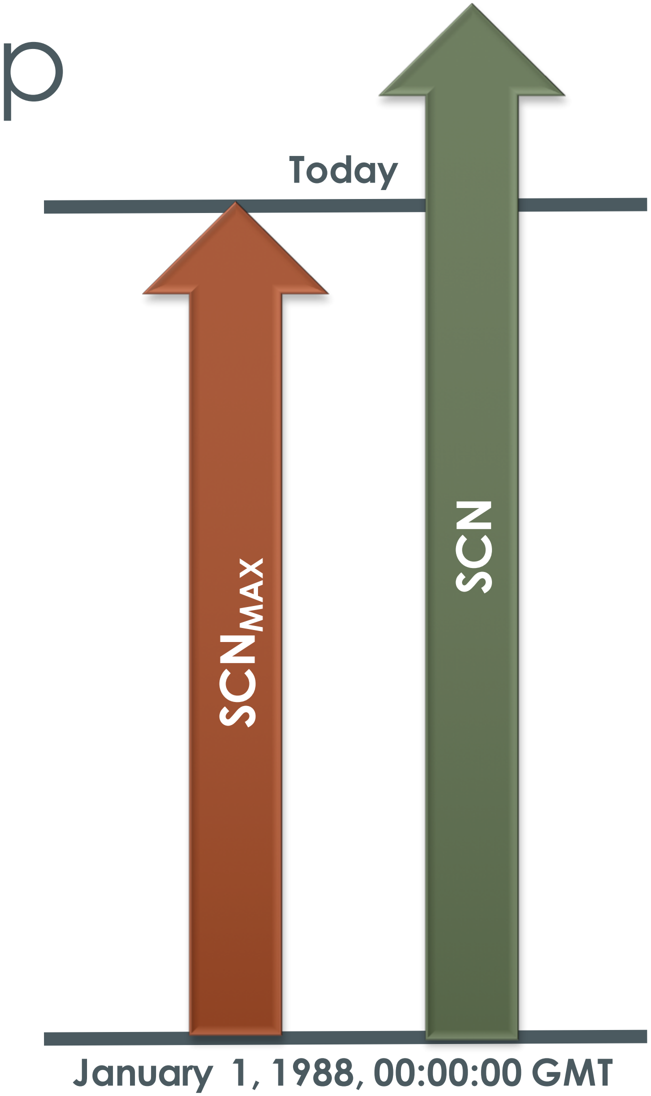
- Oracle defines a limit, **SCN$_{\text{MAX}}$** that grows over time
- Database instances refuse to run if their SCN exceeds this value



Bug: Live Backup

A critical bug surfaced recently: enabling “live backups” on the database causes the SCN to start making repeated large jumps

- Behaviour continues even after “live backups” turned off
- Eventually the SCN will exceed SCN_{MAX}



Impact

Because of clustering, one database instance with a run-away SCN could potentially take down all of a businesses' databases

- One poorly-secured database could create an opportunity for an attacker

Solutions aren't good:

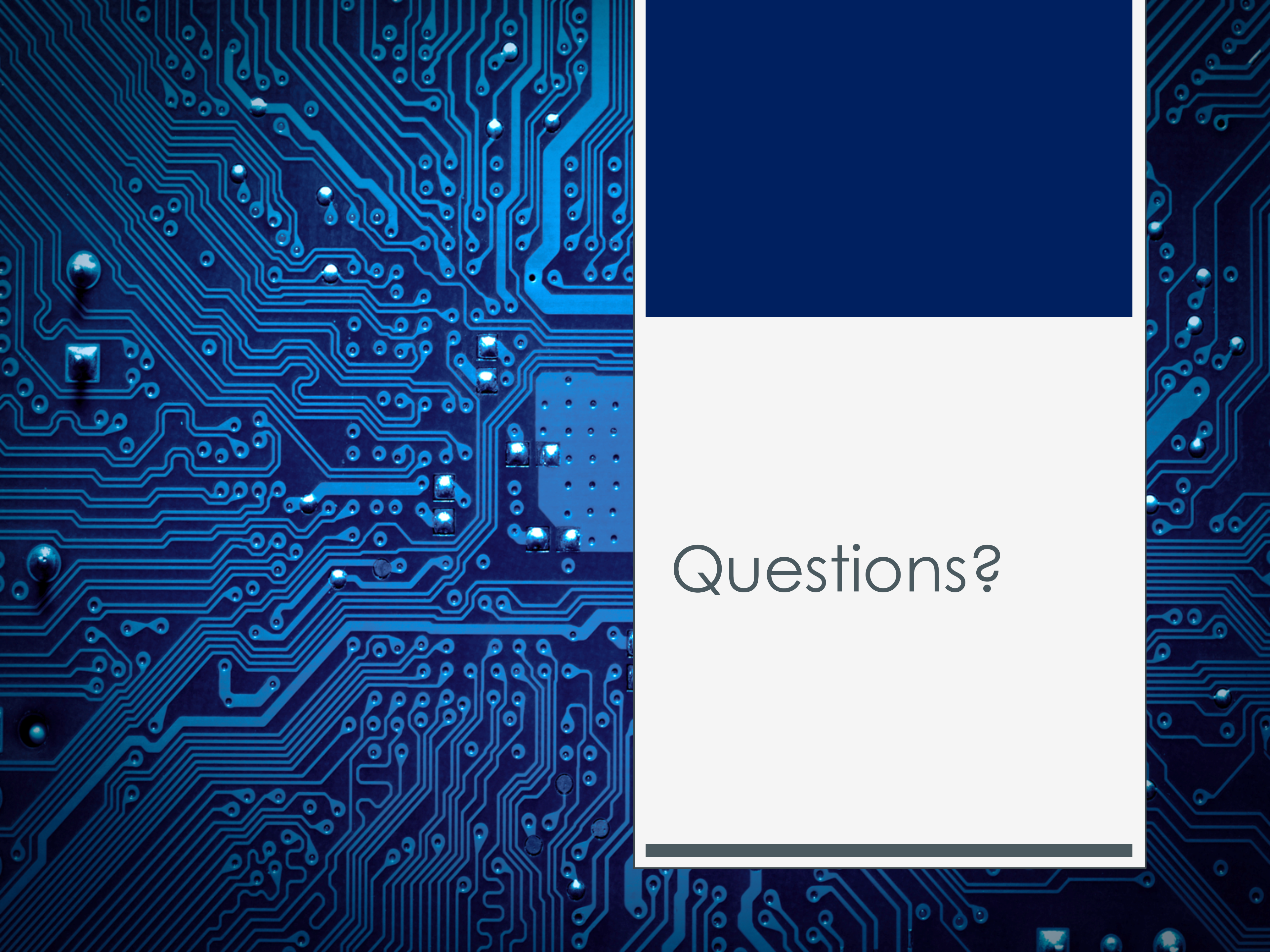
- Shut down **every** database instance and wait for $\mathrm{SCN}_{\mathrm{MAX}}$ to increase
- Dump and rebuild **every** database from scratch, so that SCNs all get reset to 1

Further Reading

For more information:

"Fundamental Oracle Flaw Revealed"
Paul Venezia, InfoWorld, January 17, 2012

http://www.infoworld.com/d/security/fundamental-oracle-flaw-revealed-184163-0



Questions?