Static Network Verification

Lecture 22, Computer Networks (198:552)

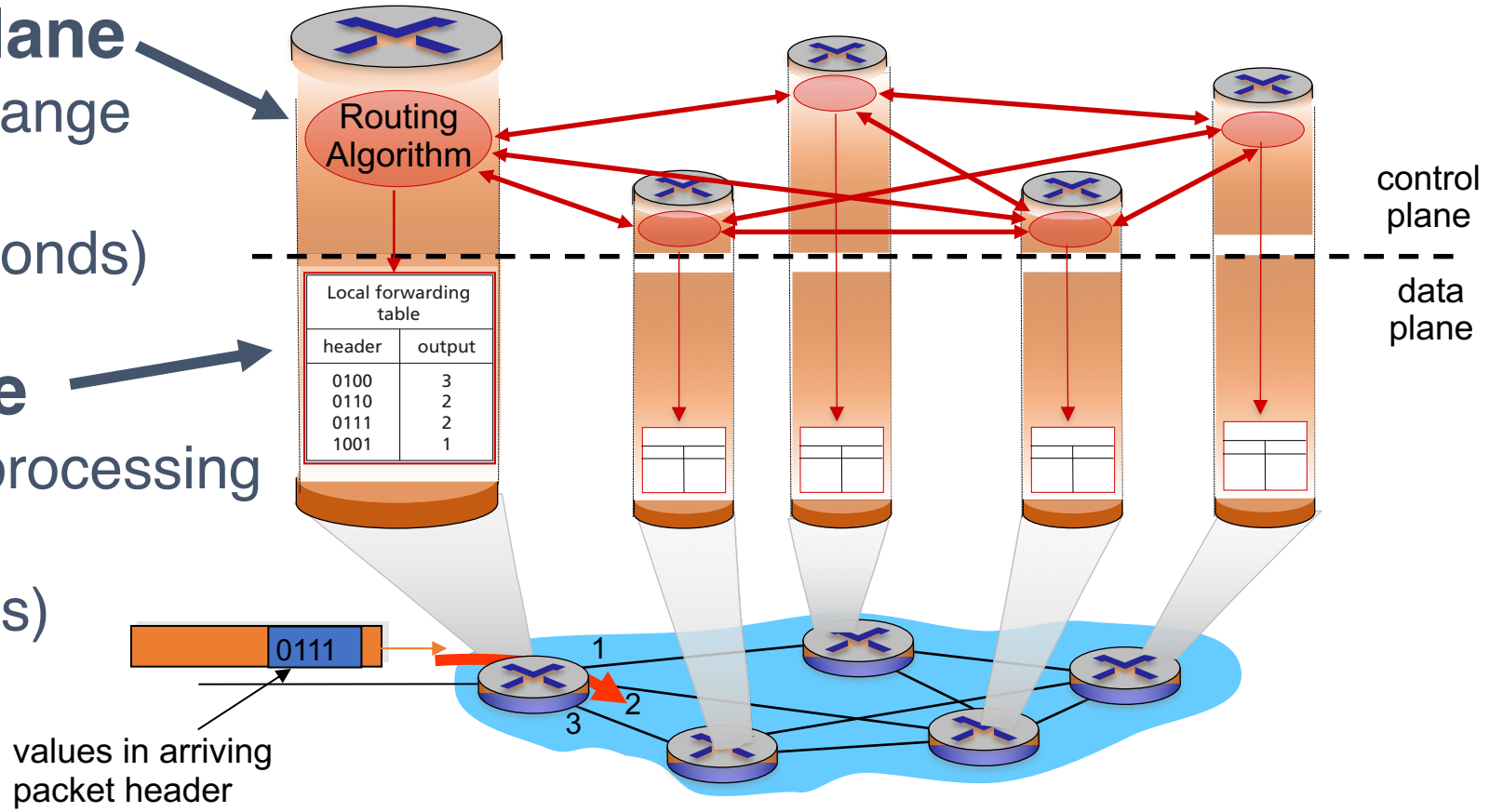
Fall 2019

RUTGERS
UNIVERSITY | NEW BRUNSWICK

Review: Control/data plane separation

Control plane
per route-change processing
(~ a few seconds)

Data plane
per-packet processing
(~ tens of nanoseconds)



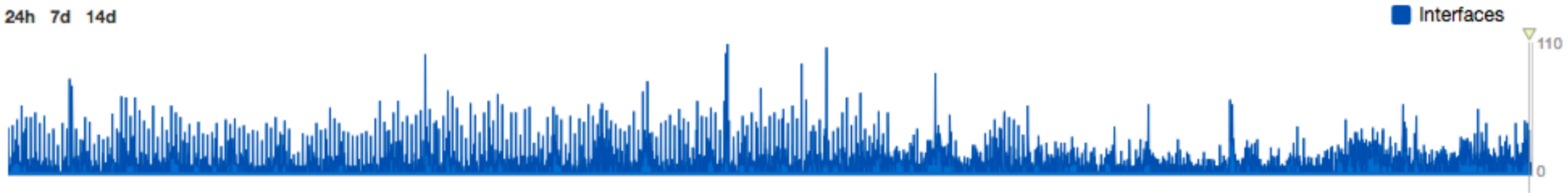
Traditionally:

Individual routing algorithm components *in each and every router* interact in the control plane

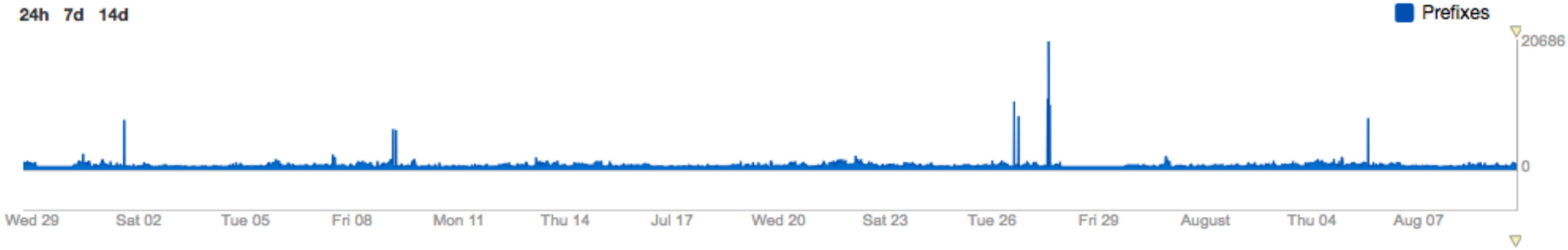
Networks are complex

- Numerous control plane protocols
  - RFCs numbering in the thousands
- Protocols interact in complex ways
  - Concerns of complexity extend to SDNs as well
  - Protocols must often work across administrative boundaries
- Significant outages often due to avoidable reasons
  - Human errors cause >50% of outages
- Network is in a constant state of change

Outages happen all the time



~ 170 affected interfaces / hour



~ 1.6K prefixes / hour

Source: https://blog.thousandeyes.com/nanog-68-decoding-performance-data-internet-outages/

Outages happen all the time

OUTAGE.REPORT

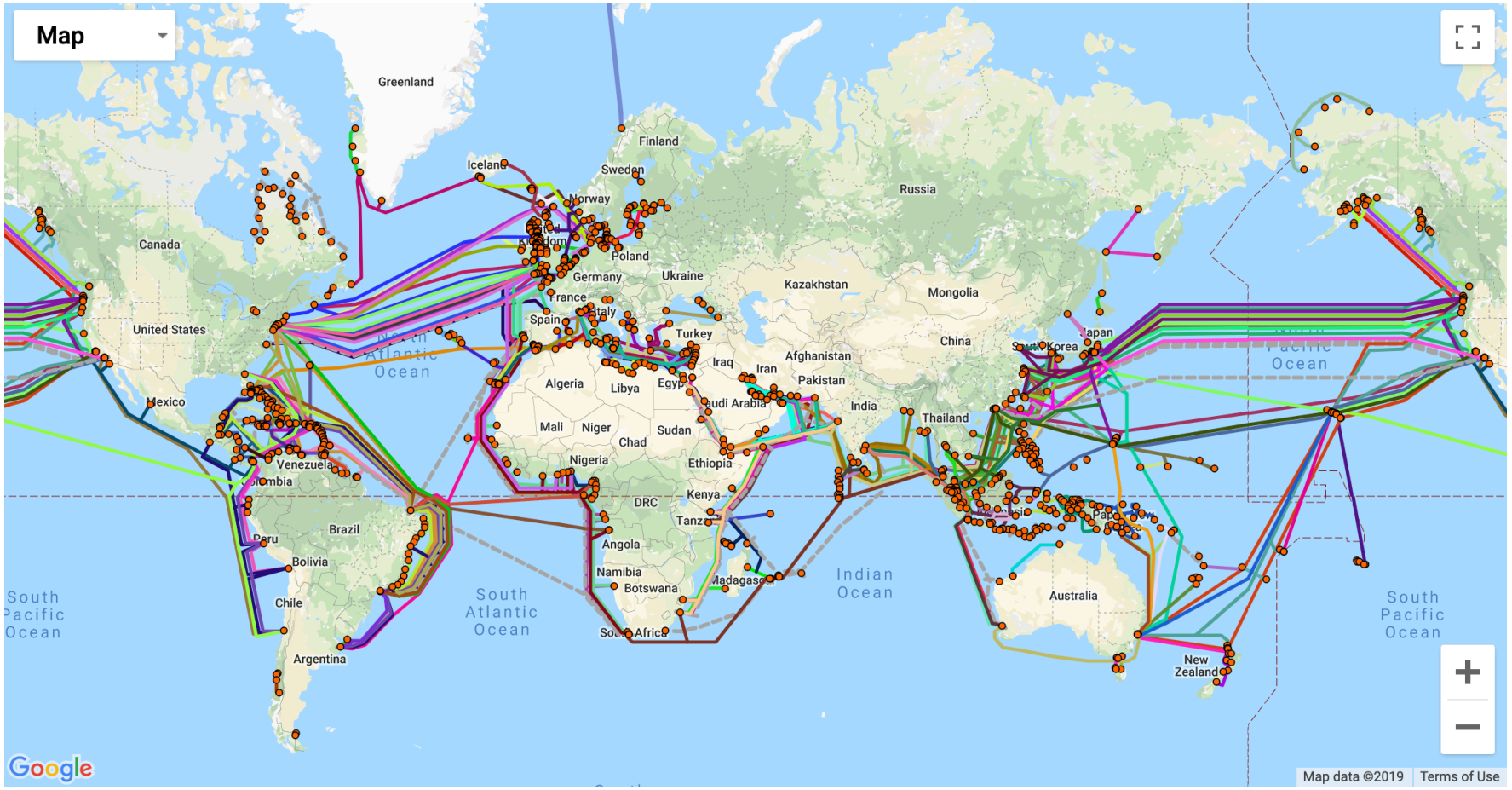
Recent Outages

Today

Destiny 2	Received 28 reports, originating from United States of America, Malaysia, Mexico, Netherlands, United Kingdom and 8 more countries	
Zerodha	Received 8 reports, mostly originating from Republic of India – Mumbai, Kashipur	
Google	Received 15 reports, originating from United States of America, Canada, Australia, United Kingdom, Republic of Indonesia and 2 more countries	
Spotify	Received 10 reports, originating from United States of America, United Kingdom, Czech Republic, Republic of France, Portuguese Republic and 2 more countries	

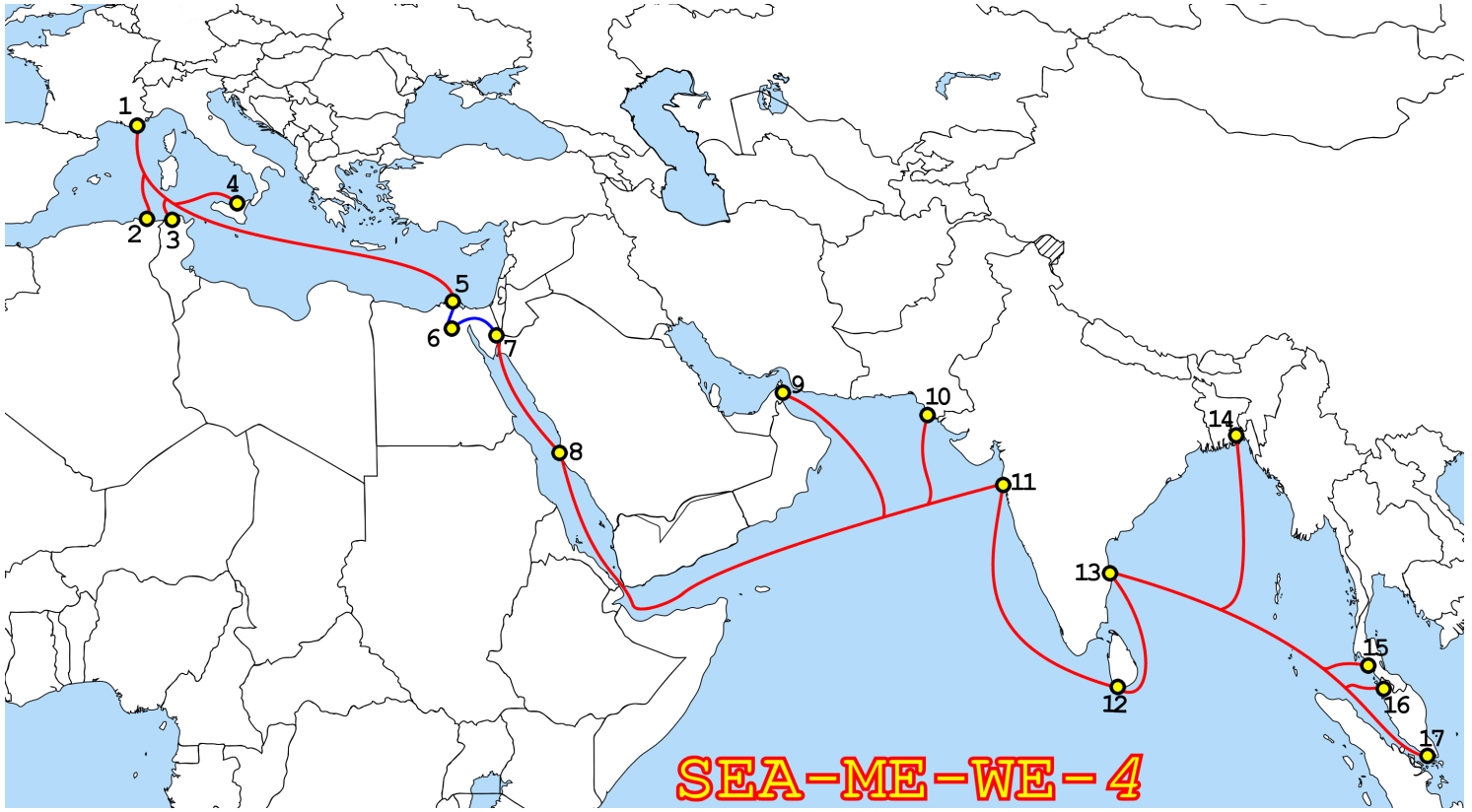
Root causes: Physical connectivity

- Cable faults



Root causes: Physical connectivity

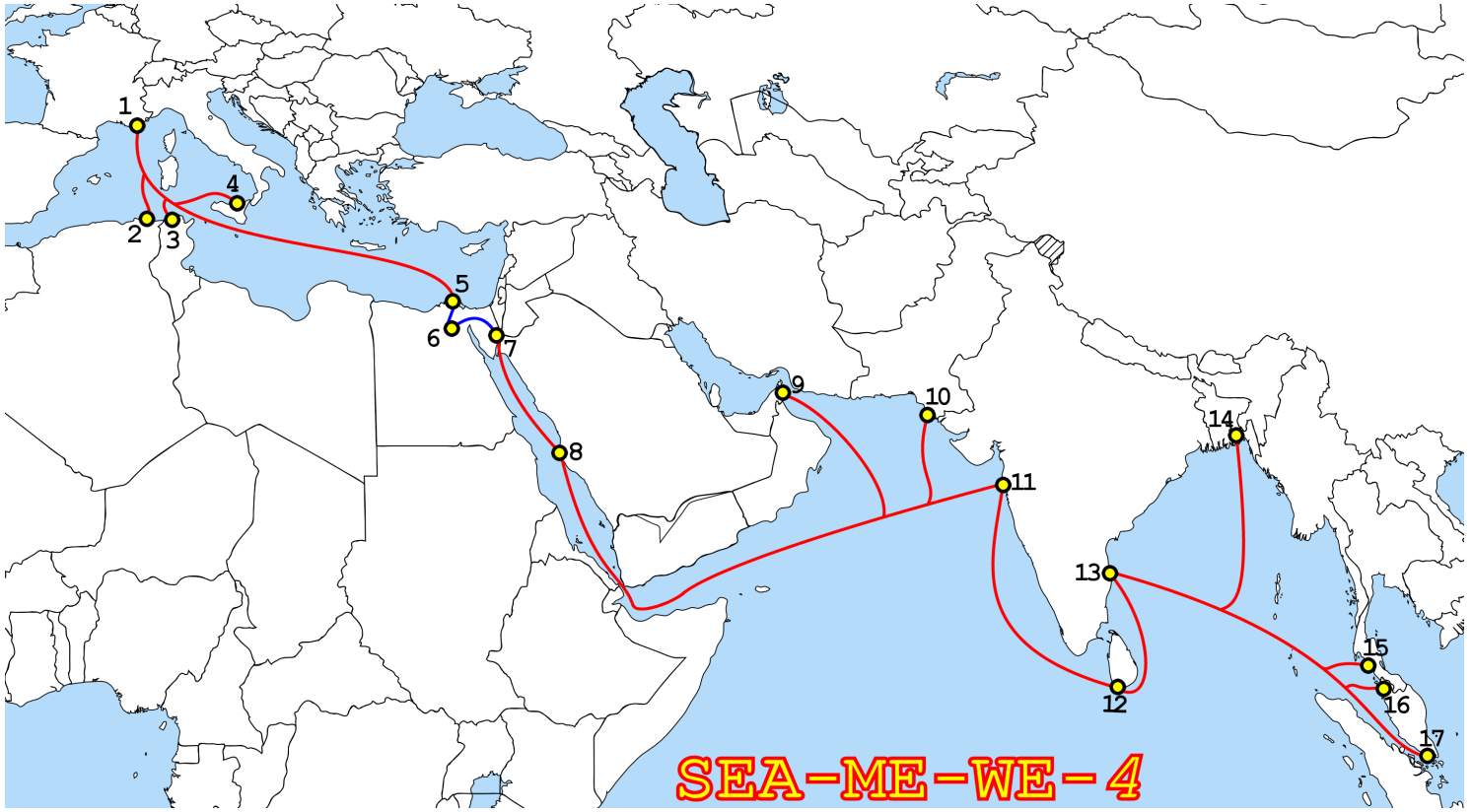
- Single cable fault or break can take out multiple ISP paths
  - Tata, Telecon Italia
- Cascading effects due to load on other links
  - New inter-dom paths taken
  - PoPs overloaded
  - Drop traffic worldwide



Root causes: Physical connectivity

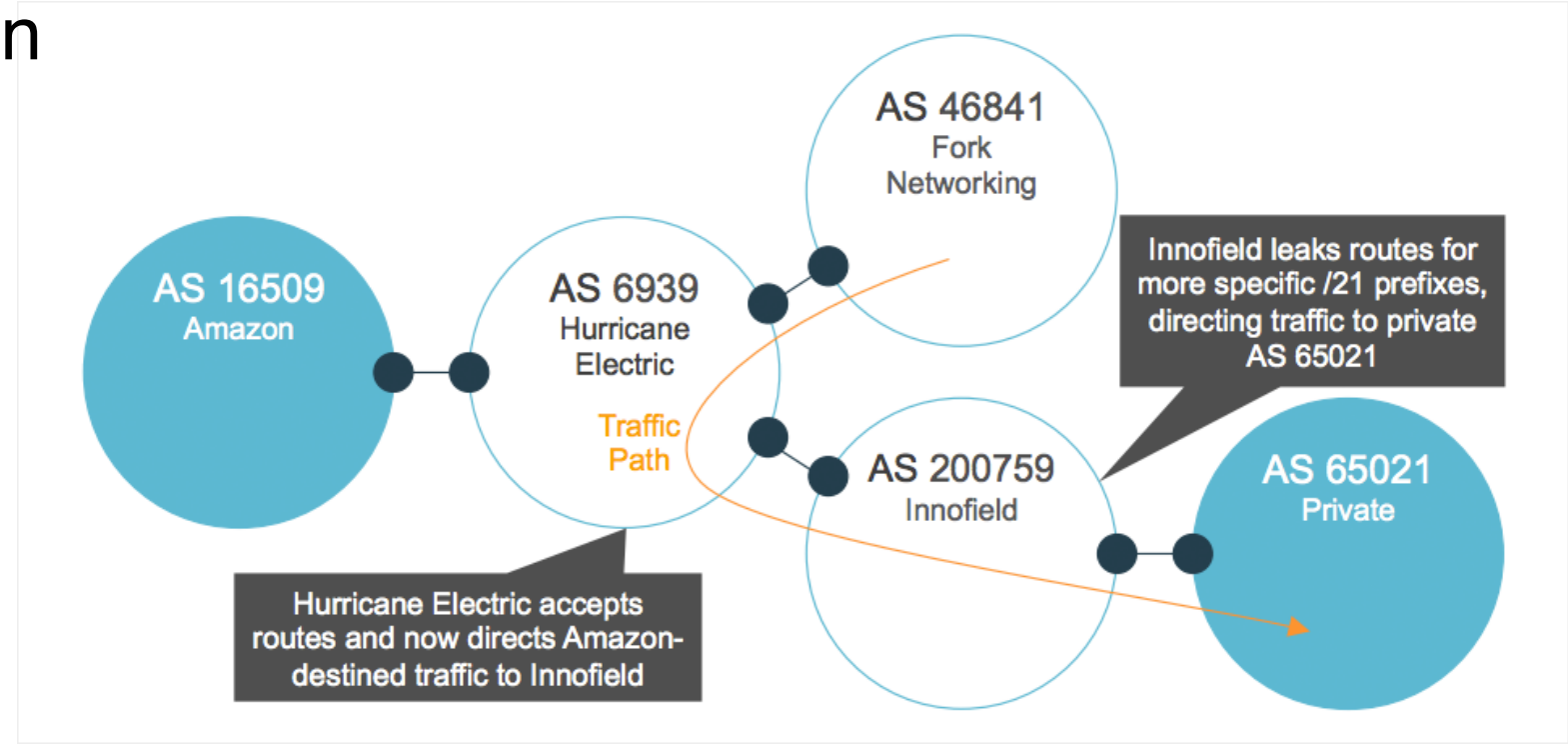
- Network interfaces can become faulty too

- Widespread intra-domain, or even inter-domain outages



Root causes: Route misconfiguration

- Leaks: e.g., ISP announces more specific routes to a destination
  - Prefix “hijacking”
- Flaps
- Likely to be misconfigurations
  - e.g., Youtube08
- But can also be deliberate: MITM
  - E.g., Belarus



Root causes

- Discussion so far about inter-domain failures
- But many intra-domain failures possible too
- Information leaks between tenants on a public cloud
  - e.g., HIPAA compliance
  - e.g., Banking regulations
- Loops in intra-domain routing
  - Transient loops due to convergence delay
  - Permanent loops due to misconfigurations
- Blackholes

A manifesto of operator requirements

- Know the answers to simple questions
  - Can A talk to B?
    - Reachability
    - A and B can be hosts, IP prefixes, “slices”
  - Are there loops, blackholes, …

- Know the effects of a change, preferably before it happens
  - What-if analyses
  - Link failures, protocol messages accepted from peers, …

- Answer these Qs fast to keep up with change in the network

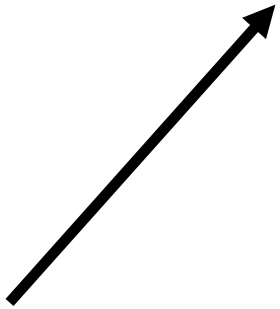
An Abstract Problem Statement

Formalizing verification as a mathematical problem

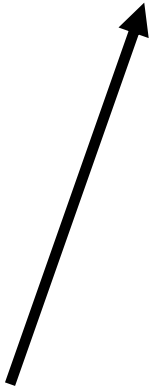
Decision Procedure: An algorithm that answers yes/no

Ask the question under assumptions about network change:
static, incremental, or dynamic

for all M, does N satisfy P?



Sequence of messages:
Packets,
Routing protocol
Link failures



Network representation:
Data plane
Control plane

Property of interest:
Loop freedom
Blackholes
Equivalence
Many complex props…

A simple example: Modeling firewall rules

- Assume packets just have 2 bits; there are only 2 ports
- Firewall config: 10 -> fwd(2); *1 -> fwd(1). All others dropped
- Boolean representation of the network:
  - N: (d1 & ~d0) | ((d1 | ~d1) & d0)
- Property: only the packets from 00 are dropped
  - P: (~d1 & ~d0)
- Messages (M): all combinations of Boolean variables d0, d1
- Verification question: for all d0, d1, is formula N | P valid? i.e.,
  - Is ((d1 & ~d0) | ((d1 | ~d1) & d0)) | (~d1 & ~d0) a tautology?
- Decision procedure: SAT solver

Typical considerations for verification

- Size of network representations
  - O(# rules)? # packets? Some product of these things?
- Speed of decision procedure, e.g., SAT solving
  - Typically NP-hard or worse in the worst case
  - Verification: leveraging average-case complexity
- Coverage of possible network events
  - Does property hold under firewall rule changes? New protocol messages? Link failures?
- Strength of properties and counter-examples
  - Does P hold for all packets? Are we looking for one counterexample, or the whole set of violating packets?

Verification, testing, synthesis, eq checks

- Verification: for all M, does N satisfy P?
- Testing: For the given M, does N satisfy P?
- Synthesis: Given P, can you produce an N that satisfies it
  - For a given set of M? (including for all M)
- Let N' be another network representation
- Equivalence checking: For all M, do N and N' behave in the same way with respect to P?, i.e.,
  - i.e., either both satisfy P or both violate it

Properties to verify

- Reachability, isolation, loop freedom
- Equivalence between data plane rules
  - Replicated configurations (for availability or performance)
  - Reducing to simpler configurations
- Waypoint properties
  - e.g., does traffic always go through a monitoring node?
  - Ordering constraints on processing: e.g., DPI must follow ACLs
- Temporal properties, e.g.:
  - After first message from a source, don’t broadcast traffic destined to it
- Performance properties: e.g., arrival distributions & congestion

Header Space Analysis

Header Space Analysis: Discussion

- Compact Boolean representation of router: union of wildcards
- Example? (say IP router)
- Operations on header spaces
  - e.g, Why is an inverse always well-defined?
- cross-product issue and the linear fragmentation assumption
- Representation matters! difference of two unions
- Properties: reachability, generic loops, infinite loops
- Loop detection: per-port vs. per-switch, any port vs. init port
- What else could you run on the HS “propagation tree”?

Scaling challenges with verification

- Too many messages and events
  - Packet headers
  - Link failures
  - Protocol messages
- Orderings between events matters
- Too many network rules
- Too large a network

10,000 ft overview of the broad literature

- Data plane verification
  - Static: header space analysis
  - Incremental: Veriflow
  - Dynamic: NICE
- Control and data plane verification
  - Static: p4v
  - Incremental: Batfish
  - Dynamic: Minesweeper