**SAN: Access Control and Management**

---

**What is it?**
- A form of higher level network design.
- Managing quality of service (QoS) and some aspects of security.
- Controlling which nodes can:
  - enter a SAN.
  - communicate with each other and in what way.
  - access select network resources.

---

**Why is it needed?**
- Only permitted nodes should be capable of entering the network (authentication).
- Some nodes may not be considered trustworthy by others (trusted nodes).
- Not all network services may be free (resource access control).
- Certain resources (e.g. audio) may require a specific minimum level of QoS.

---

**Quality of service (QoS)**
- Maximising QoS becomes an even greater issue with a medium prone to burst errors.
- QoS is measured in terms of:
  - Link reliability, saturation and latency.
  - Security levels.
- Using this information, routes with QoS best suited to specific needs can be selected.

**Assessing Latency:**
- Simple heuristic to size packets: lower reliability, smaller packets; higher reliability, larger packets.

---

**Node authentication**
- The process of verifying that a node is what it claims to be.
- Important since only authenticated nodes should be valid SAN participants.
- Each node is assigned a serial number and authentication key that uniquely identify it.
- These are stored at each node and known also to administration nodes.
- When a node first enters, the following one-off procedure occurs: Node B receives master authentication capability. Only Nodes C and E are reachable by Node A.

---

**Resource access control**
- There are six prototype resource types (audio/video/gateway/generic data, bandwidth, authentication).
- Using a capability model, each node has a set of capabilities used to access resources.
- Capabilities for each resource type include:
  - Resource propagation.
  - Propagation spread (that is, the ability to propagate the propagation capability).

**Security level management**
- Nodes may dynamically specify levels of security. Levels may be set:
  - On an end-to-end basis (per resource type, or at the application level).
  - On a node-to-node basis.
- Levels are agreed upon using negotiations.

---

**Trusted and untrusted nodes**
- Each node maintains a list of other nodes that are considered trustworthy.
- Data can only be sent to/received from other trusted nodes.
- Trust status is not applicable when forwarding data on behalf of another node.

---

**Management databases**
- The setting and storing of run-time parameters is crucial to network management.
- Each node maintains a set of small management databases (security levels, trusted nodes, capability related etc.).

---

**Future work**
- Test access control and management functionality with wireless network cards.
- Design SAN-specific protocols (i.e. audio, video, etc.).
- Extend the QoS implementation to include bandwidth allocation.
- Automate reactions to (possibly) malicious events.