TRIGTRAN Problem Statement

draft-dawkins-trigtran-probstmt-00.txt

Spencer Dawkins
sdawkins@cynetanetworks.com
Carl E. Williams
carlw@mcsr-labs.org
Alper E. Yegin
Alper@docomolabs-usa.com

Problem Statement Topics

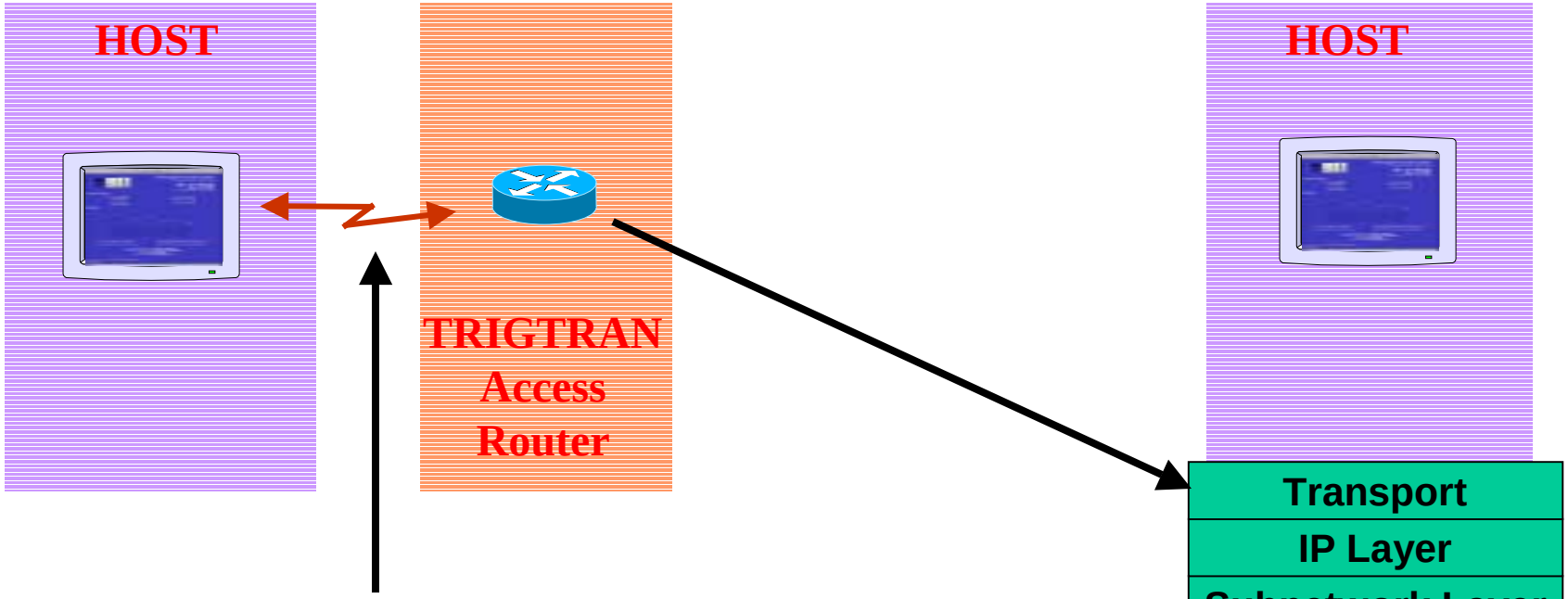
- Why do we think there's a problem?
- Minimal TRIGTRAN Strawman Architecture
- Partial TRIGTRAN Deployment
- TRIGTRAN Basics
- Security Considerations

What's The Problem?

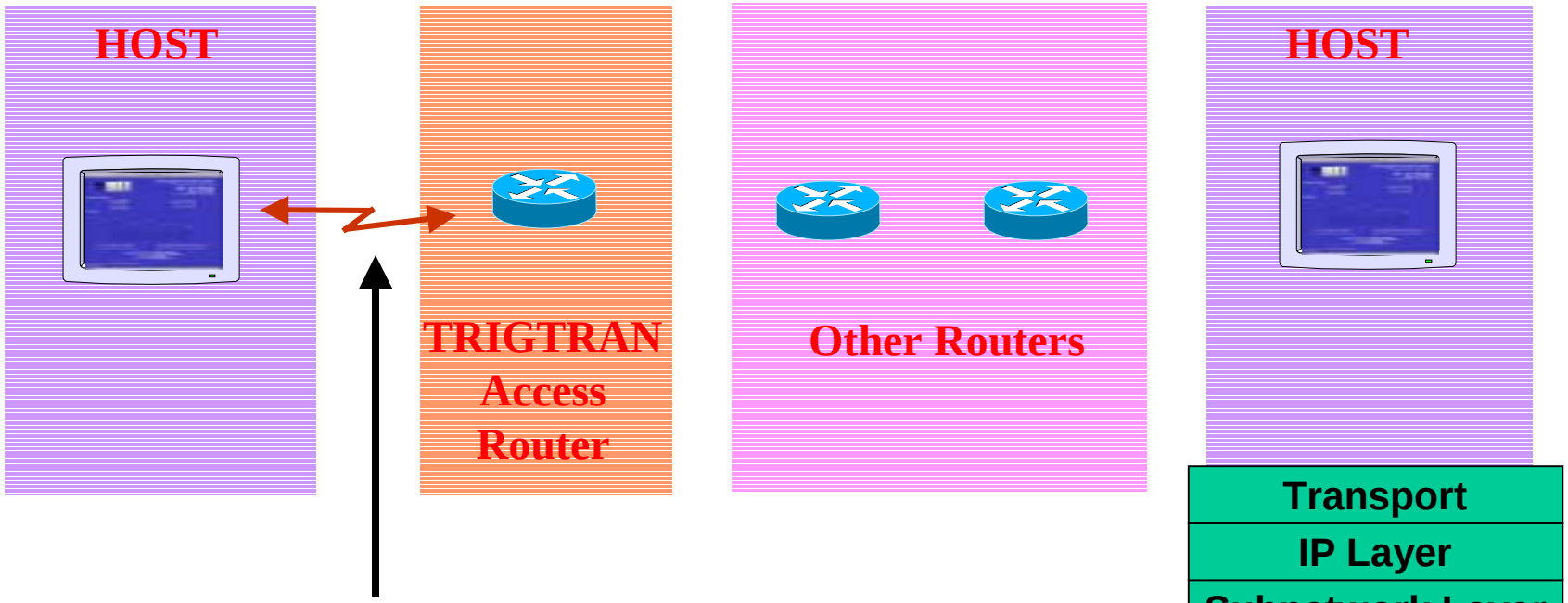
- End to end mechanisms work
  - … and we're not going to change them
- We're looking at paths with
  - Long – multi-second – RTTs
  - Transmission errors, not (just) congestion losses
  - Painful to lose a packet and retransmit
- Today's TCPs
  - Use multiple RTTs for end-to-end mechanisms
  - Can't tell the difference between errors and congestion
  - Run at a fraction of line speed on links with errors
- Can subnetworks provide hints that help TCP?

Minimal TRIGTRAN Strawman Architecture

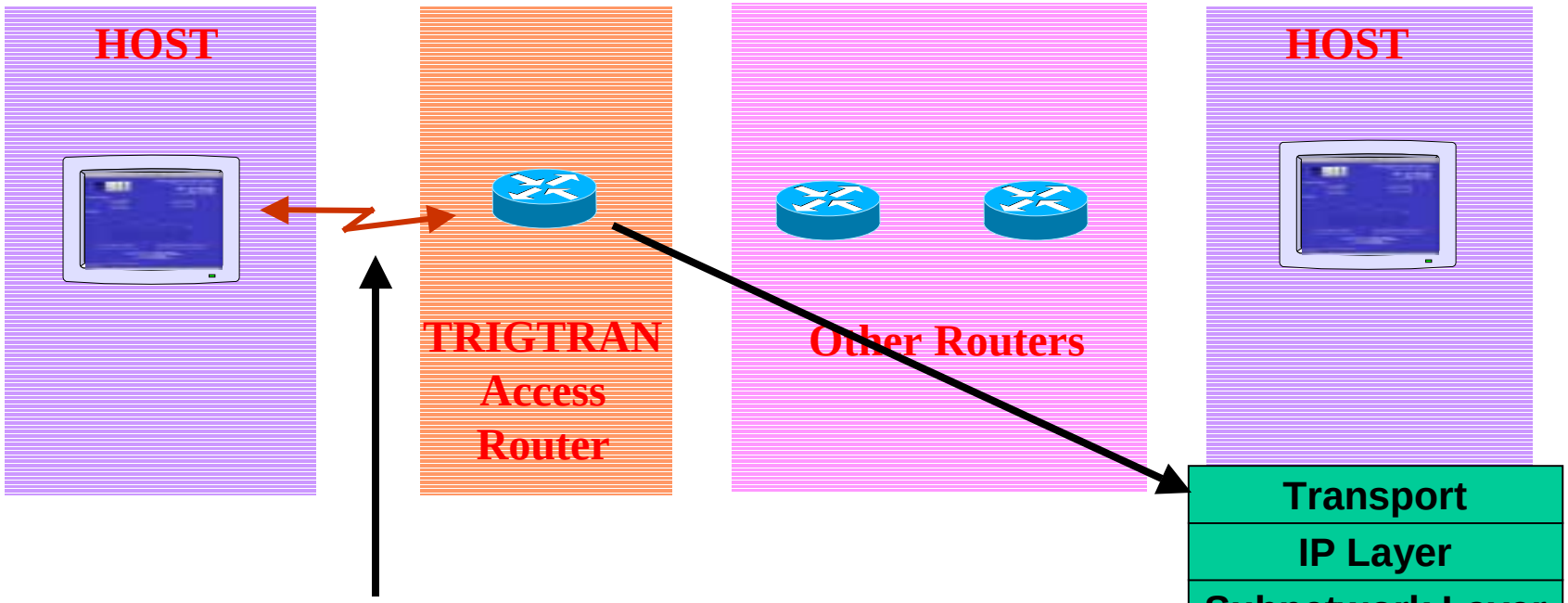
Minimal TRIGTRAN Strawman Architecture



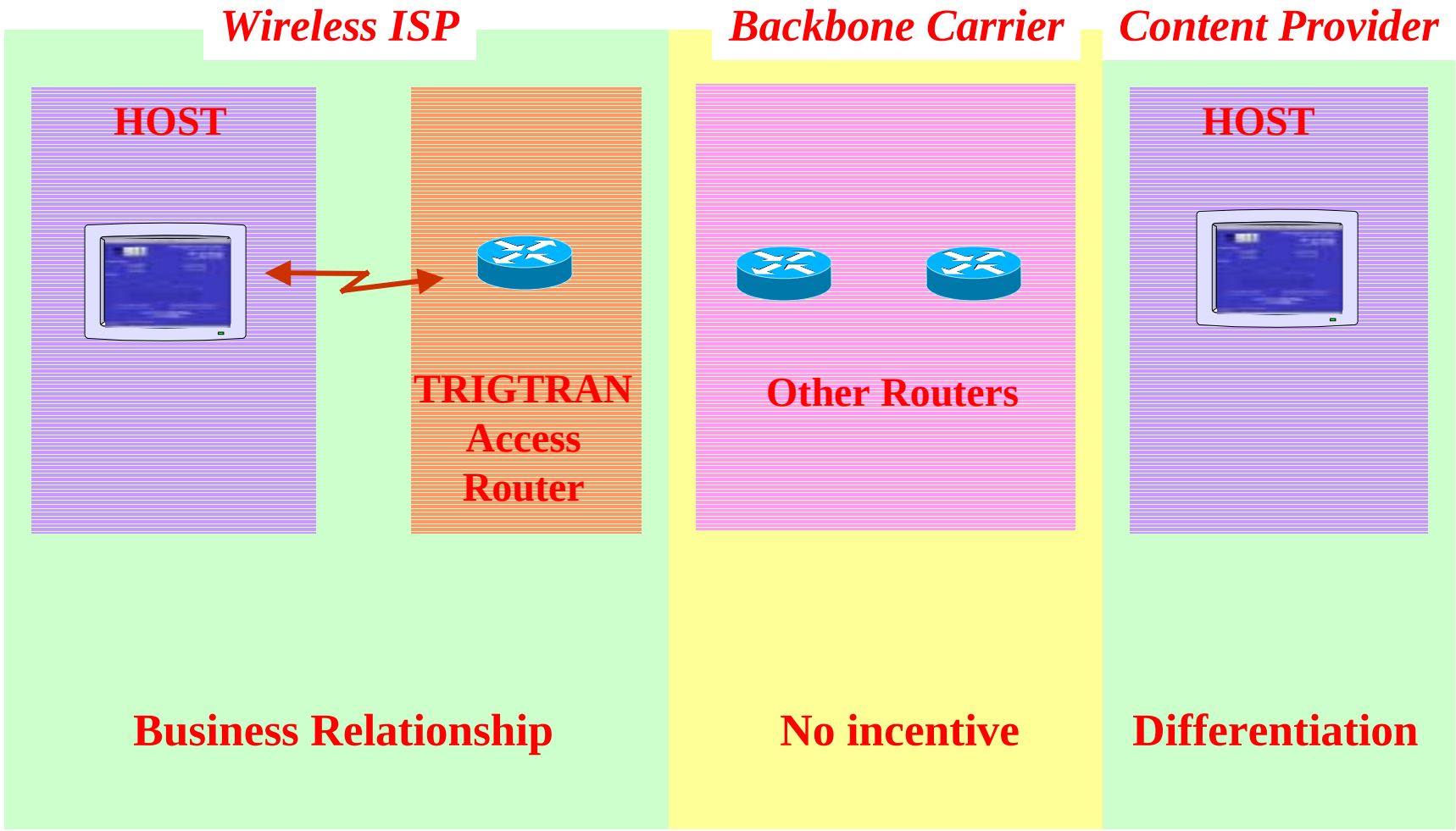
TRIGTRAN supported by Some, But Not All, Routers



TRIGTRAN supported by Some, But Not All, Routers



Incentives for Deployment?



What events cause notification?

"An event may not be applicable to every type of subnetwork, but it MUST NOT be technology-specific." – from the draft

- **Minimal set of TRIGTRAN events:**
  - **"link up" / "link down" events**
  - **Routing protocols have propagated these events for decades**
  - **Transports may care about "intermittent connectivity"**
- **Additional TRIGTRAN events**
  - **Packets discarded by subnetwork, not lost due to congestion**
  - **Sub-network path changes**
  - **Nominal sub-network bandwidth change**
  - **Other generic events identified by a TRIGTRAN working group**

Who receives notifications?

- **Hosts request event trigger coverage**
- **Hosts express interest in events**
- **TRIGTRAN routers notify interested hosts**

Notification model impacts scalability and ease of deployment

Protocol mechanisms for events

- **Open question to be explored.**
  - **An ICMP message**
  - **A unicast message to transport that requests triggers**
  - **A multicast message to listening transports**
- **Some questions to be answered:**
  - **The sending rate of trigger notifications assumed**
  - **Current Internet architecture issues (firewalls, NAT, ALG)**
  - **Current Internet deployment issues (ICMP black holes)**
  - **Security threat analysis**

What do transport entities do when they receive notifications?

- **Transports often ignore notification today**
  - **RFC 1122 - ICMP DESTINATION UNREACHABLE messages with codes of 0 (Net), 1 (Host), or 5 (Bad Source Route) are hints, not proof that a host is unreachable**
- **TRIGTRAN asks transports to consider notifications. Possible responses include:**
  - **Reducing TCP's congestion window**
  - **Sending a probe**
  - **Deferring packets until additional event notifications arrive**
  - **Notifying applications that an event has occurred**
- **Reasonable response varies by specific event**

Some Security Considerations

- **TRIGTRAN notifications can affect ongoing communications on the recipient hosts.**
  - **Malicious nodes can launch attacks on its victims.**
  - **Ex: an attacker can spoof a TRIGTRAN event to convince a victim that it can no longer use the network.**
- **DOS attack on TRIGTRAN router – by spoofing very high numbers of registration requests on behalf of non-existent hosts.**
  - **Attack would exhaust limited resources on the router**
- **Spurious notification by malicious host?**

TRIGTRAN protocol must include authentication for messages that can potentially create or alter state on protocol entities.

Threat model would reflect the types of events defined