Certificates

- Solving the public key distribution problem
- Trust (having somebody's public key) is transitive
  - A trusts C and B trusts C
    ⇒ A can establish trust with B

- Where to start?
  - who to trust
  - how is the initial trust established
- Solution: **Certificate Authority (CA)**

Certificates

Goal: A wants to prove its identity to B

Given: A and B trust CA and both have CA's public key

Broad approach: ***Public key certificate***

- A's public key encrypted with CA's private key (ensures integrity of the key)
- … plus additional information

Use: A presents its certificate when initiating communication with B

Certificates - Questions

Man in the Middle Attack: How does B know that it is A's certificate and not an impostor's one?

- Include A's human-readable identification

Replay Attack: Attacker overhears/requests A certificate and presents it when pretending to be A

- Use nonce encrypted with A's public key during communication

Compromised certificate: Either A's or CA's private keys are compromised

- Limited validity and certificate revocation

Certificates - Issuance

- A generates public/private key pair
- A sends its public key to CA (certificate signing request)
- CA verifies A's identity (hopefully)
- CA generates the certificate and sends it to A

Network Management

- Networks are complicated...
- Targets of management:
  - configuration
  - faults
  - performance
  - security
  - accounting

Network Management

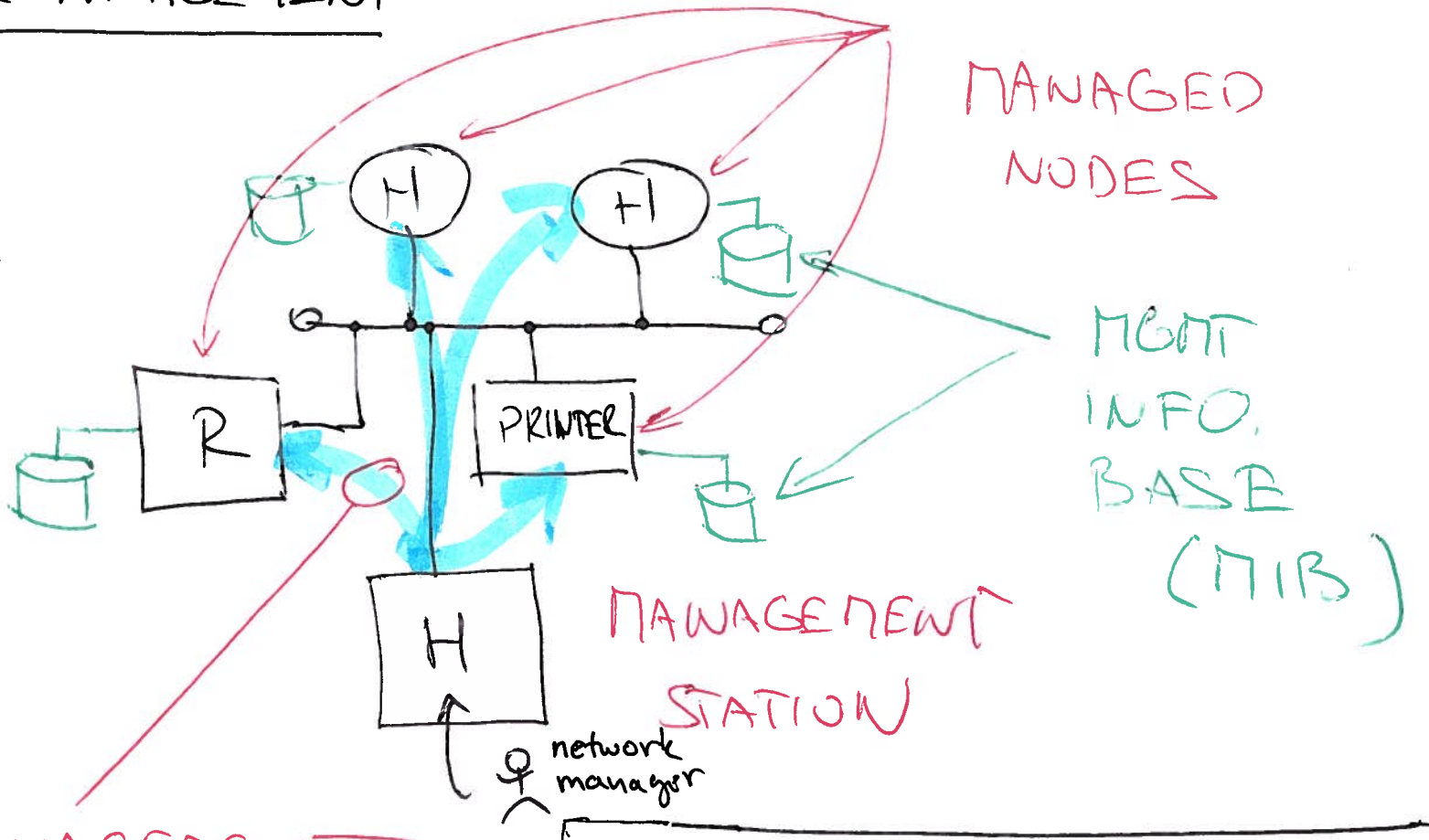
- Two aspects of management
  - information collection and dissemination
  - decision making

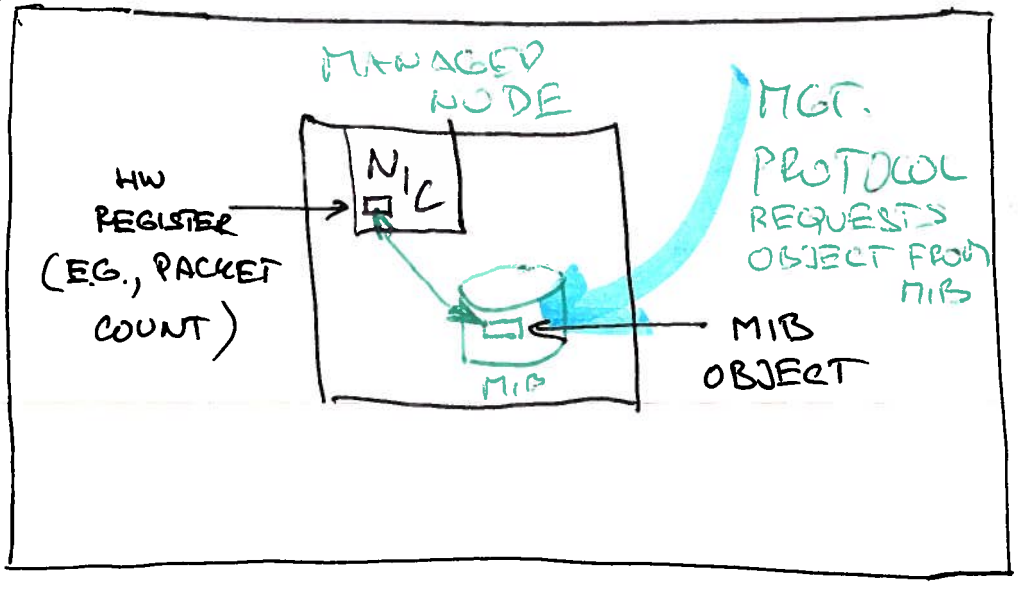
- Components:
  - managed node
  - management station
  - management protocol
  - management information base (MIB)

NETWORK MANAGEMENT

H host

R router





Management Protocols

- Simple Network Management Protocol (SNMP)
  - another “simple” protocol...
  - polling and trapping
  - data representation (ASN.1)
  - object identifiers (OIDs)
- OID Example
  - iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) ip(4) ipInReceives(3)
  - 1.3.6.1.2.1.4.3