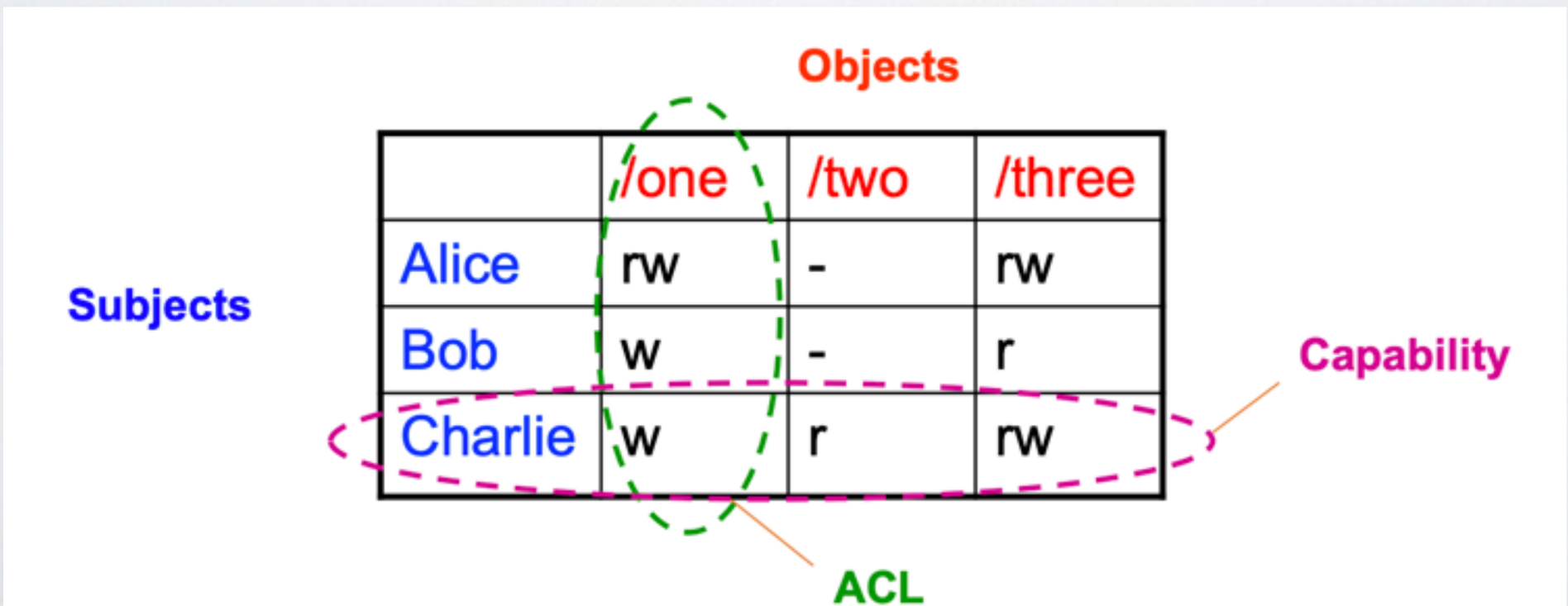
Representing Protection

Access Control Lists (ACL)
For each object, maintain a list of subjects and their permitted actions

Capabilities
For each subject, maintain a list of objects and their permitted actions



ACLs and Capabilities

Approaches differ only in how the table is represented

➡ Capabilities are easier to transfer
They are like keys, can handoff, does not depend on subject

➡ But ACLs are easier to manage in practice

- Object-centric, easy to grant, revoke
- To revoke capabilities, have to keep track of all subjects that have the capability – a challenging problem

ACLs have a problem when objects are heavily shared

- The ACLs become very large
- Use groups (e.g. Unix)