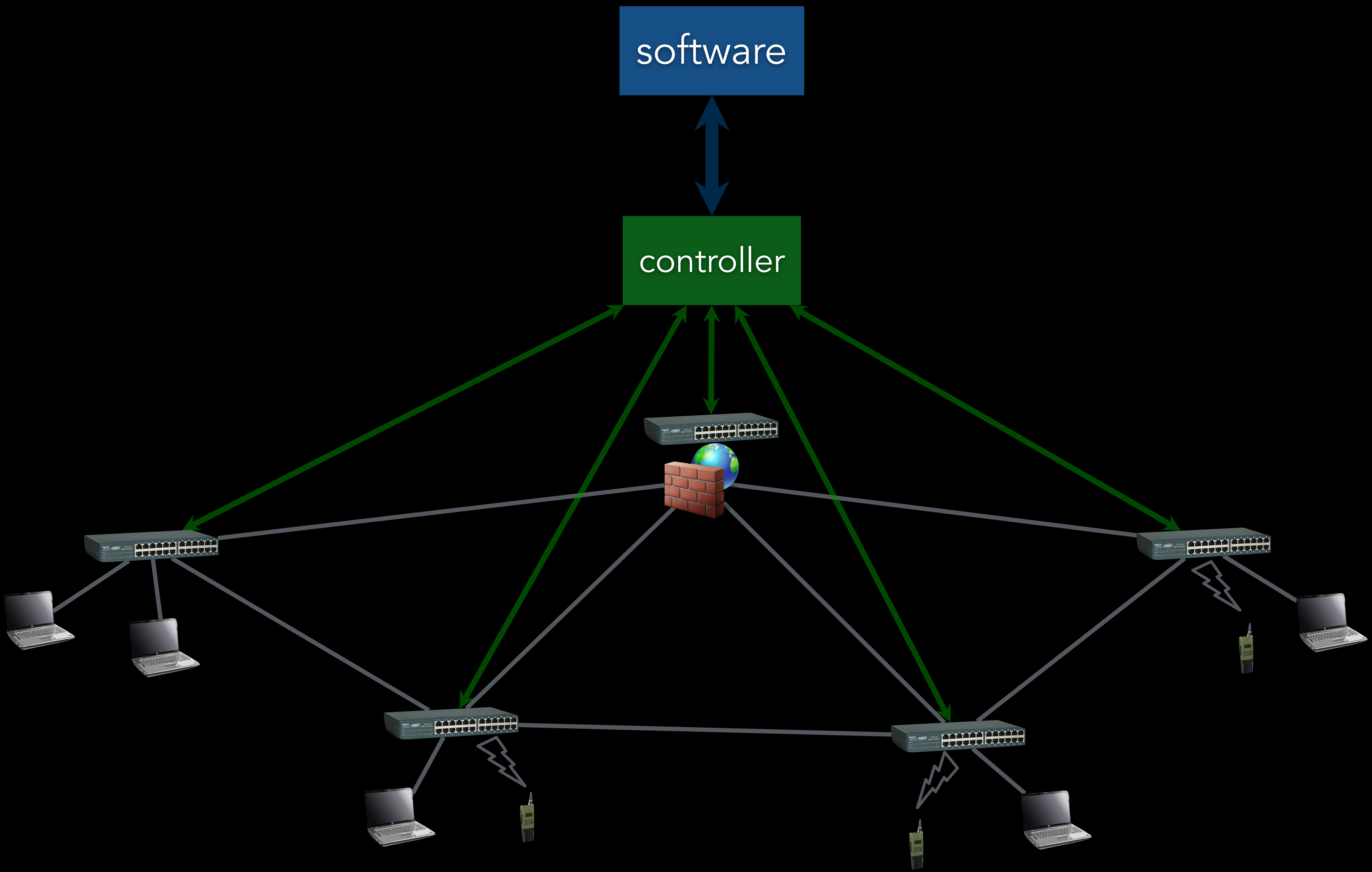
Midterm Report: Access Control For a Database-Defined Network

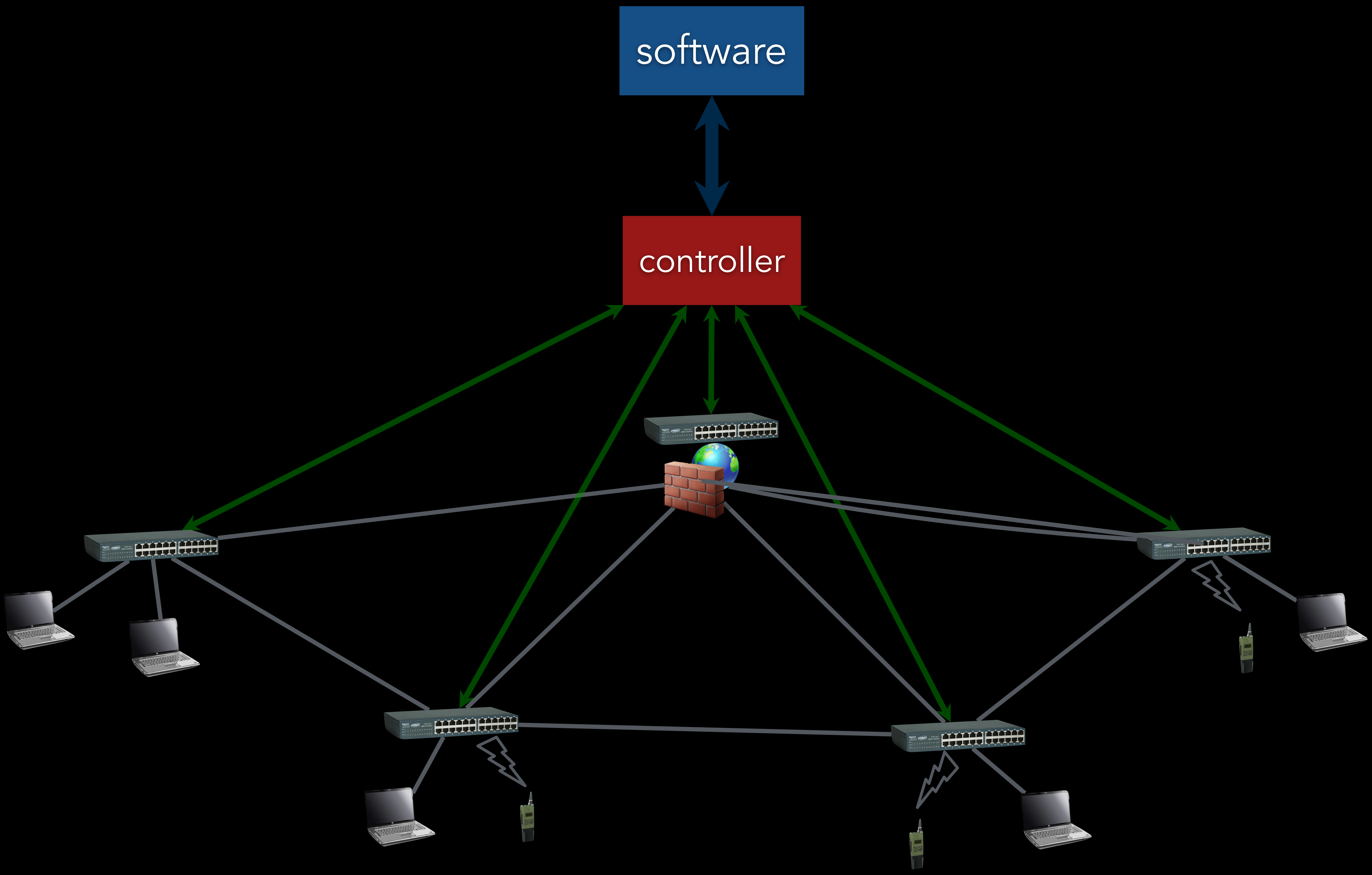
Noemi Glaeser

24 June 2016
Temple University REU program

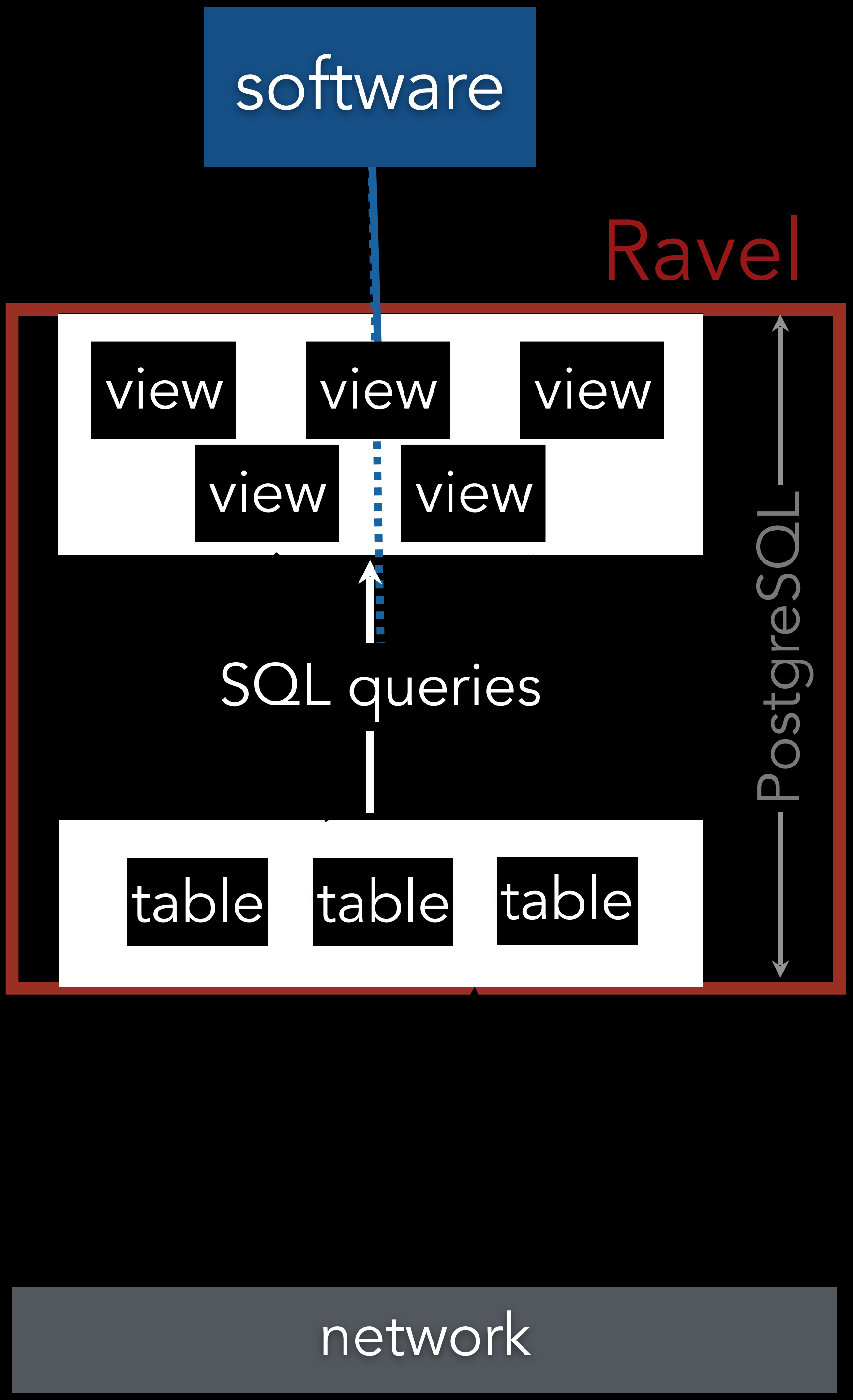
Software-Defined Networking (SDN)



Software-Defined Networking (SDN)



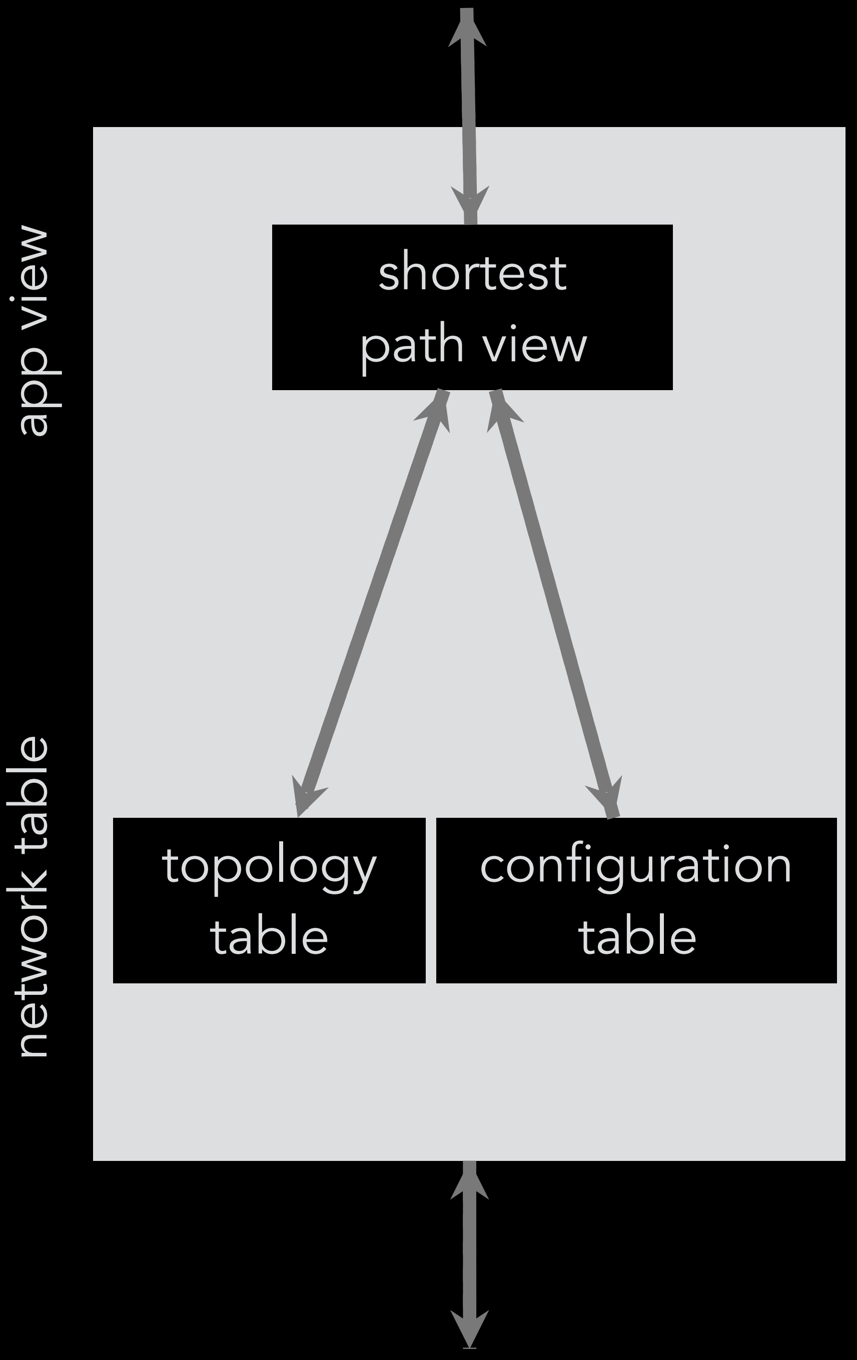
Ravel: A Database Controller



- Using database as the controller

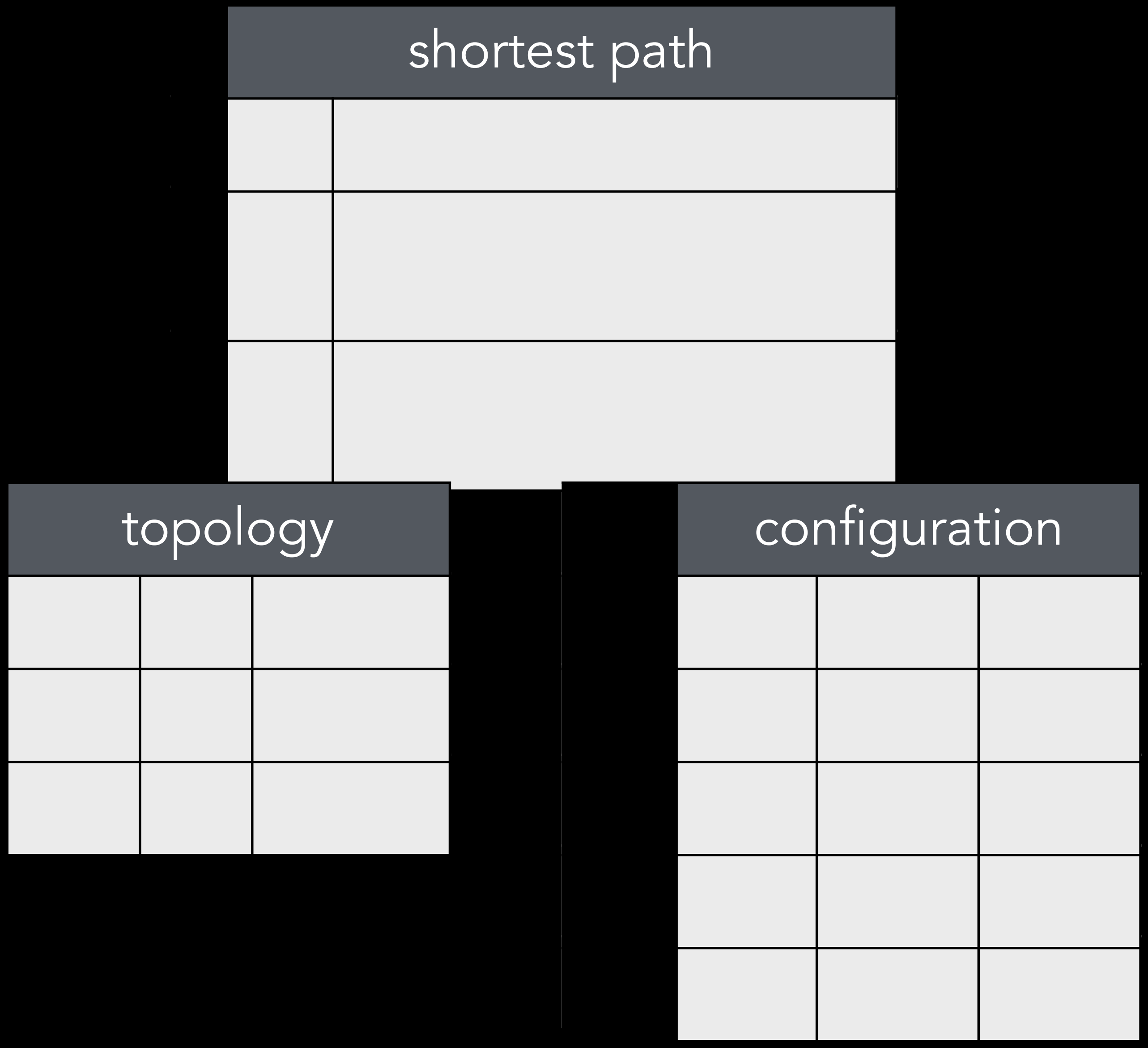
Ravel in Action

routing app: check
broken path, re-route

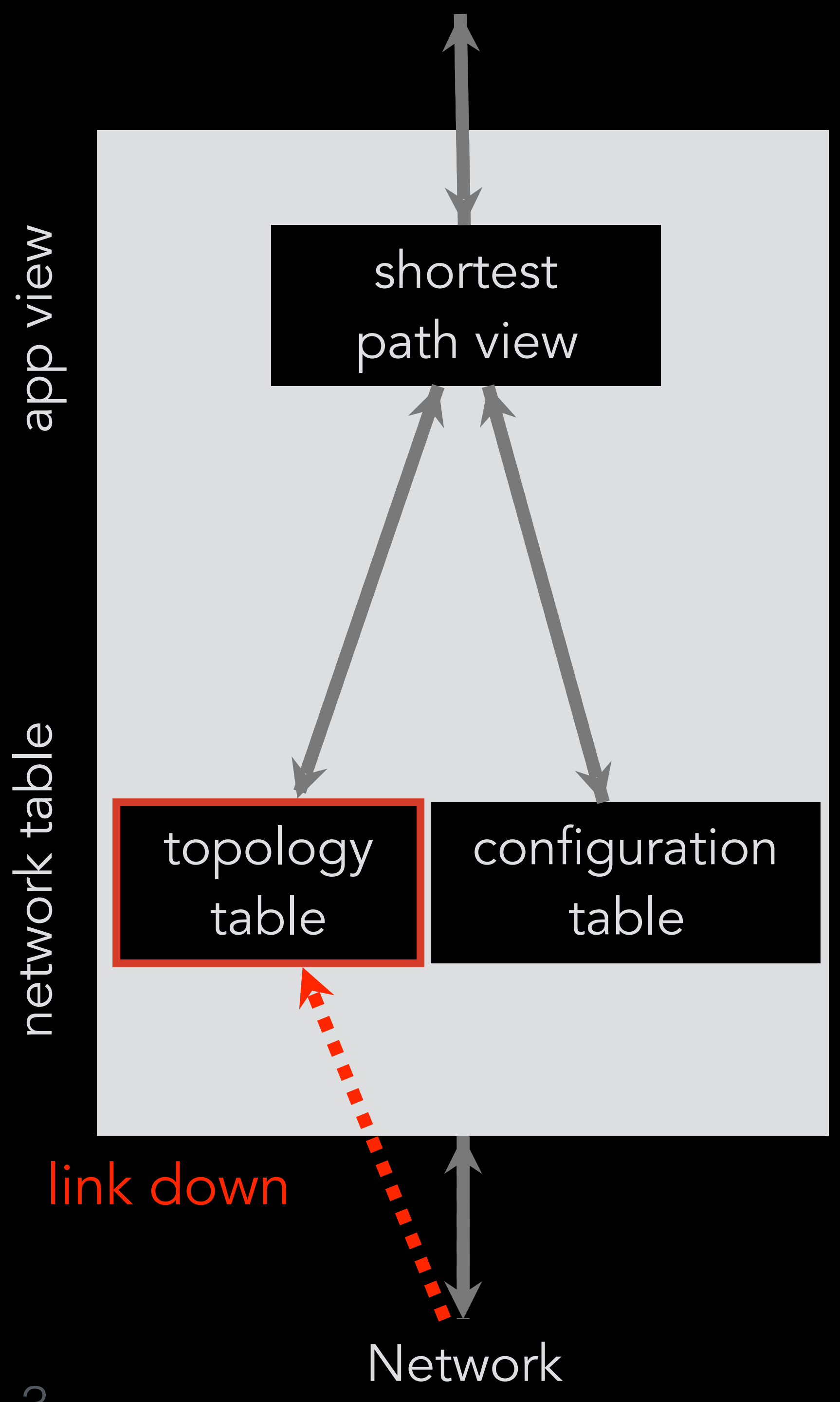


Network

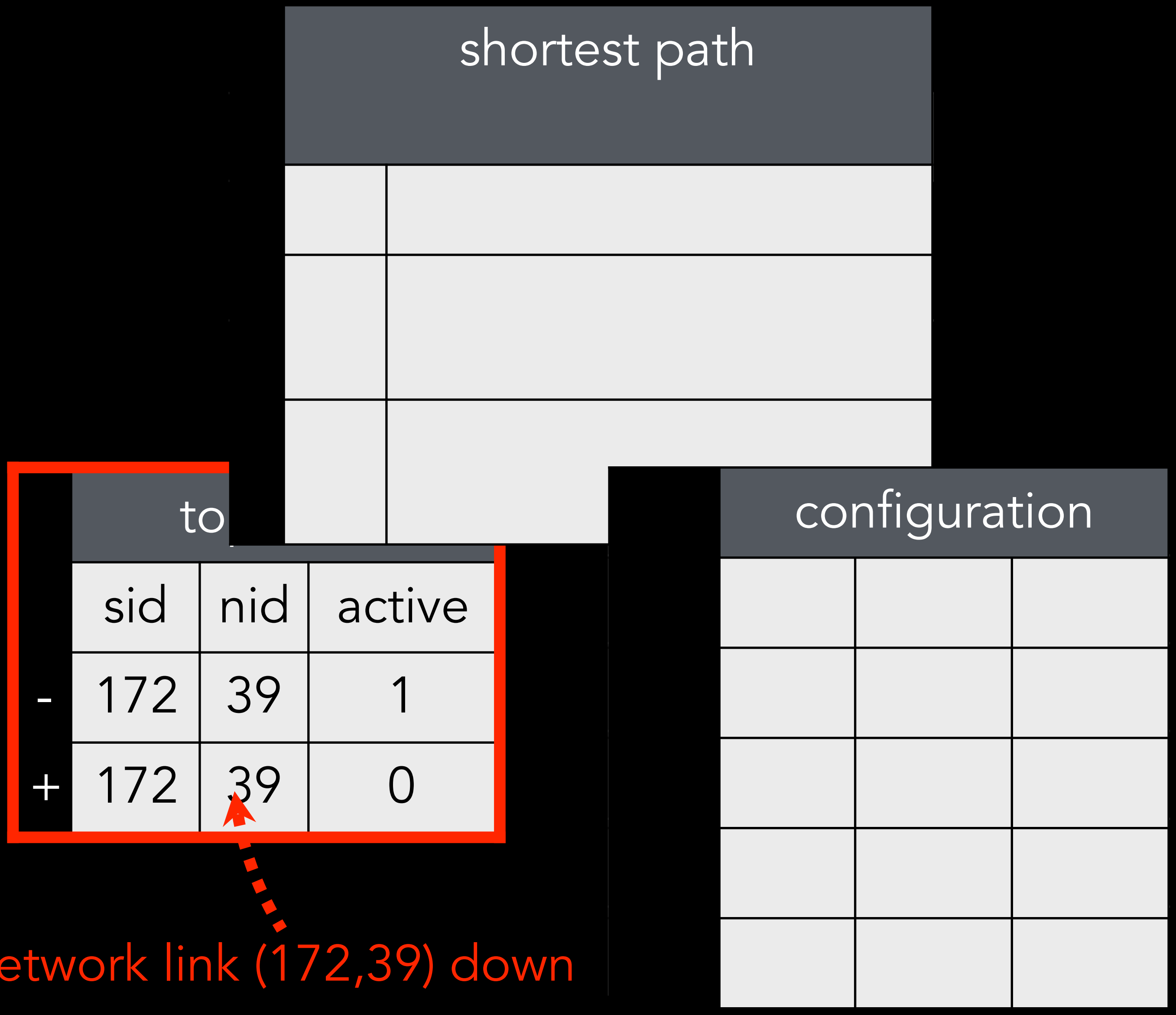
SQL rule:
upon broken path, re-route



Ravel in Action



SQL rule:
upon broken path, re-route

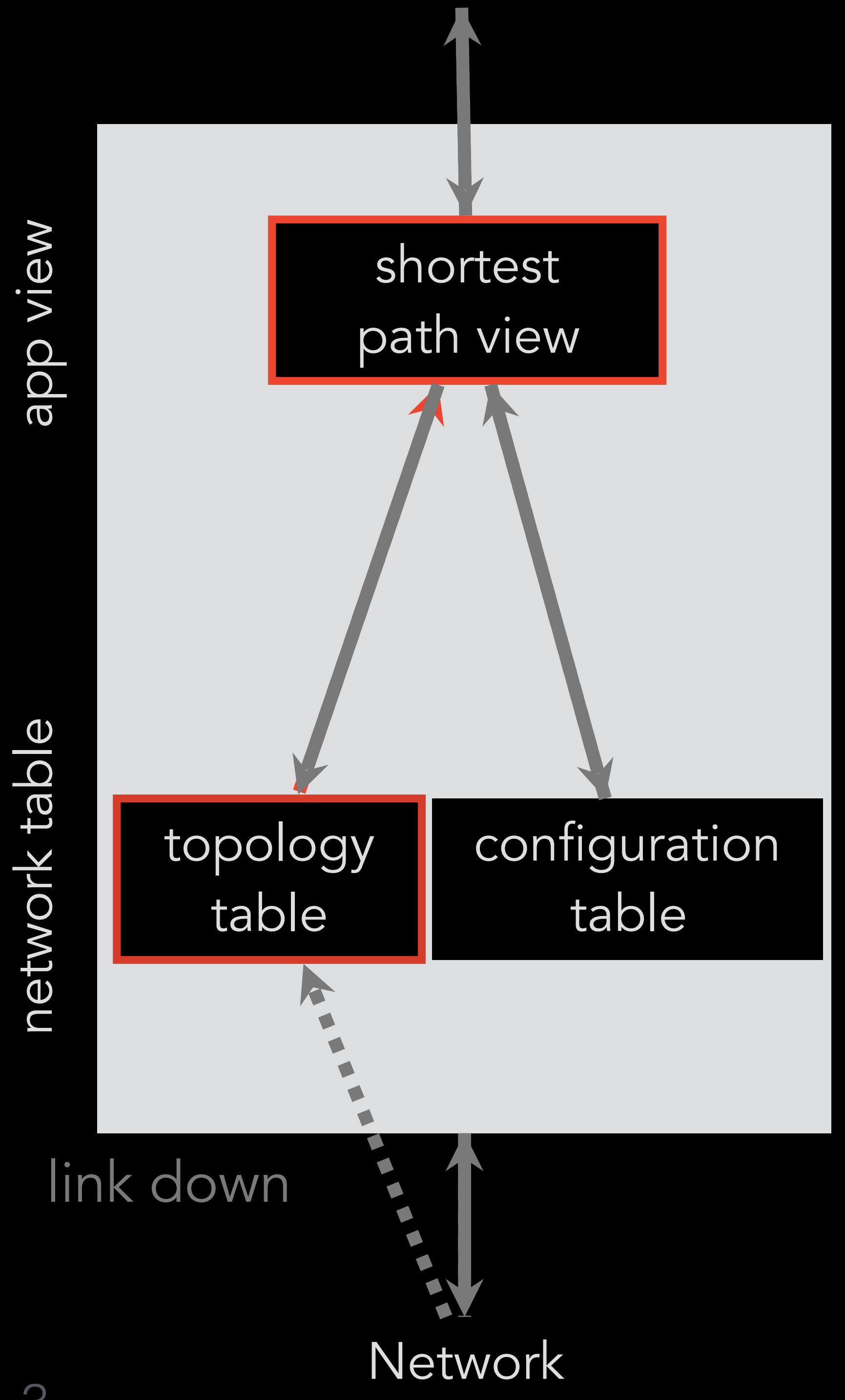


	sid	nid	active
-	172	39	1
+	172	39	0

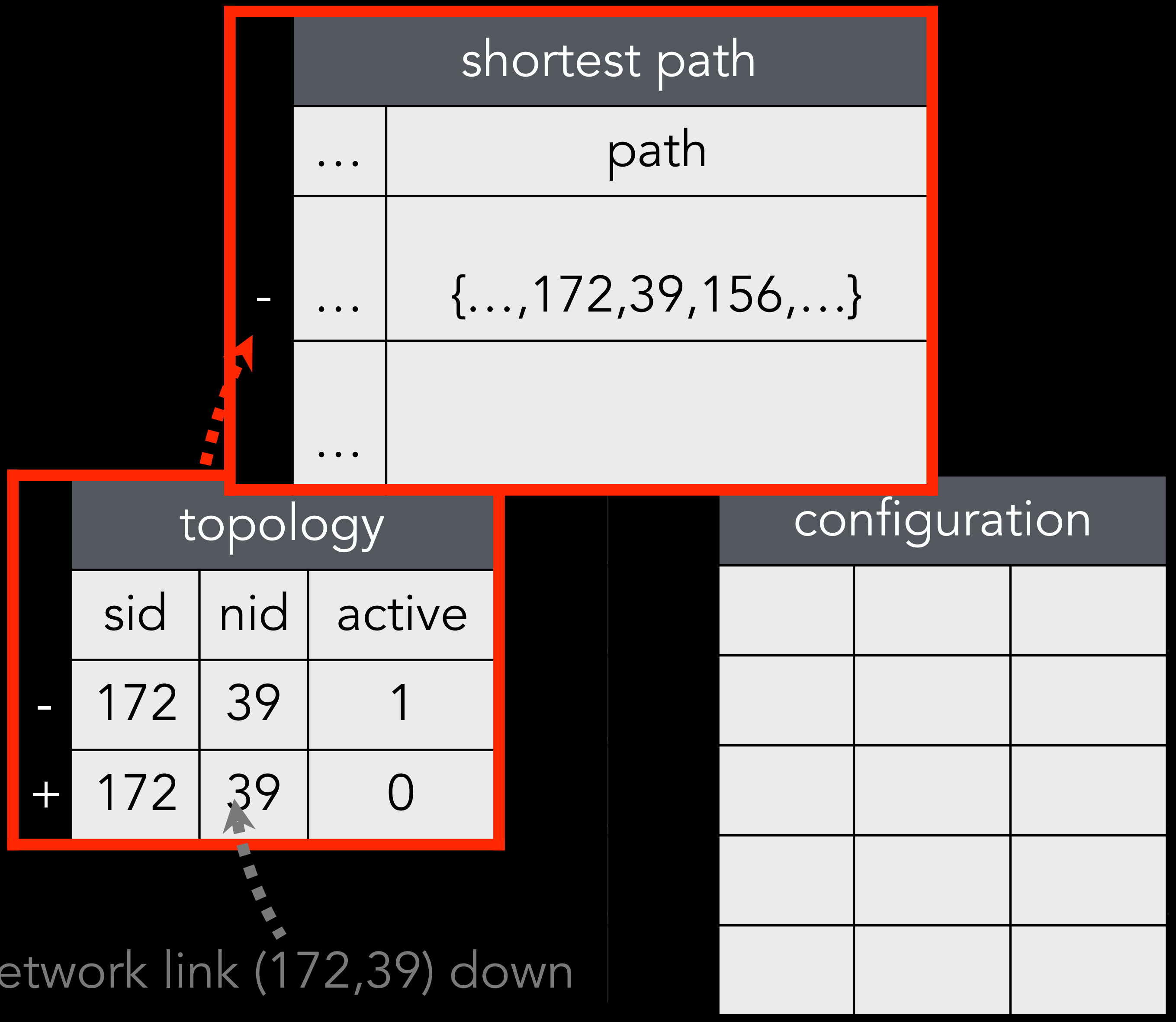
Network link (172,39) down

Ravel in Action

routing app: check
broken path, re-route



SQL rule:
upon broken path, re-route



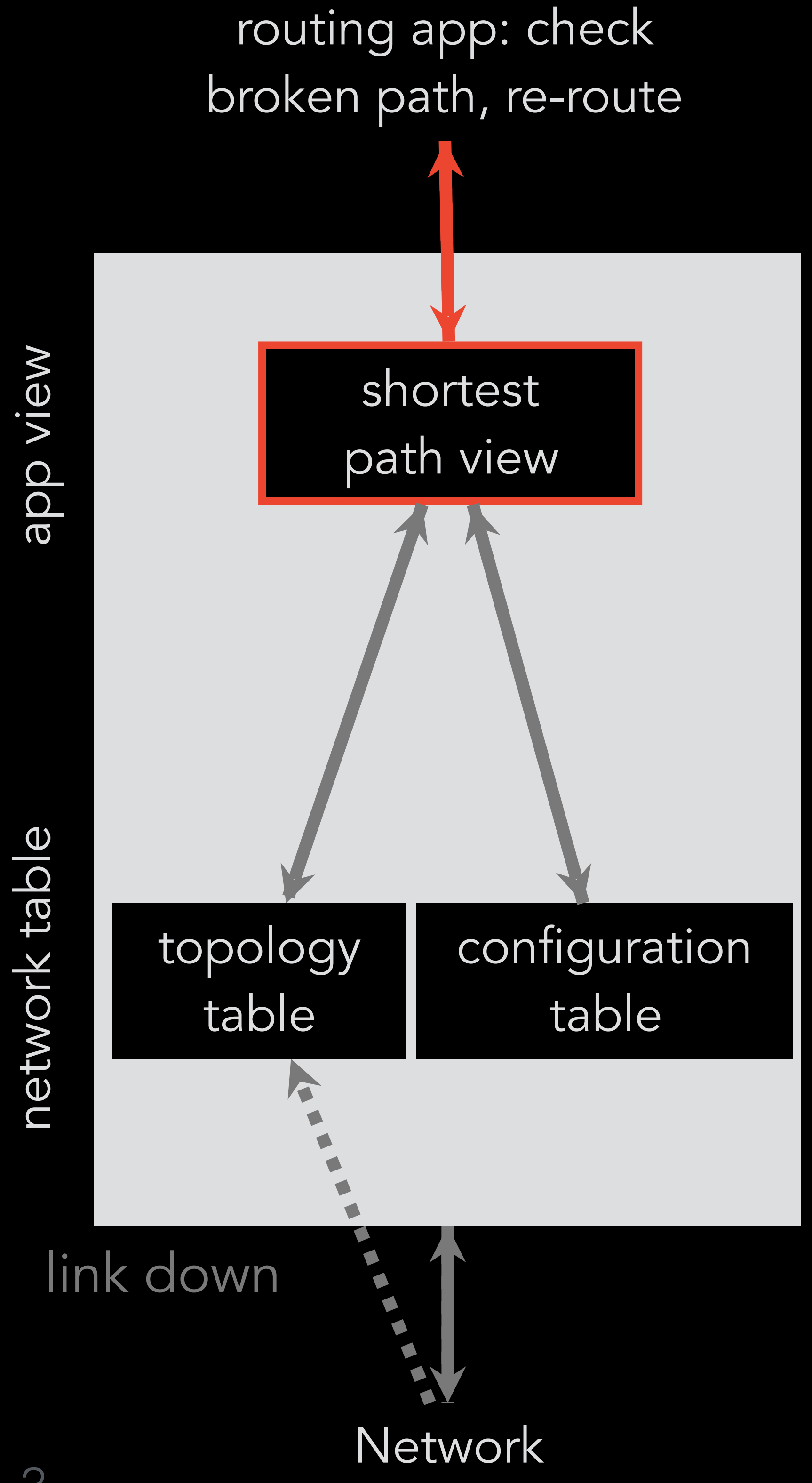
	shortest path	
	…	path
-	…	{…,172,39,156,…}
	…	

	topology		
	sid	nid	active
-	172	39	1
+	172	39	0

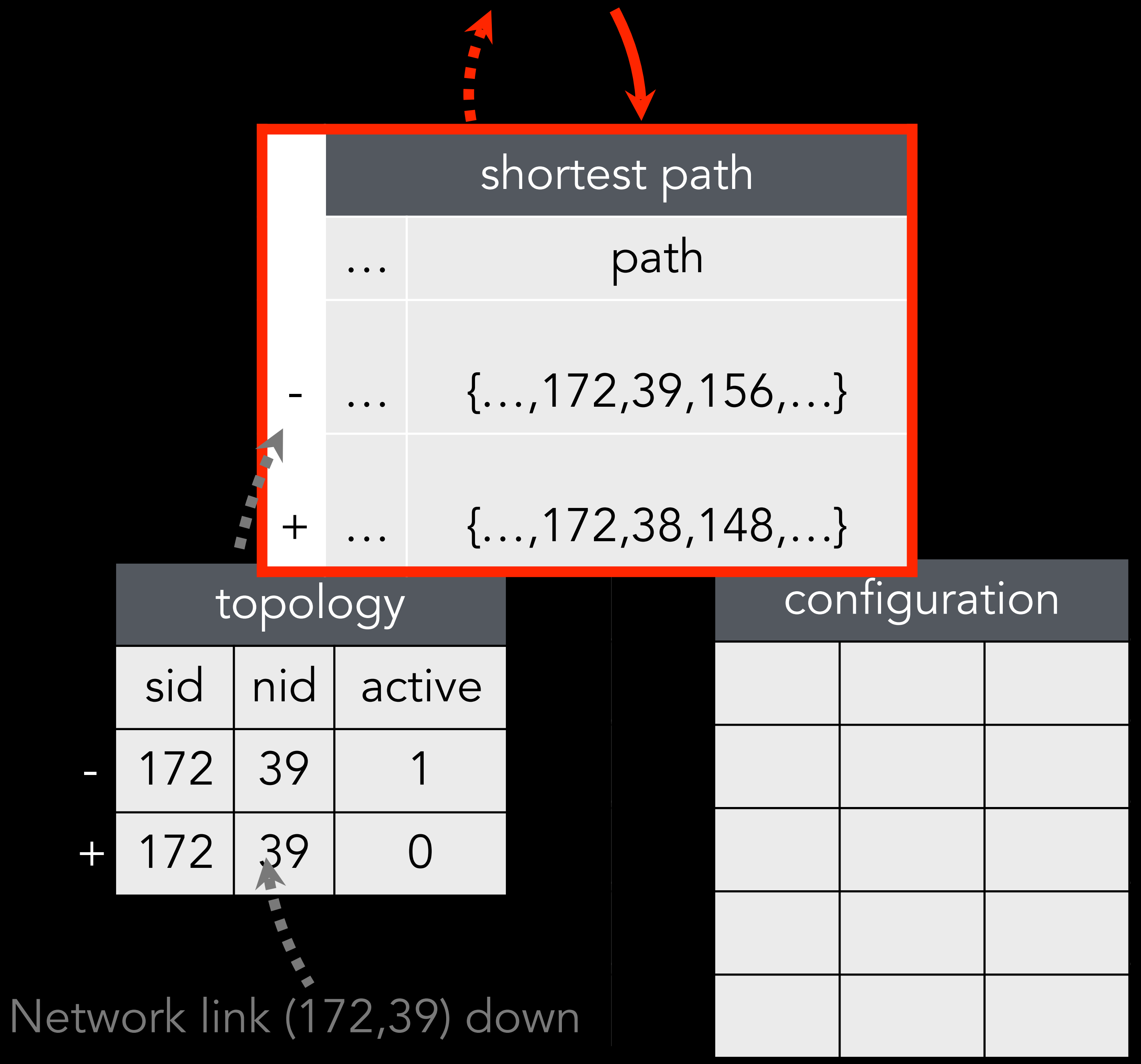
configuration		

Network link (172,39) down

Ravel in Action



SQL rule:
upon broken path, re-route

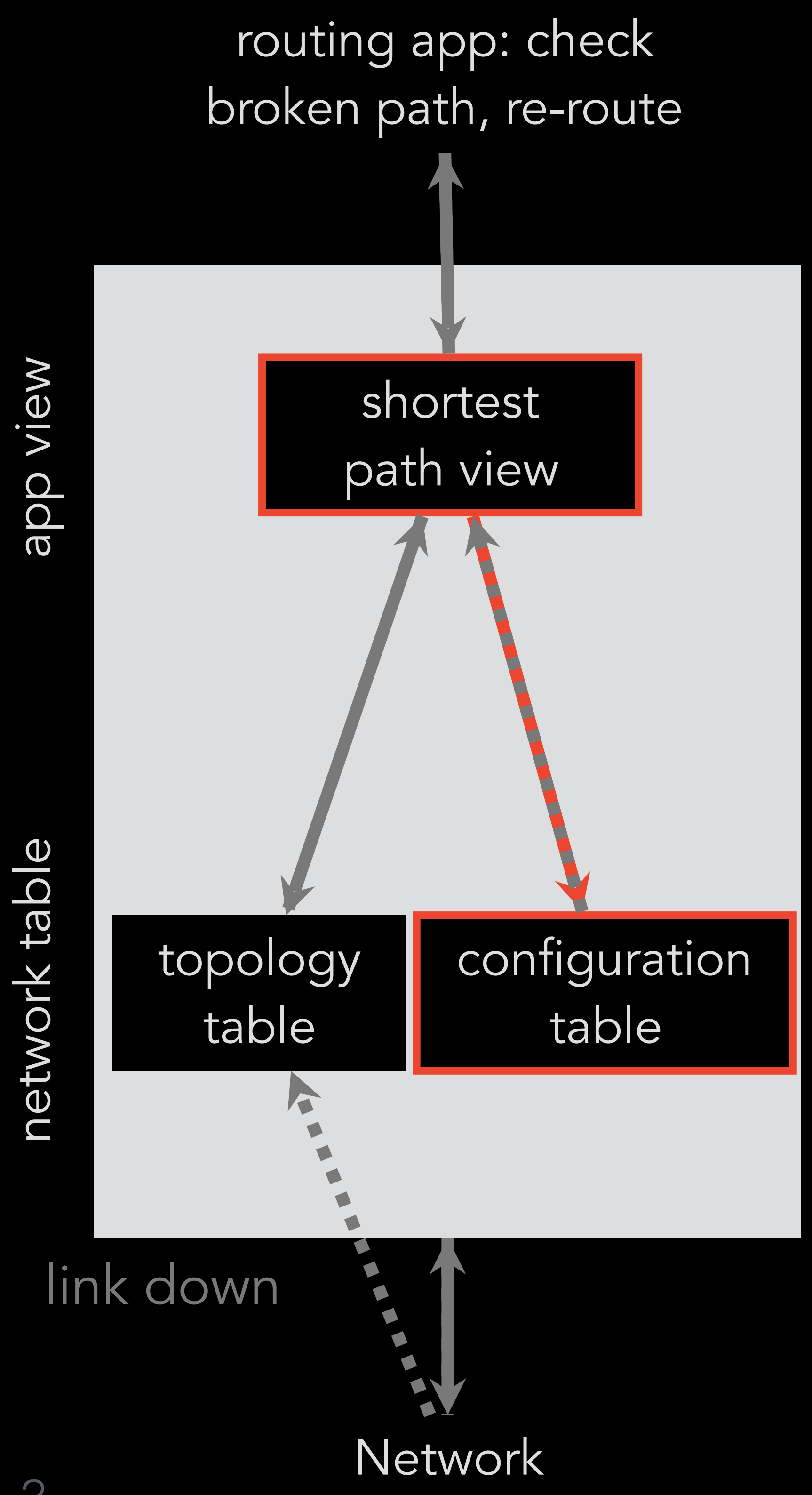


	shortest path	
	…	path
-	…	{…,172,39,156,…}
+	…	{…,172,38,148,…}

	topology		
	sid	nid	active
-	172	39	1
+	172	39	0

configuration		

Ravel in Action



routing app: check broken path, re-route

app view

shortest path view

network table

topology table

configuration table

link down

Network

SQL rule:
upon broken path, re-route

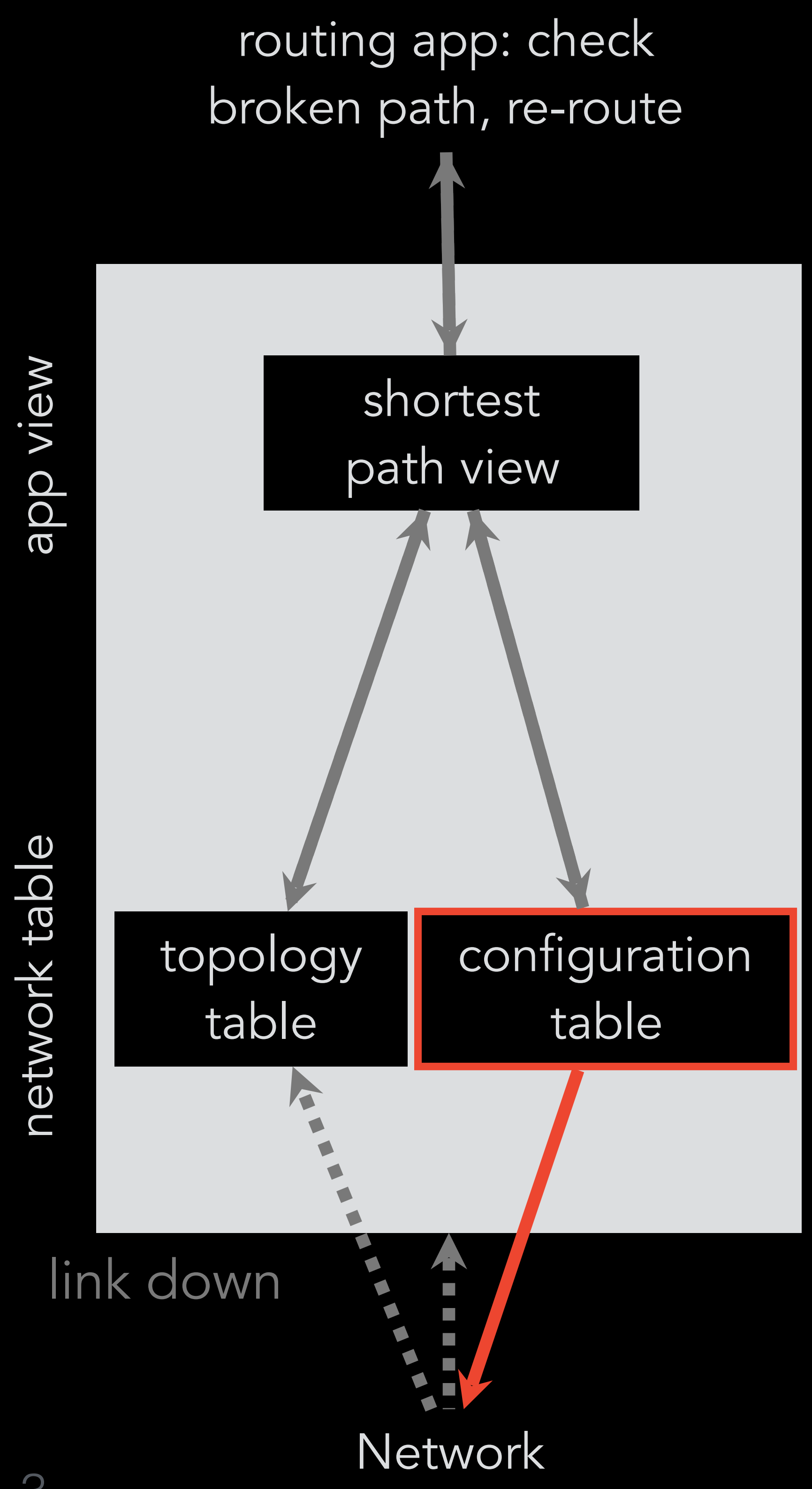
	shortest path	
	…	path
-	…	{…,172,39,156,…}
+	…	{…,172,38,148,…}

	topology		
	sid	nid	active
-	172	39	1
+	172	39	0

	configuration		
	fid	sid	nid
-	…	172	39
-	…	39	156
+	…	172	38
+	…	38	148

Network link (172,39) down

Ravel in Action



routing app: check
broken path, re-route

app view

shortest
path view

network table

topology
table

configuration
table

link down

Network

SQL rule:
upon broken path, re-route

	shortest path	
	…	path
-	…	{…,172,39,156,…}
+	…	{…,172,38,148,…}

	topology		
	sid	nid	active
-	172	39	1
+	172	39	0

	configuration		
	fid	sid	nid
-	…	172	39
-	…	39	156
+	…	172	38
+	…	38	148

Network link (172,39) down

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today
- Most SDN controllers do not implement security

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today
- Most SDN controllers do not implement security
- Security requirements still under development

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today
- Most SDN controllers do not implement security
- Security requirements still under development
  - Direction of information flow

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today
- Most SDN controllers do not implement security
- Security requirements still under development
  - Direction of information flow
  - Access control

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today
- Most SDN controllers do not implement security
- Security requirements still under development
  - Direction of information flow
  - Access control
- Currently, the Ravel controller exposes all network states to users

Toward a Secure Database-Defined Network

- Critical but less-studied aspect in SDN today
- Most SDN controllers do not implement security
- Security requirements still under development
  - Direction of information flow
  - Access control
- Currently, the Ravel controller exposes all network states to users
- This project: enhance Ravel with access control support

Strawman Solution

- Explicit specification (principal, object, privilege)

Strawman Solution

- Explicit specification (principal, object, privilege)

('alice', topology, insert)

Strawman Solution

- Explicit specification (principal, object, privilege)

  (‘alice’, topology, insert)

- Manual, tedious

Strawman Solution

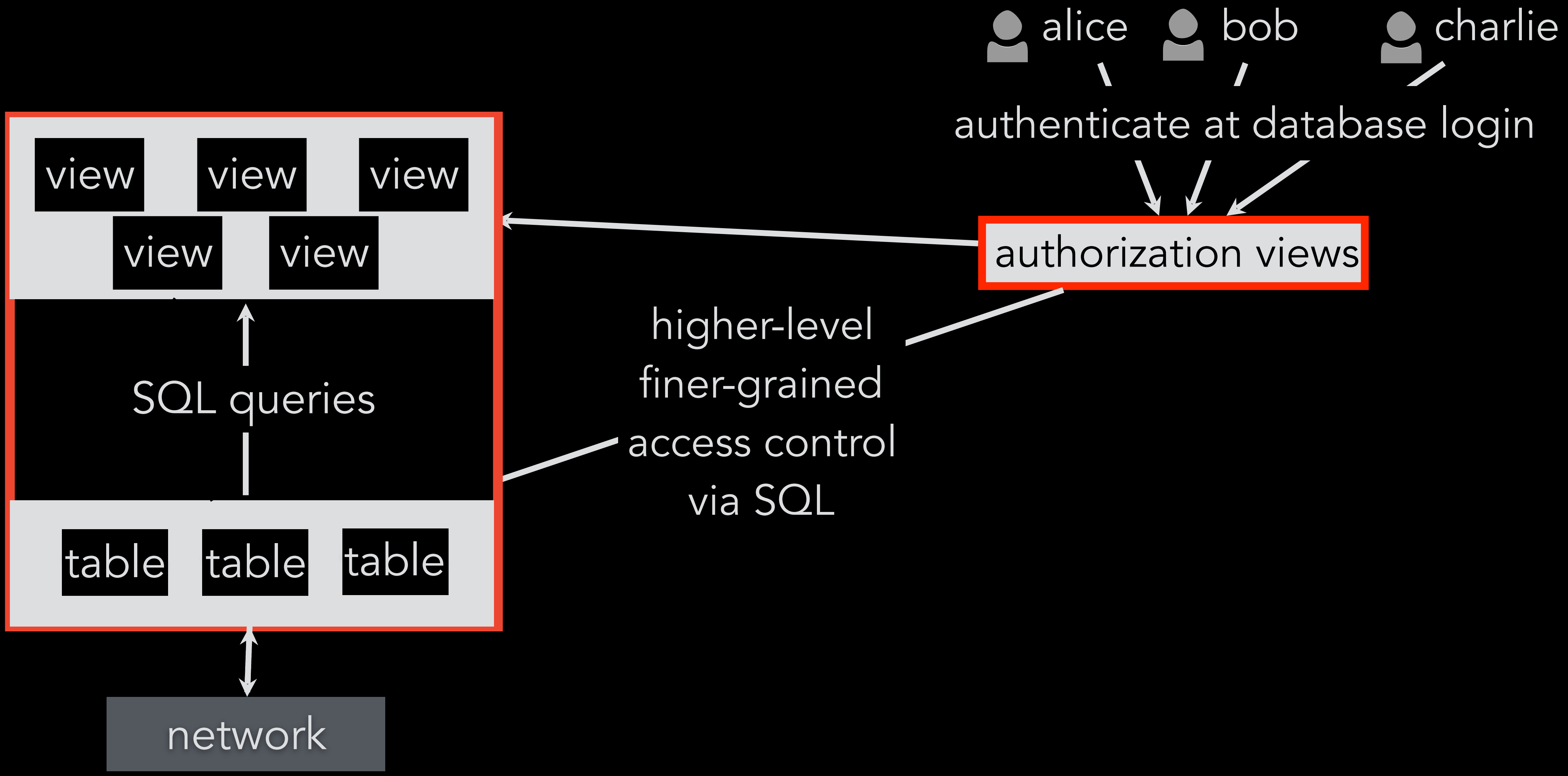
- Explicit specification (principal, object, privilege)

('alice', topology, insert)

- Manual, tedious
- Does not scale up

Our approach: ACL in Ravel

- Access control



Higher-level, finer-grained

- Advantages

Higher-level, finer-grained

- Advantages
  - dynamic

Higher-level, finer-grained

- Advantages
  - dynamic
  - content-based

Higher-level, finer-grained

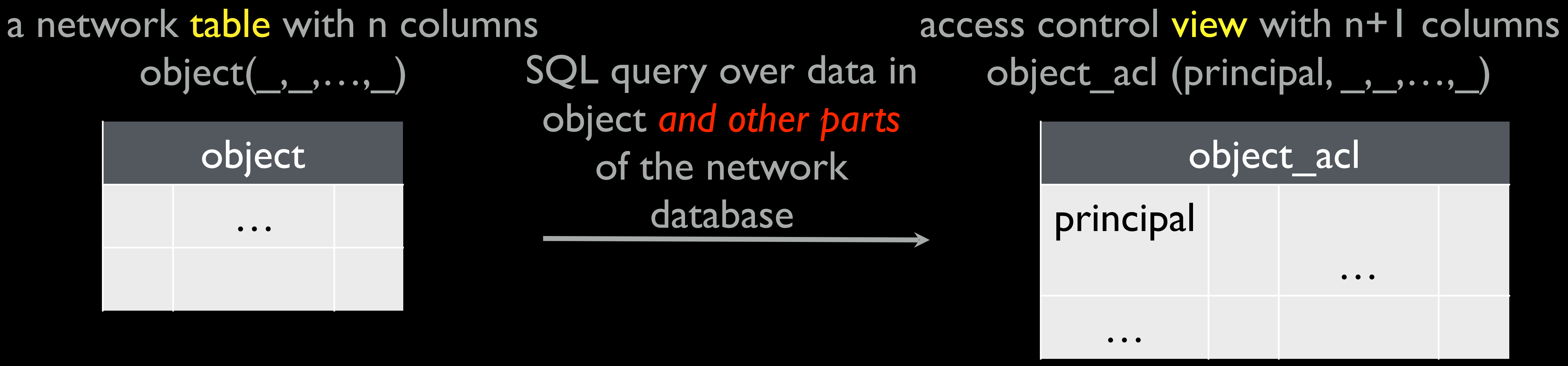
- Advantages
  - dynamic
  - content-based

} **intent** rather than **extent**

Higher-level, finer-grained

- Advantages
  - dynamic
  - content-based

} **intent** rather than **extent**



a network **table** with n columns
object(_,_,…,_)

	object	
	…	

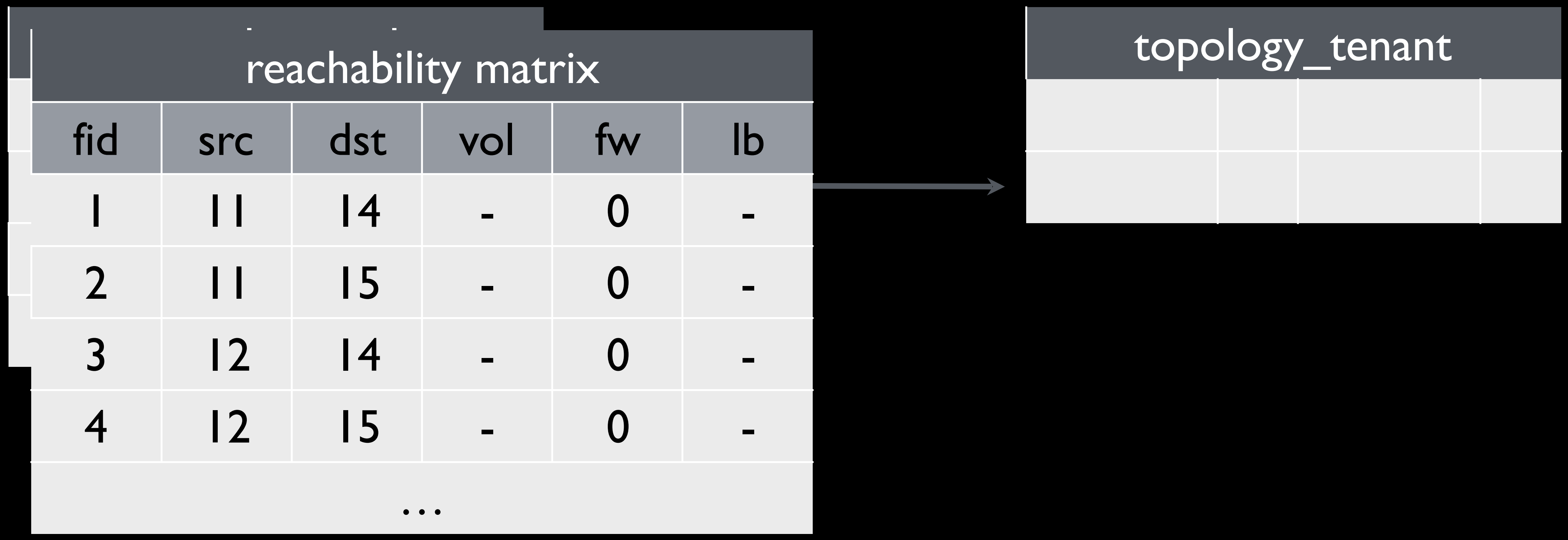
SQL query over data in object *and other parts* of the network database

access control **view** with n+1 columns
object_acl (principal, _,_,…,_)

object_acl			
principal		…	
…			

Enforcing Access Control

access control view
topology_acl(principal, _,_,…,_)



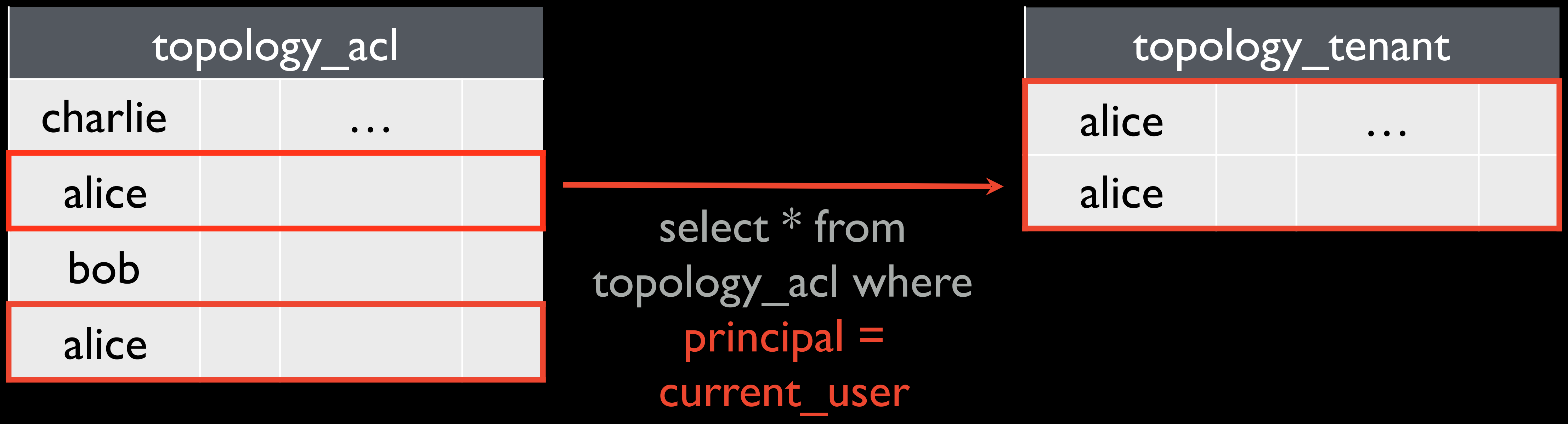
reachability matrix

fid	src	dst	vol	fw	lb
1	11	14	-	0	-
2	11	15	-	0	-
3	12	14	-	0	-
4	12	15	-	0	-
…					

topology_tenant

Enforcing Access Control

access control view
topology_acl(principal, _,_,…,_)



topology_acl			
charlie		…	
alice			
bob			
alice			

select * from topology_acl where principal = current_user

topology_tenant			
alice		…	
alice			

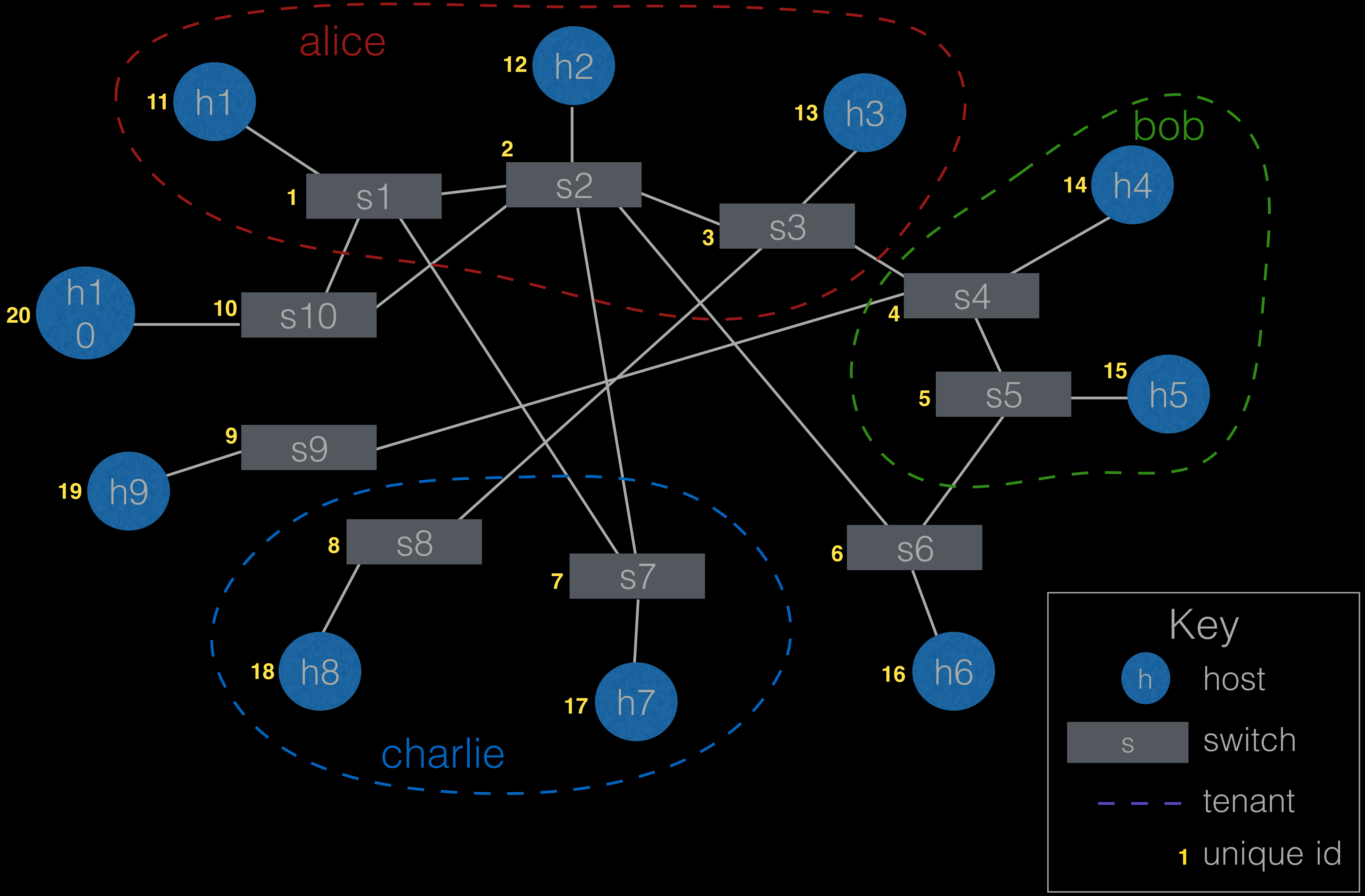
Code

```
CREATE OR REPLACE VIEW topology_acl AS (
    ( SELECT ‘admin’ AS principal, sid, nid FROM tp )
    UNION
    ( SELECT s.name AS principal, sid, nid FROM tp, sla s
        WHERE tp.sid IN (SELECT nodeid FROM sla WHERE name=s.name)
        AND tp.nid IN (SELECT nodeid FROM sla WHERE name=s.name) )
);

CREATE OR REPLACE VIEW topology_public AS (
    SELECT sid, nid FROM topology_acl
    WHERE principal = current_user);

GRANT SELECT ON topology_public TO PUBLIC;
```

Demo


alice
bob
charlie
11
h1
12
h2
13
h3
14
h4
15
h5
16
h6
17
h7
18
h8
19
h9
20
h1
0
1
s1
2
s2
3
s3
4
s4
5
s5
6
s6
7
s7
8
s8
9
s9
10
s10
Key
h
host
s
switch
tenant
1
unique id

Conclusion

- SDN: Programming networking with software via a centralized controller

Conclusion

- SDN: Programming networking with software via a centralized controller
- Ravel: a database controller

Conclusion

- SDN: Programming networking with software via a centralized controller
- Ravel: a database controller
- Security: an important, but less-visited aspect

Conclusion

- SDN: Programming networking with software via a centralized controller

- Ravel: a database controller

- Security: an important, but less-visited aspect

- This project: Adding access control to a database controller for SDN

References

Ravel: A Database-Defined Network. Wang, A., Mei, X., Croft, J., Caesar, M., & Godfrey, B. (2016). In The Symposium on SDN Research (SOSR)

Olson, L. E., Gunter, C. A., Cook, W. R., & Winslett, M. (2009, July). Implementing reflective access control in SQL. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 17-32). Springer Berlin Heidelberg.

Casado, M., Garfinkel, T., Akella, A., Freedman, M. J., Boneh, D., McKeown, N., & Shenker, S. (2006, August). SANE: A Protection Architecture for Enterprise Networks. In Usenix Security.

Porras, P., Shin, S., Yegneswaran, V., Fong, M., Tyson, M., & Gu, G. (2012, August). A security enforcement kernel for OpenFlow networks. In Proceedings of the first workshop on Hot topics in software defined networks (pp. 121-126). ACM.

http://github.com/ravel-net/REU-access-control