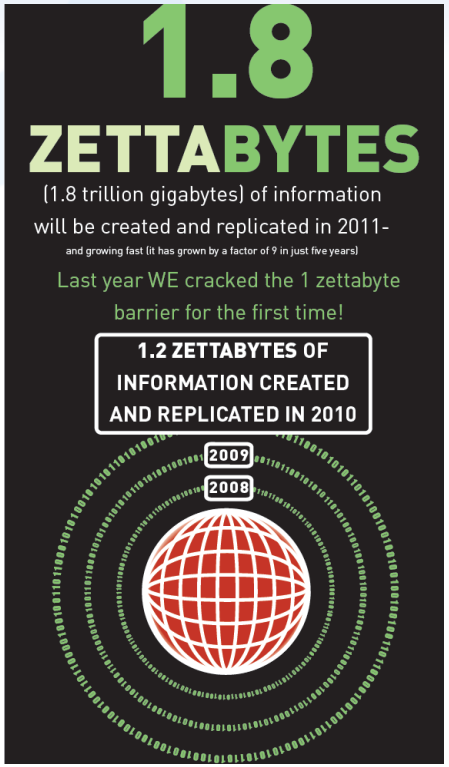
The Security Aspects of Cirrostratus Private Cloud Storage

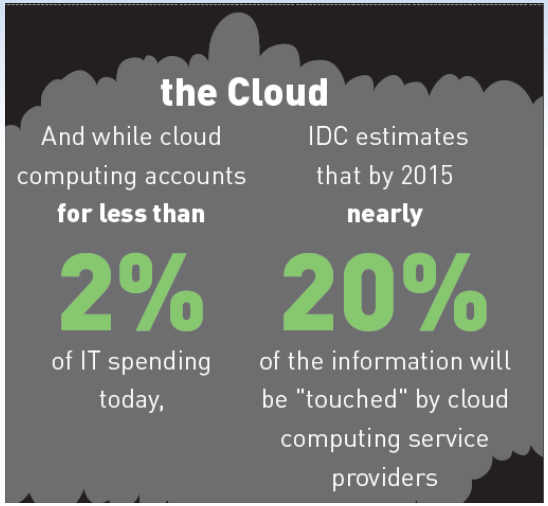
Vitaly Petrov, MSc student

Department of Communications Engineering

Tampere University of Technology

Problem topicality

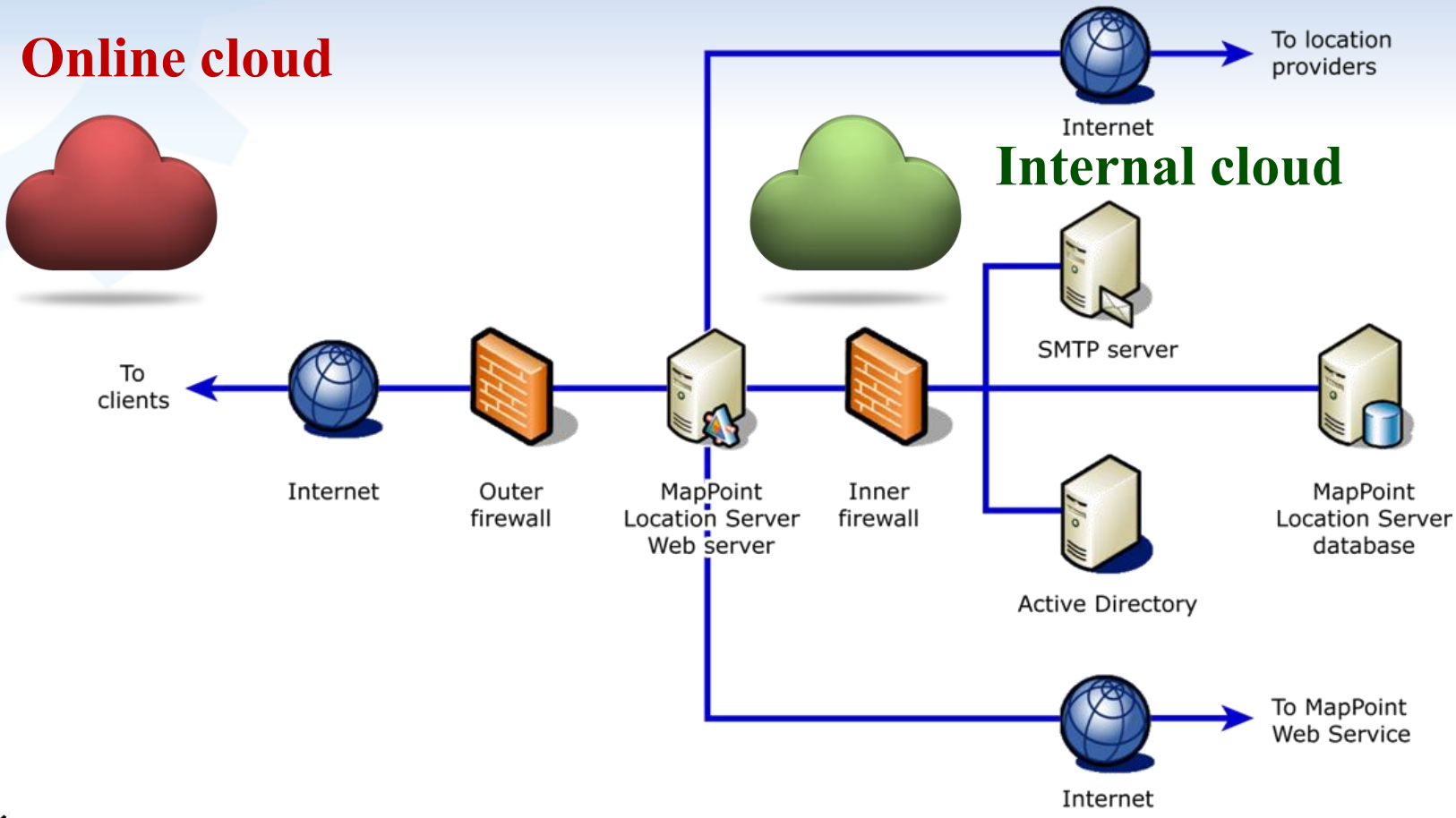




EMC Corporation, "EMC digital universe study", 2005

Cloud computing paradigm

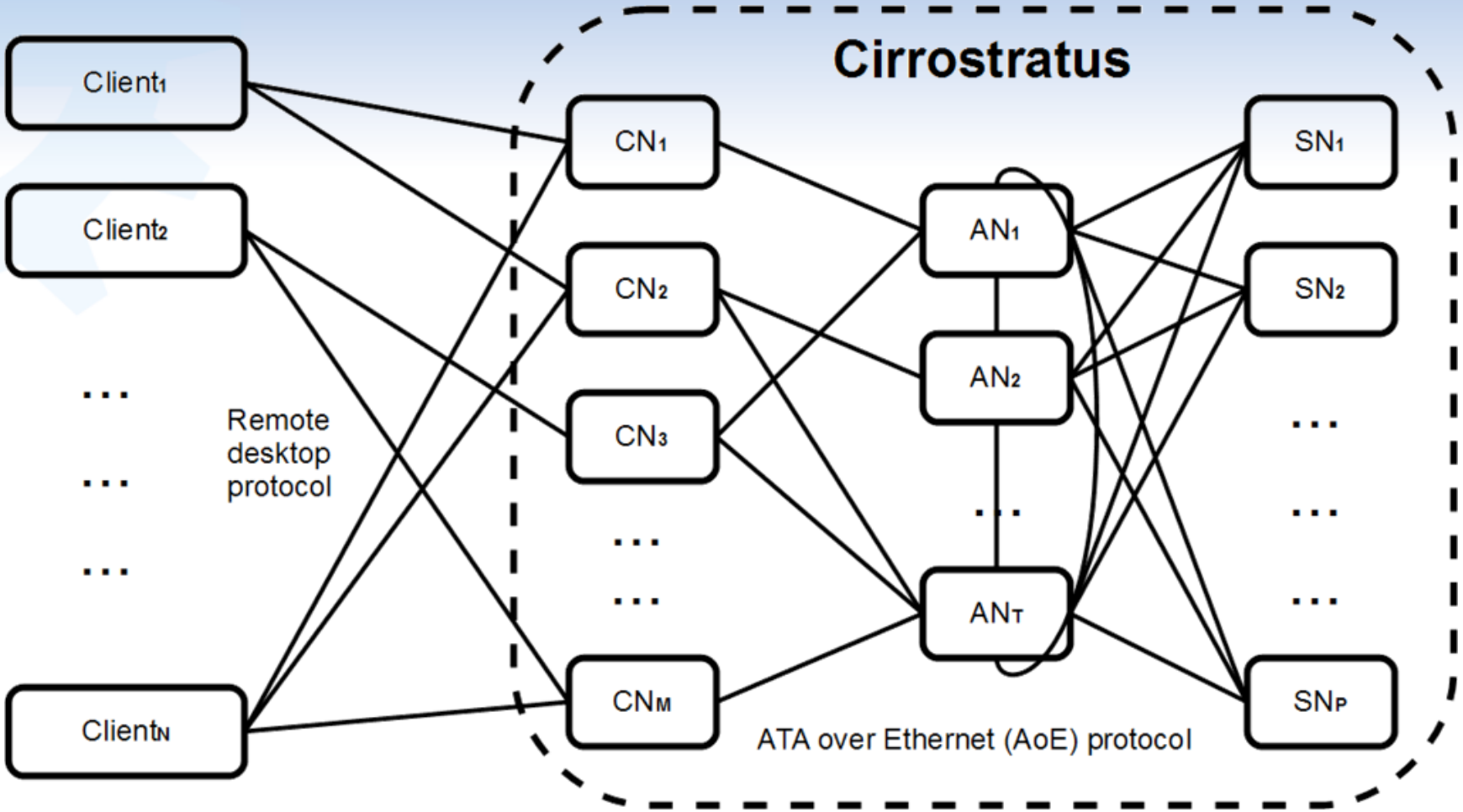
Clouds classification



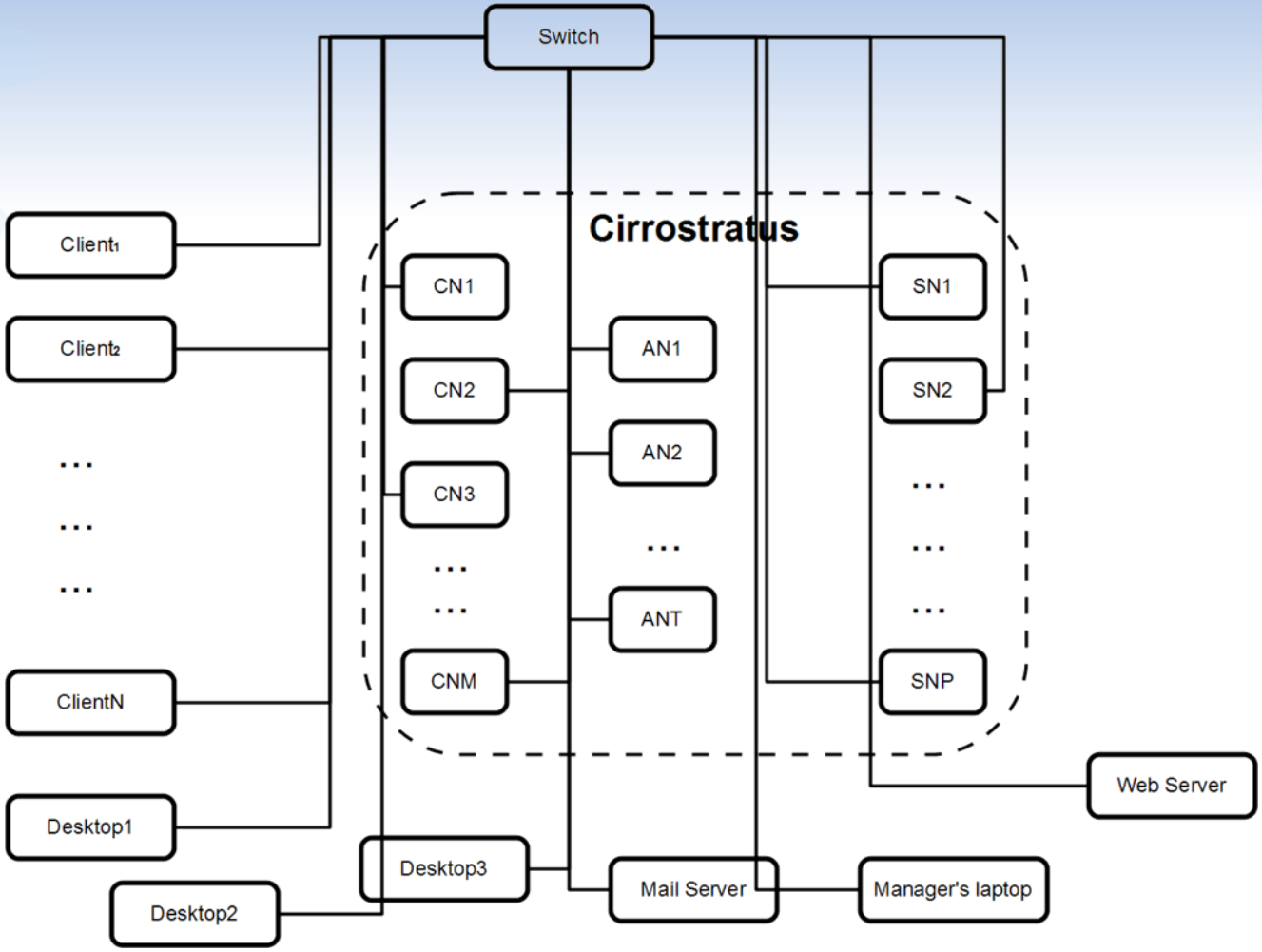
Internal cloud use cases

- Traffic limits
- Performance reasons
- Strong security level

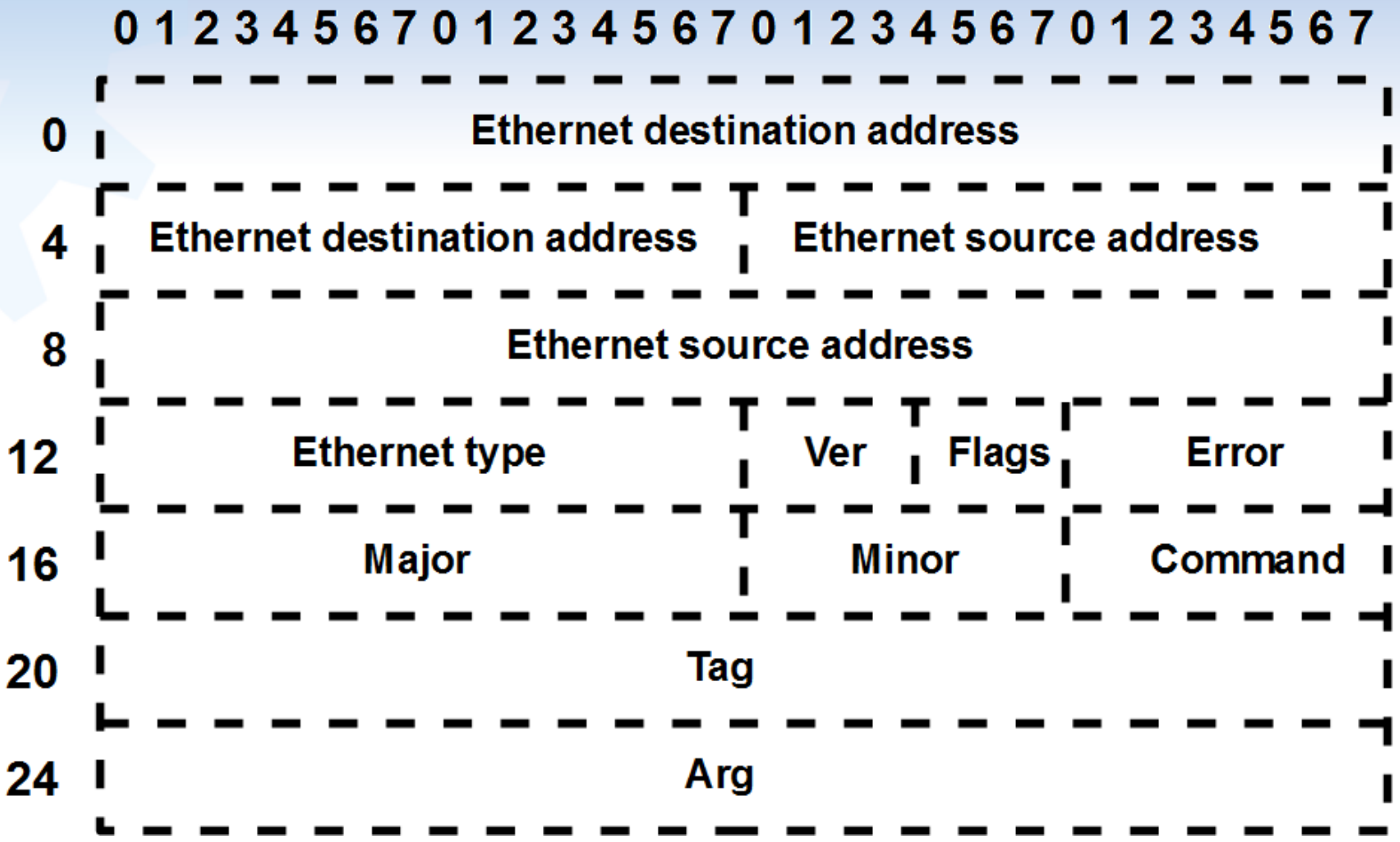
Cirrostratus cloud storage



Cirrostratus network map



AoE header

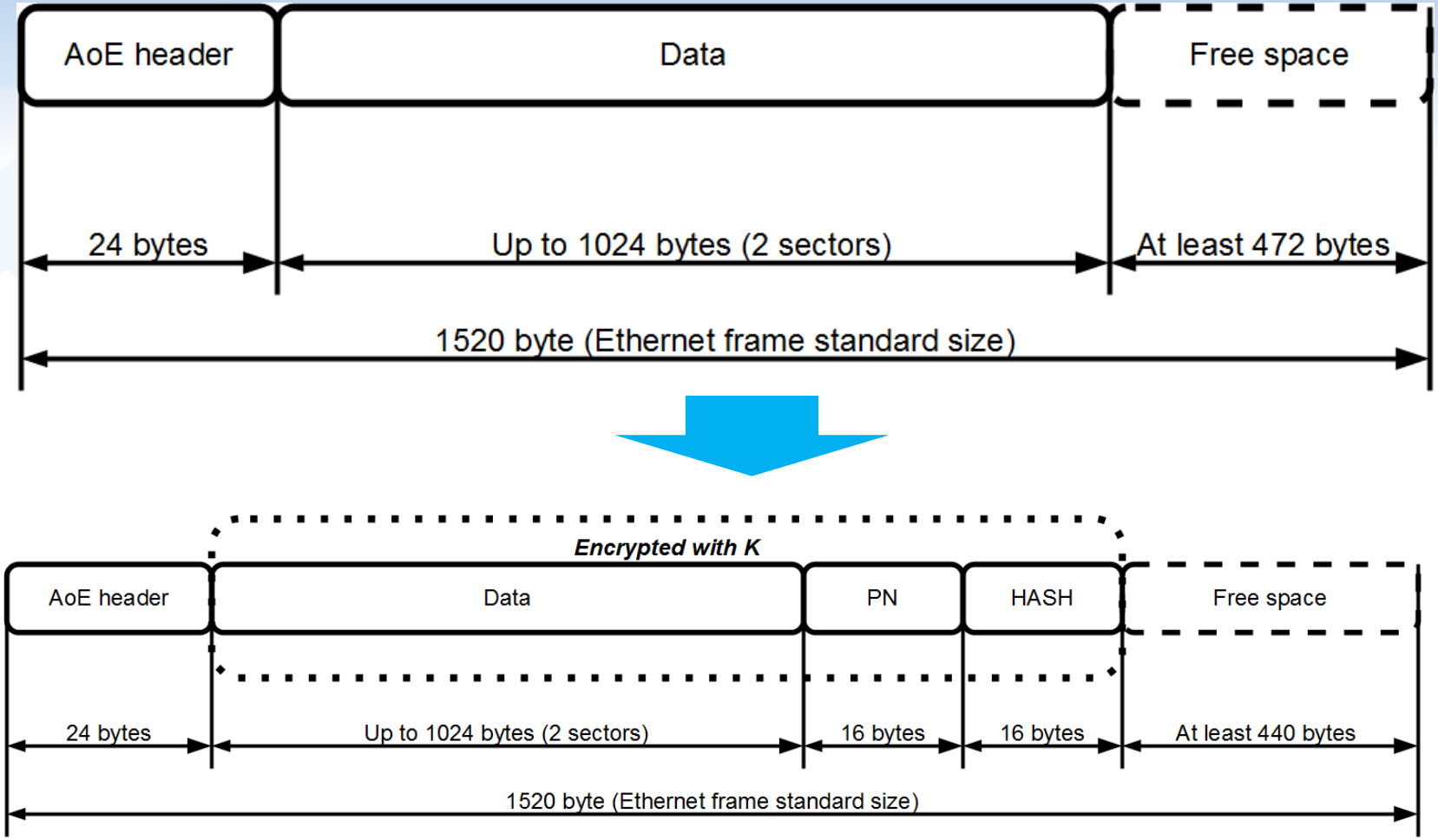

0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
0
Ethernet destination address
4
Ethernet destination address
Ethernet source address
8
Ethernet source address
12
Ethernet type
Ver
Flags
Error
16
Major
Minor
Command
20
Tag
24
Arg

Considered attacks

- **Reply attack**
  - Retransmitting the captured packet
  - No sequence number
- **Unauthenticated disk access**
  - MAC address filter
  - No real authentication
- **Man-in-the-middle attack**
  - ARP-spoofing
  - Switch as a single point of failure
- ✓ **DOS attack**
  - Almost impossible in LAN

**C. Purvis, "Access over Ethernet: Insecurities in AoE", White paper, Security Assesment, 2006*

AoE security extension (1)



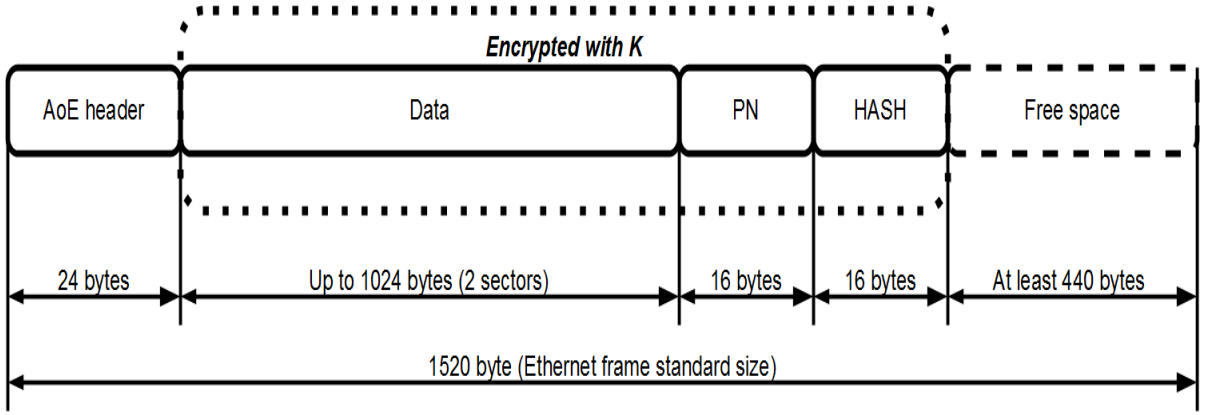
AoE security extension (2)

Signature:

1. Add packet number PN
2. Hash
3. Encrypt
4. Add AoE header
5. Send

Keys table

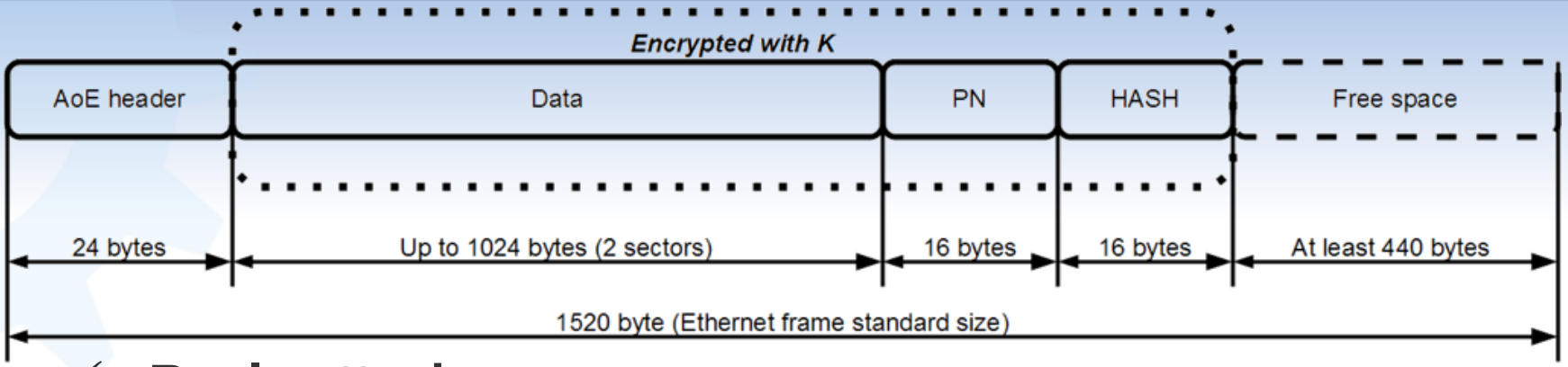
	ID 1	ID 2	ID 3
ID 1		Key 1-2	Key 1-3
ID 2	Key 1-2		Key 2-3
ID 3	Key 3-1	Key 3-2	



Verification:

1. Remove AoE reader
2. Decrypt
3. Chech the number
4. Check the hash value
5. Proceed

Proposed solution resistance to attacks



- ✓ **Reply attack**
  - Unique PN and Signature
- ✓ **Unauthenticated disk access**
  - Unique key for a pair of nodes
- ✓ **Man-in-the-middle attack**
  - Encryption
- ✓ **DOS attack**
  - Almost impossible in LAN

**C. Purvis, "Access over Ethernet: Insecurities in AoE", White paper, Security Assesment, 2006*

Conclusions

- ✓ **Results:**
  - AoE extension proposed
  - Resistance to major attacks highlighted

- ❑ **Research directions:**
  - Performance evaluation
  - Initialization procedure development