CS 725/825 & IT 725

Lecture 13

Network Management Transport Layer

October 21, 2026

Certificates

- Goal: A wants to prove its identity to B
- Given: A and B trust CA (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 identification (hostname, human-readable info)
- Replay Attack: Attacker overhears/requests A certificate and presents it when pretending to be A
  - Use nonce encrypted with A's private key during communication
- Compromised certificate: Either A's or CA's private keys are compromised
  - Limited validity and certificate revocation

Certificates - Issuance

- A gets a certificate from a CA
  - A generates public/private key pair
  - A generates a Certificate Signing Request (CSR)
  - CA (hopefully) makes sure that it interacts with A and not an impostor
  - CA encrypts the certificate (public key + A's identification + ...) with its own private key
  - certificate is delivered to A (can be done securely since A has CA's public key)

Certificates - Use

- B authenticates A
  - B requests a certificate from A together with a nonce
  - A sends back the certificate together with the nonce encrypted with A's private key
  - B decrypts the certificate with CA's public key and verifies that it was issued to A
  - B decrypts the nonce using A's public key and verifies that the value matches the value sent

Network Management

Network Management

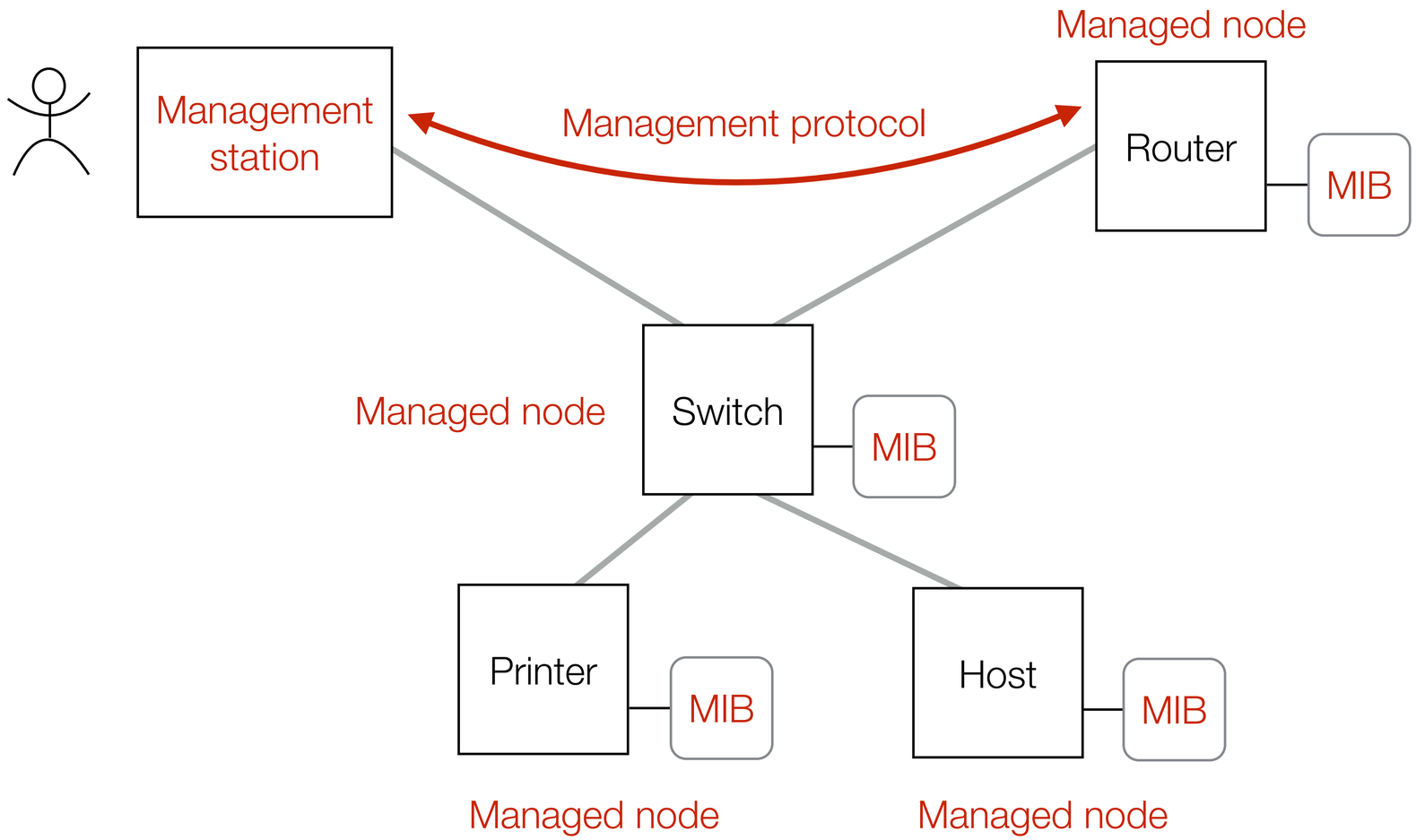
- Networks are complicated...
- Targets of management:
  - configuration
  - faults
  - performance
  - security
  - accounting

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



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

NETCONF

- Network Configuration Protocol (NETCONF)
  - "provides mechanism to install, manipulate, and delete the configuration of network devices." (RFC 6241)
  - XML-based, realized as remote procedure calls (RPC)
  - underlying transport must provide authentication and authorization
  - a NETCONF implementation must support ssh transport
- YANG
  - data modeling language
  - describes data structures, data integrity constants, and data operations
  - *…Yet Another Next Generation*

Transport Layer

Transport Layer

- Big leap in the level of abstraction:
  - Application Layer: reliable, bidirectional, stream-oriented service
  - Network Layer: unreliable datagram service
- End-to-End Principle
  - as simple as possible network
  - all “smarts” at the end nodes

Functions of Transport Layer

- Addressing
  - port numbers (?)
- Error control
  - packet loss detection and retransmissions
- Flow and congestion control
  - controlling the transmission rate
- Session management