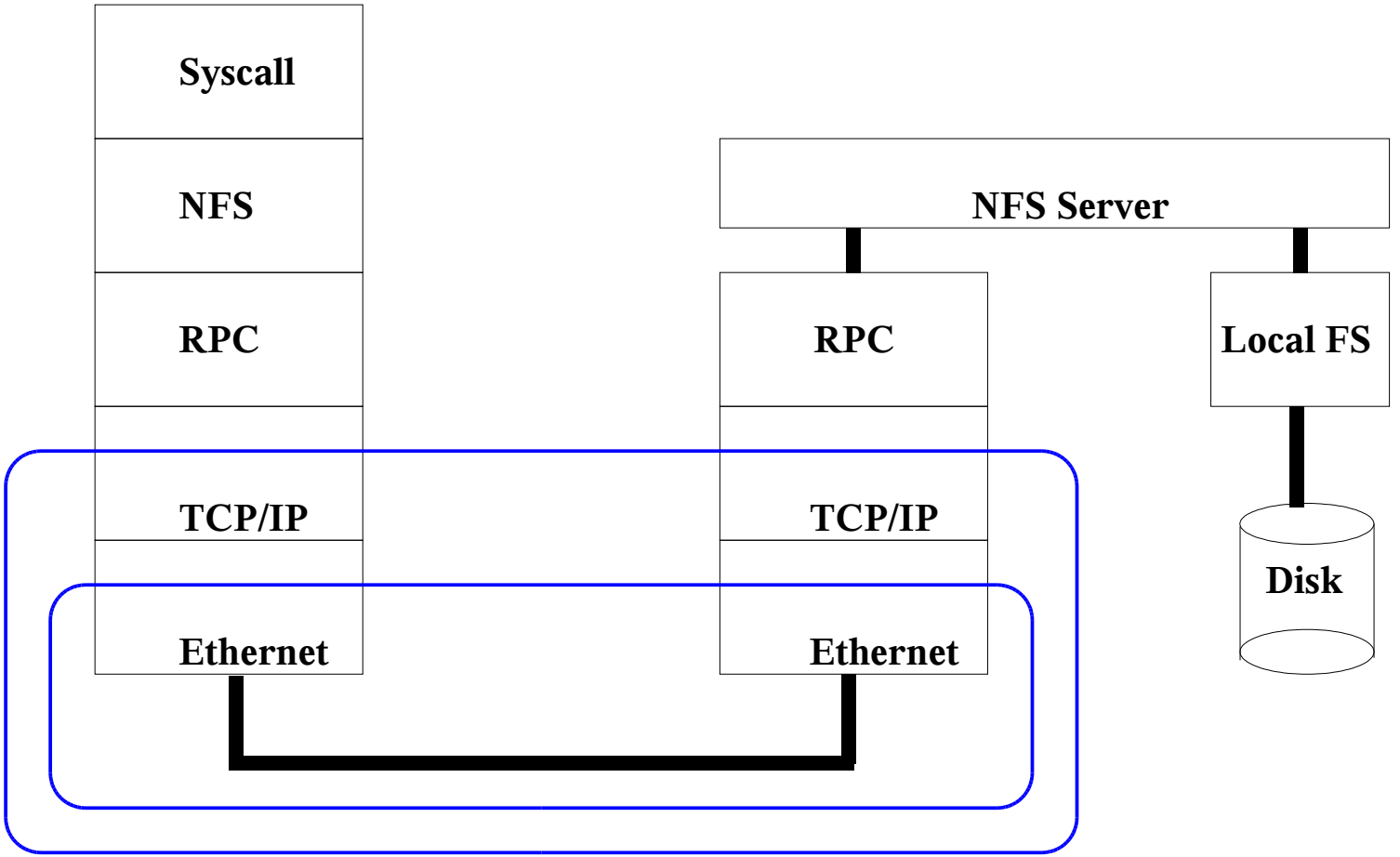
NFS Data Integrity

Without krb5i



NFS Data Integrity

Without krb5i

- Reliance on TCP checksums
  - Standard checksum is one's complement of 16bit integers
    - Designed for speed, byte order independence
    - Weak in the face of single bit errors
    - Weak in it's ability to detect transposition of octets/words in a datagram
  - Alternate checksum algorithm optional
    - Never really took off, not widely implemented

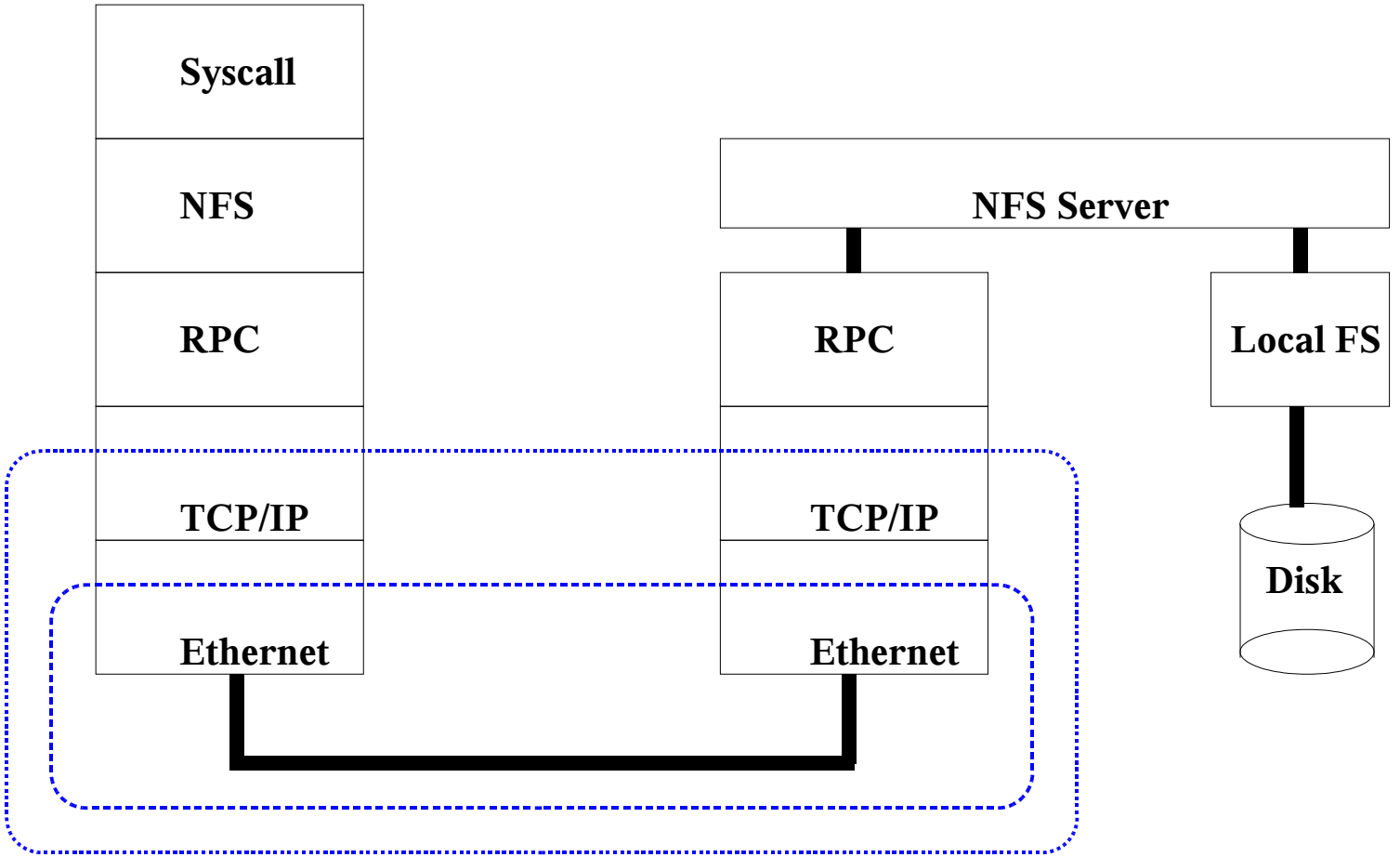
NFS Data Integrity

Without krb5i

- Reliance on Ethernet checksums
  - CRC32 used as the standard checksum
    - Efficient in error detection and error correction
    - Downside is it's not end-to-end and gets re-computed at every hop

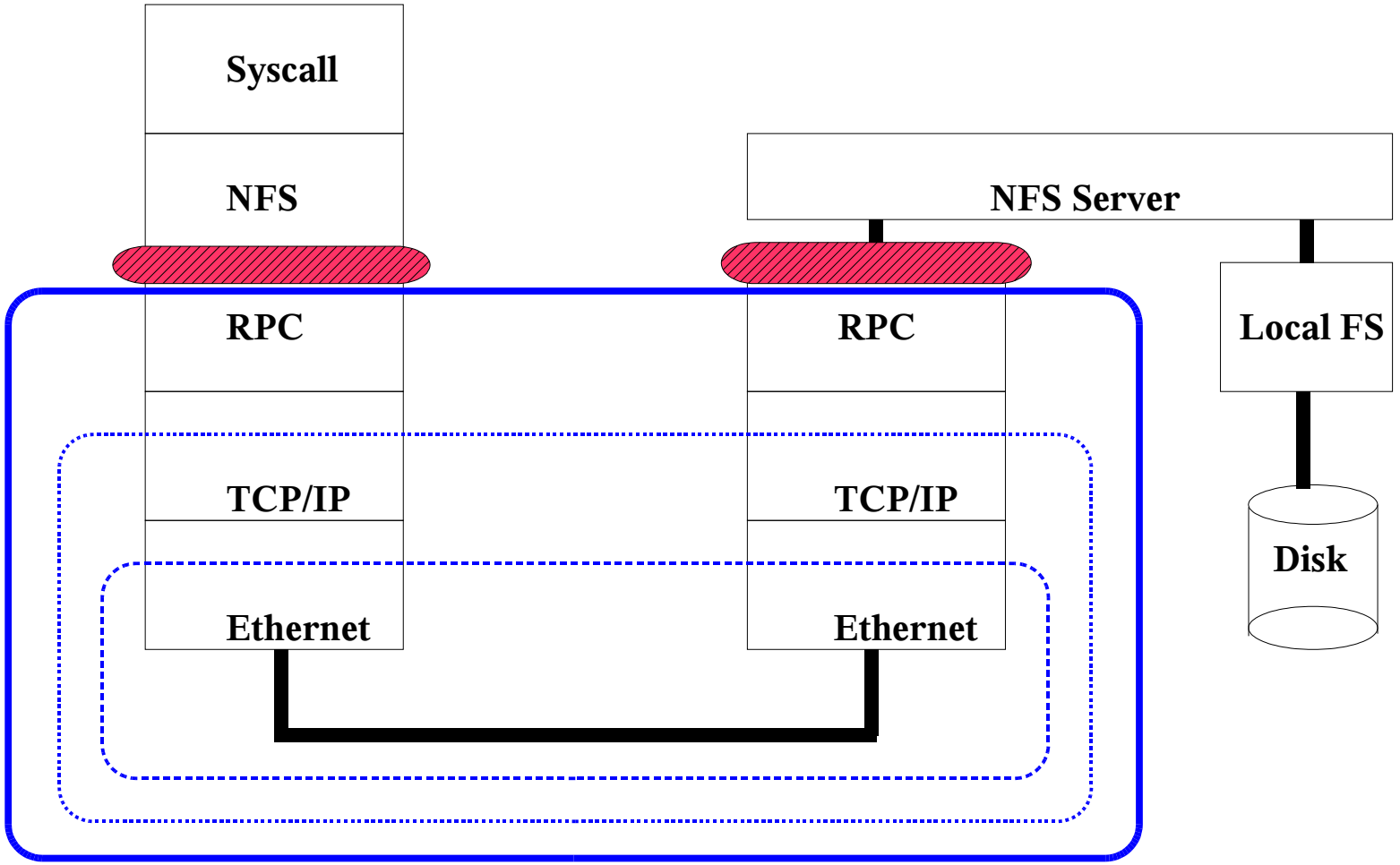
NFS Data Integrity

What are we left with – Not Much!



NFS Data Integrity

With krb5i



NFS Data Integrity

With krb5i

- Entire RPC payload protected
  - Strong protection
- Data is vulnerable after its decoded
  - No Integration between the NFS and the RPC layer
- Kerberos needs to be configured!

Checksums for NFSv4

End-to-End Integrity