

**NIS/CpE 691CE**

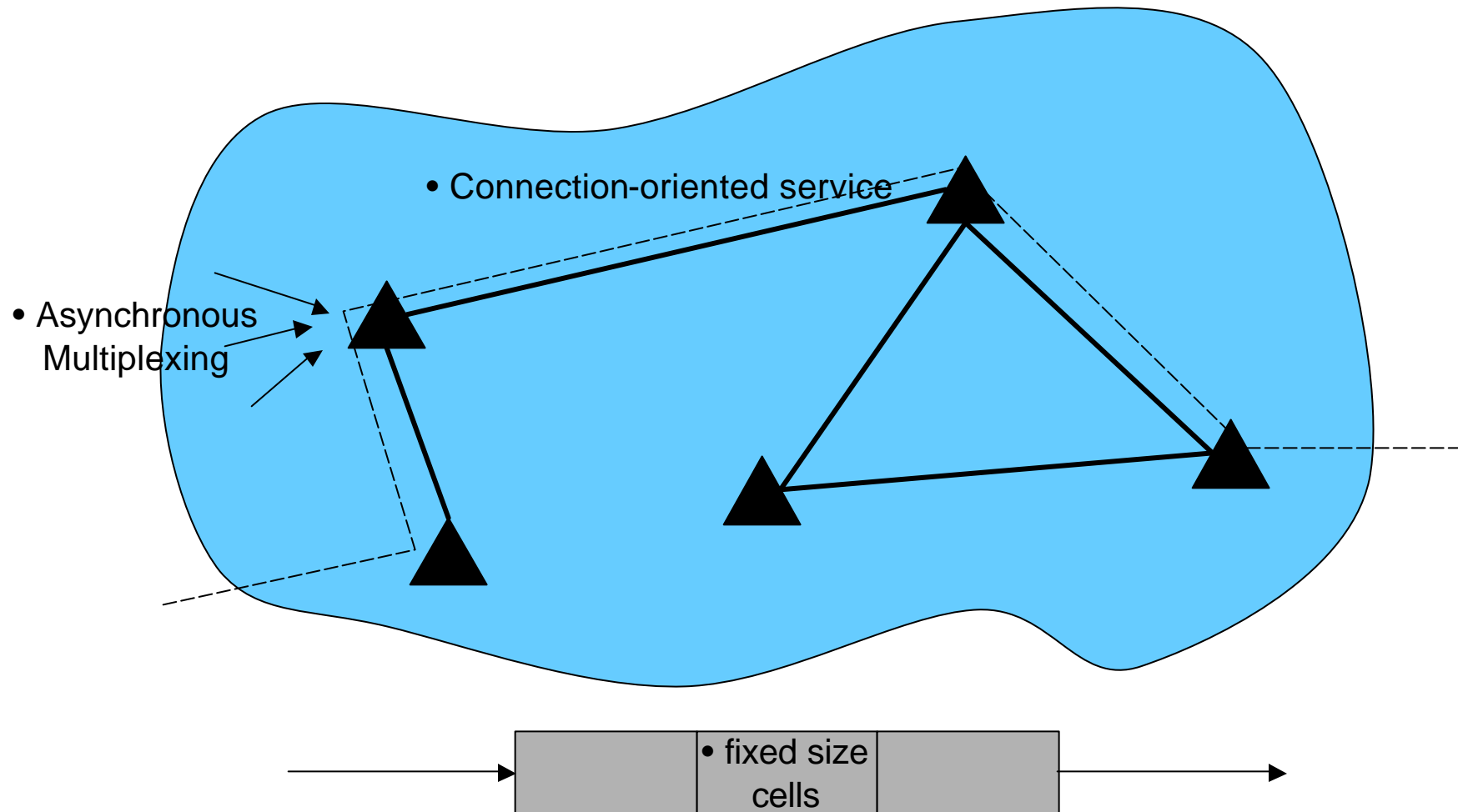
**Information System Security**

**Class 7 – 10/28/02**

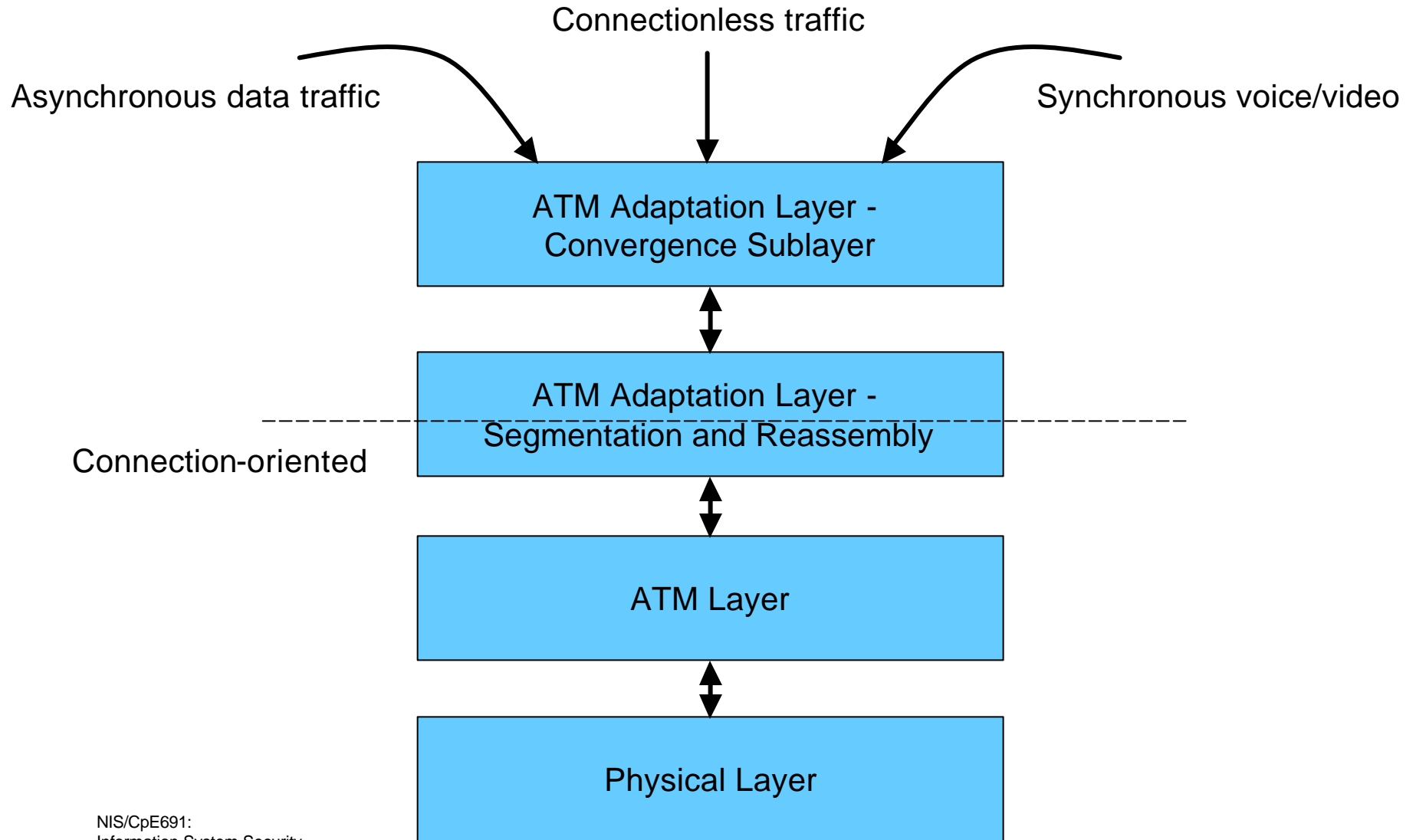
# Tonight's topics

- [Midterm review](#)
- Begin discussion of ATM networks (Ghosh, section 6.2)

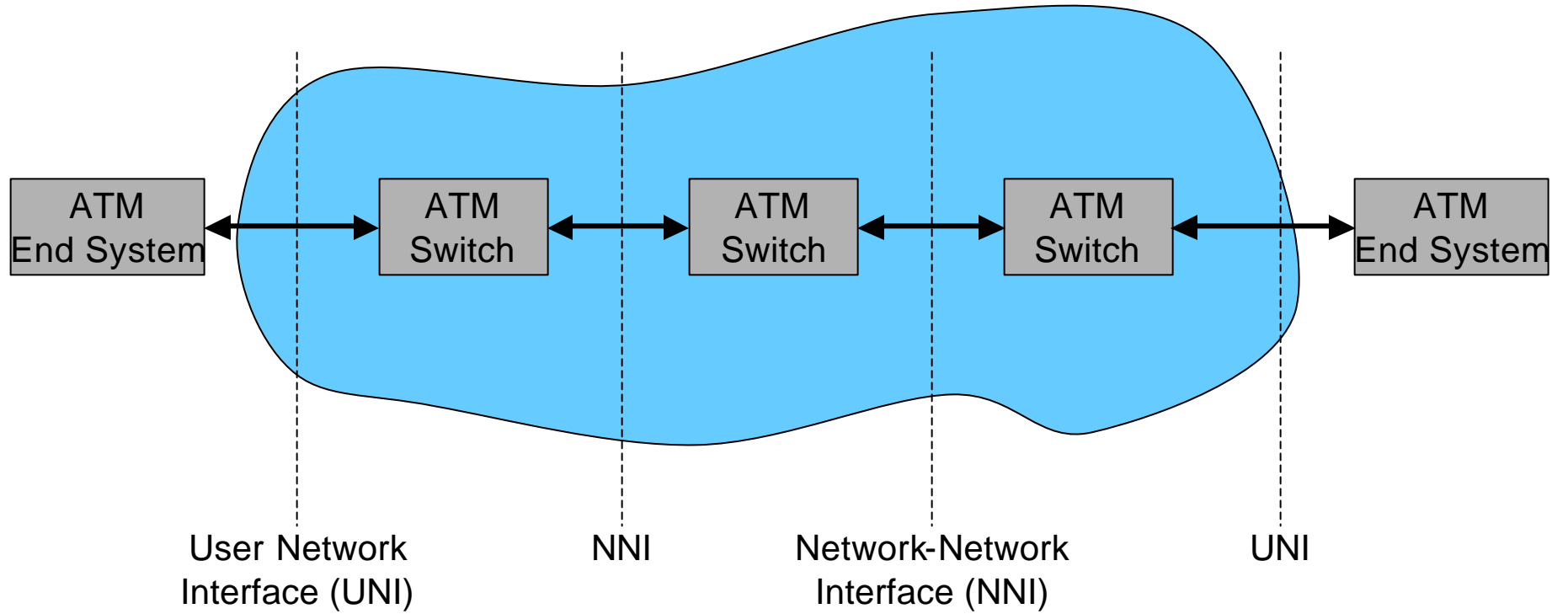
# Characteristics of ATM networks



# ATM layers



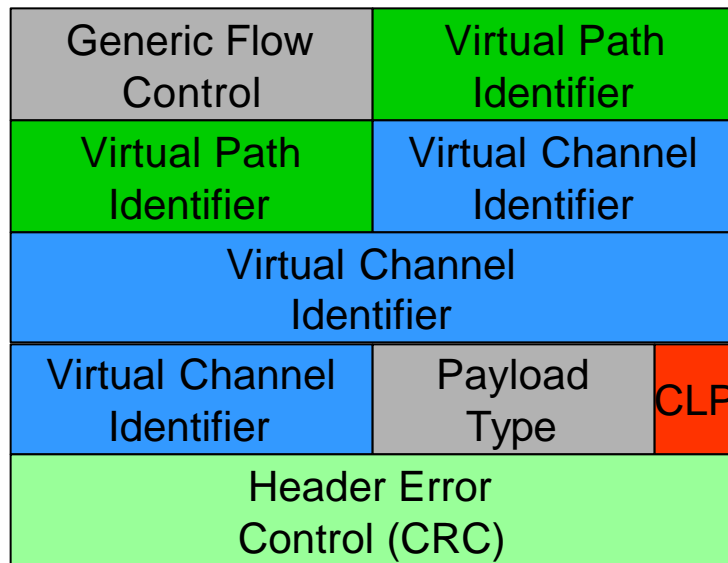
# ATM Network



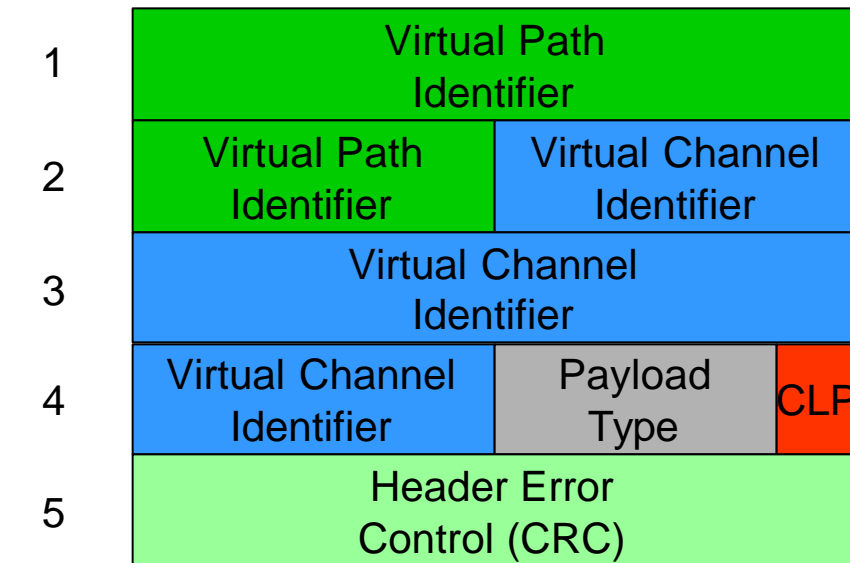
# ATM Cell



- Fixed size packets simplifies hardware
- Small packets reduce latency - 48 bytes is a compromise



UNI format



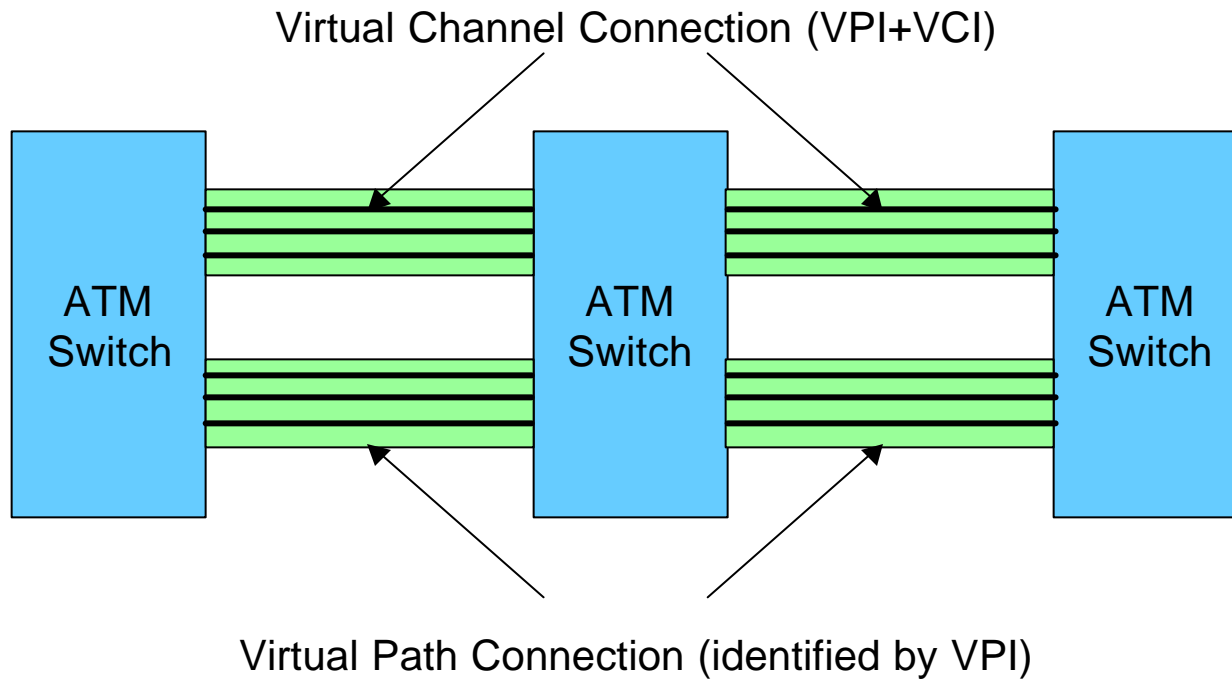
byte

NNI format

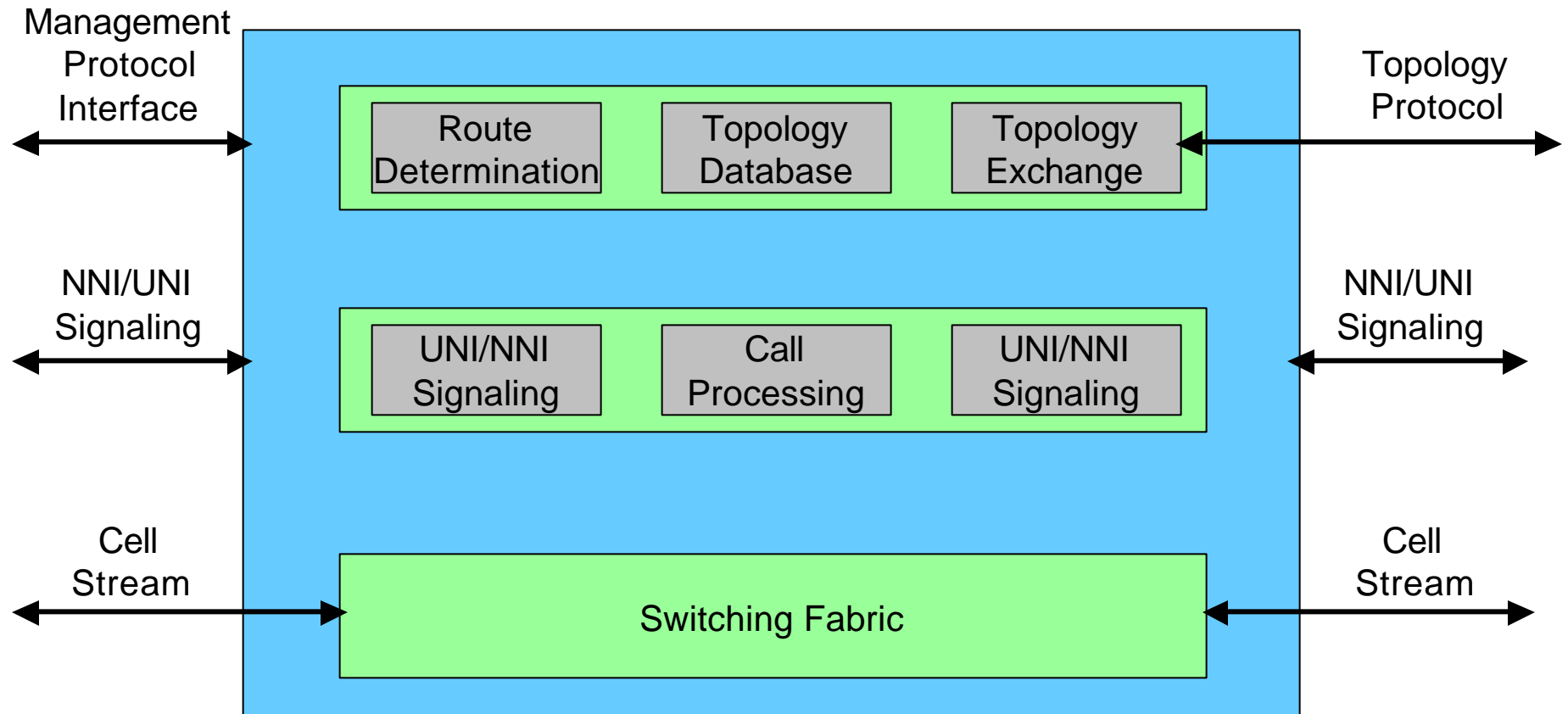
- Payload type signals user data vs. OAM
- During congestion, Cell Loss Priority=1 cells are discarded first

- NNI will generally require more paths, hence more VPI bits.

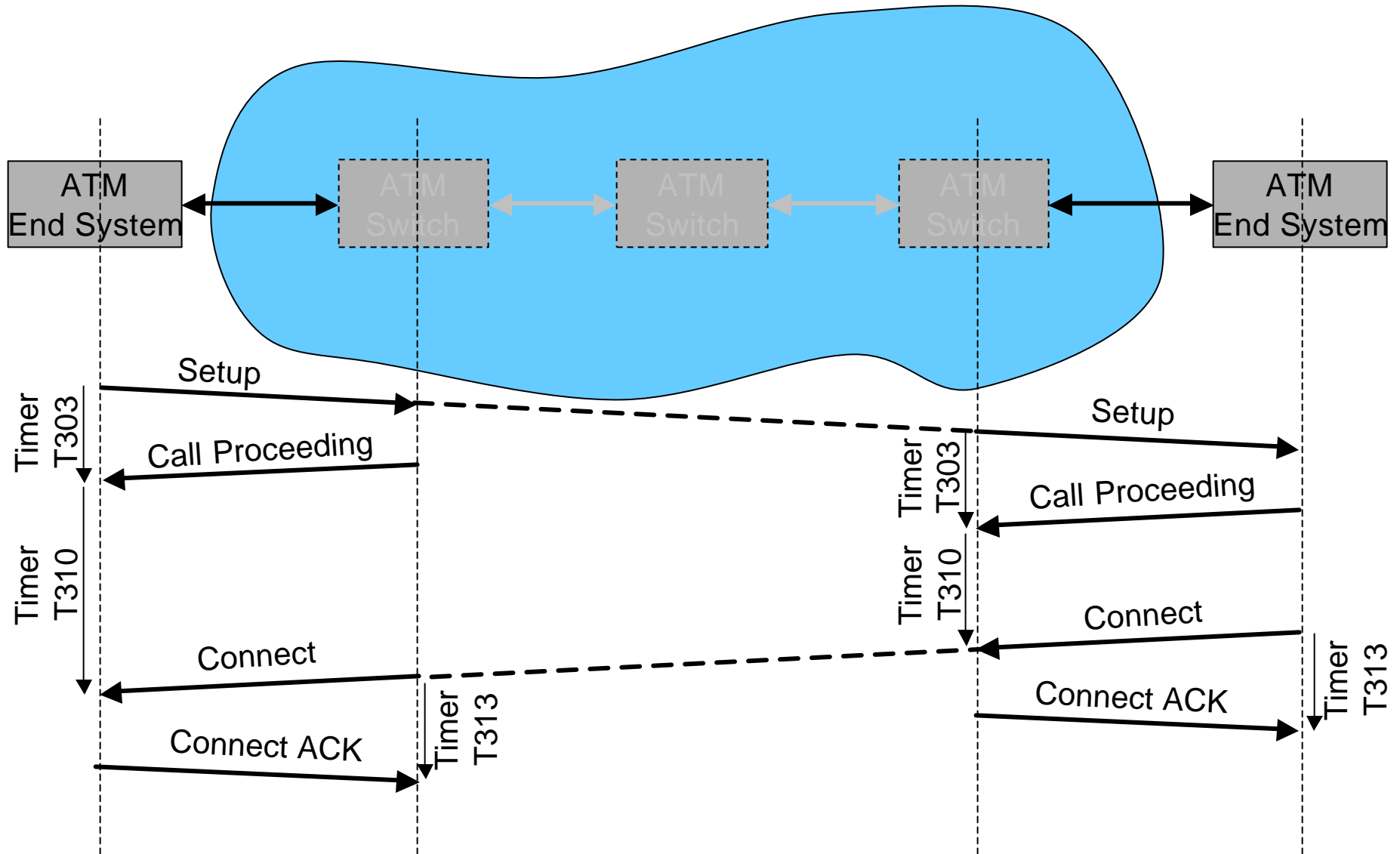
# ATM Virtual Connections



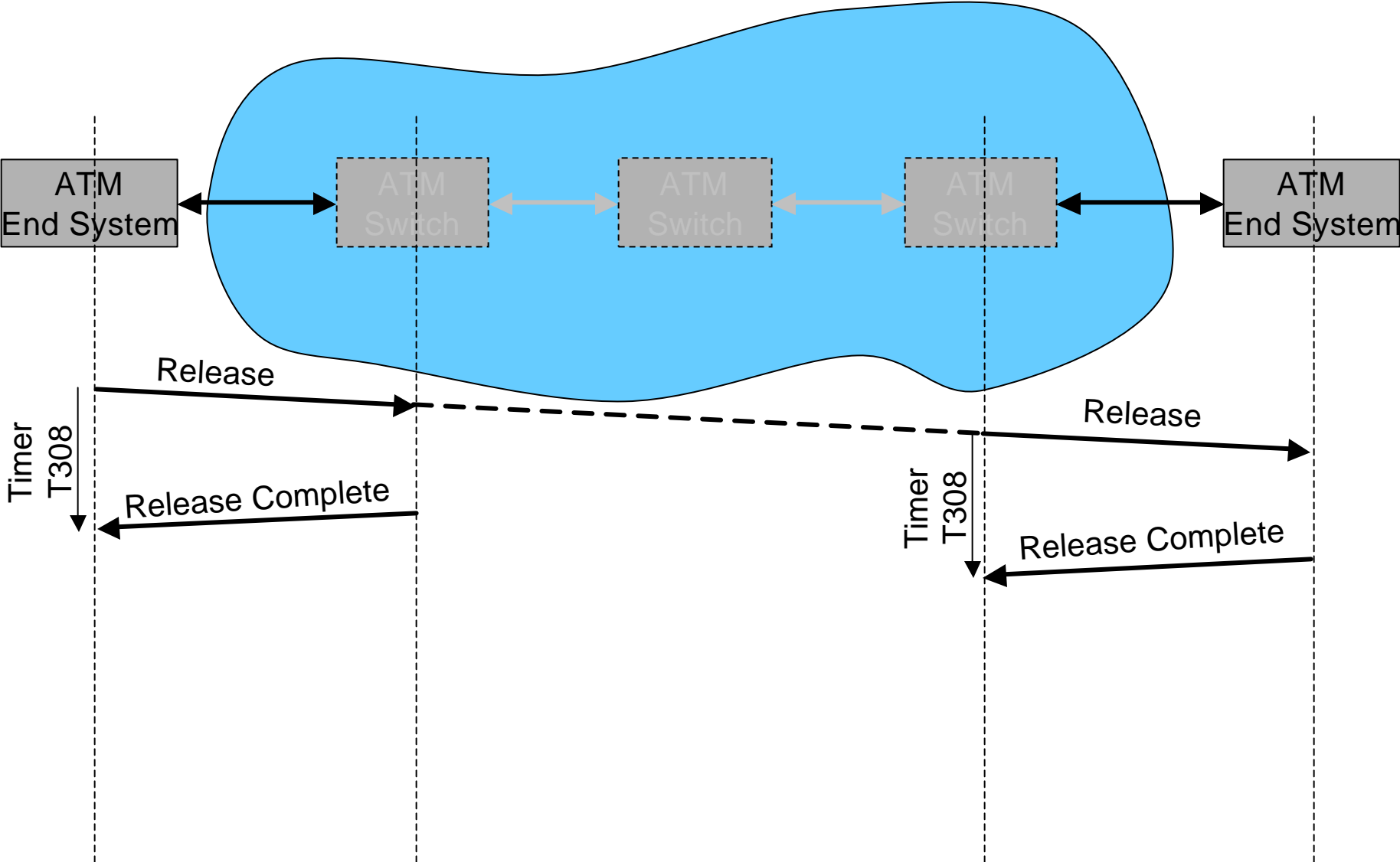
# ATM Switch Reference Model



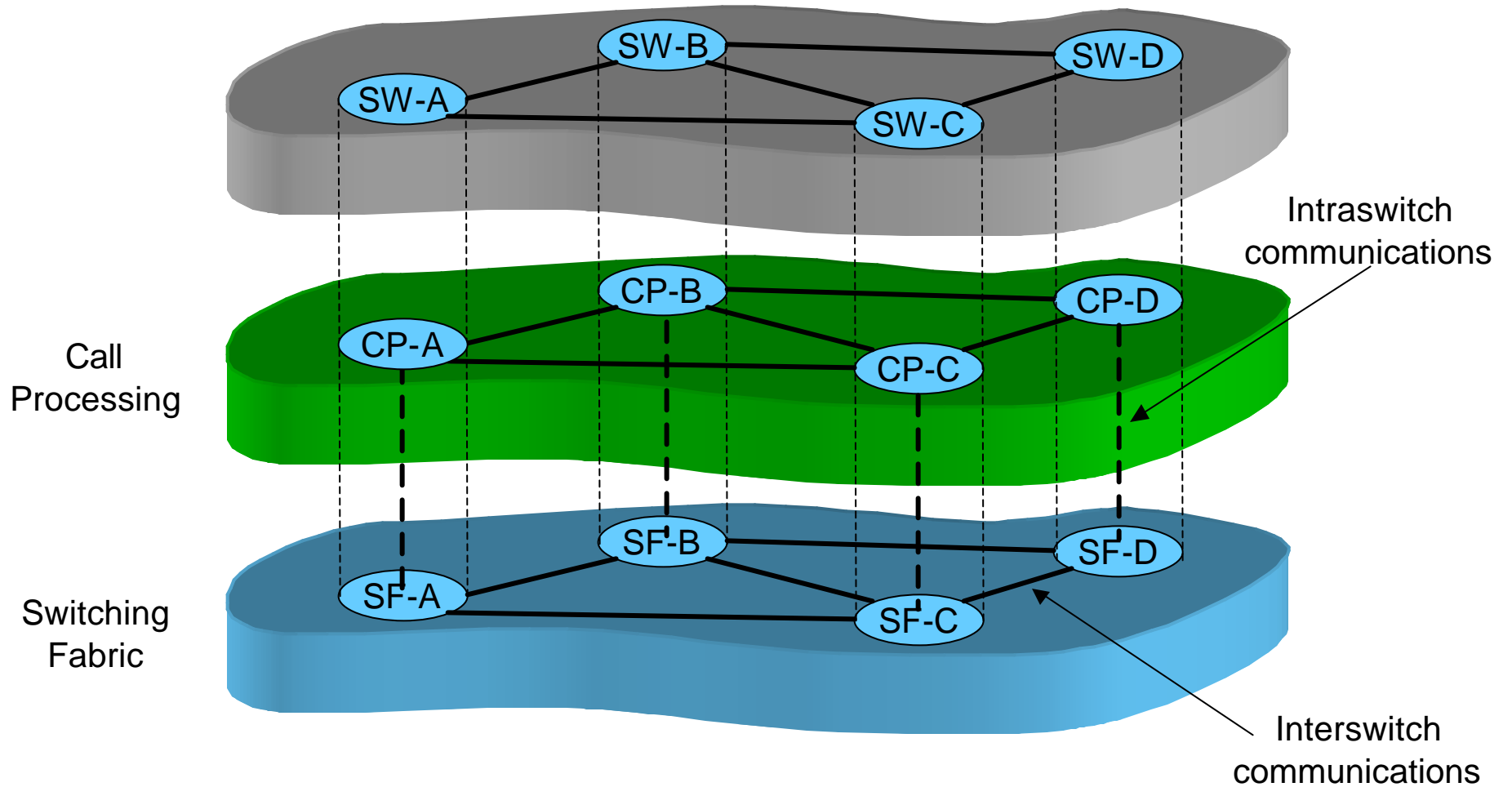
# ATM Call Establishment



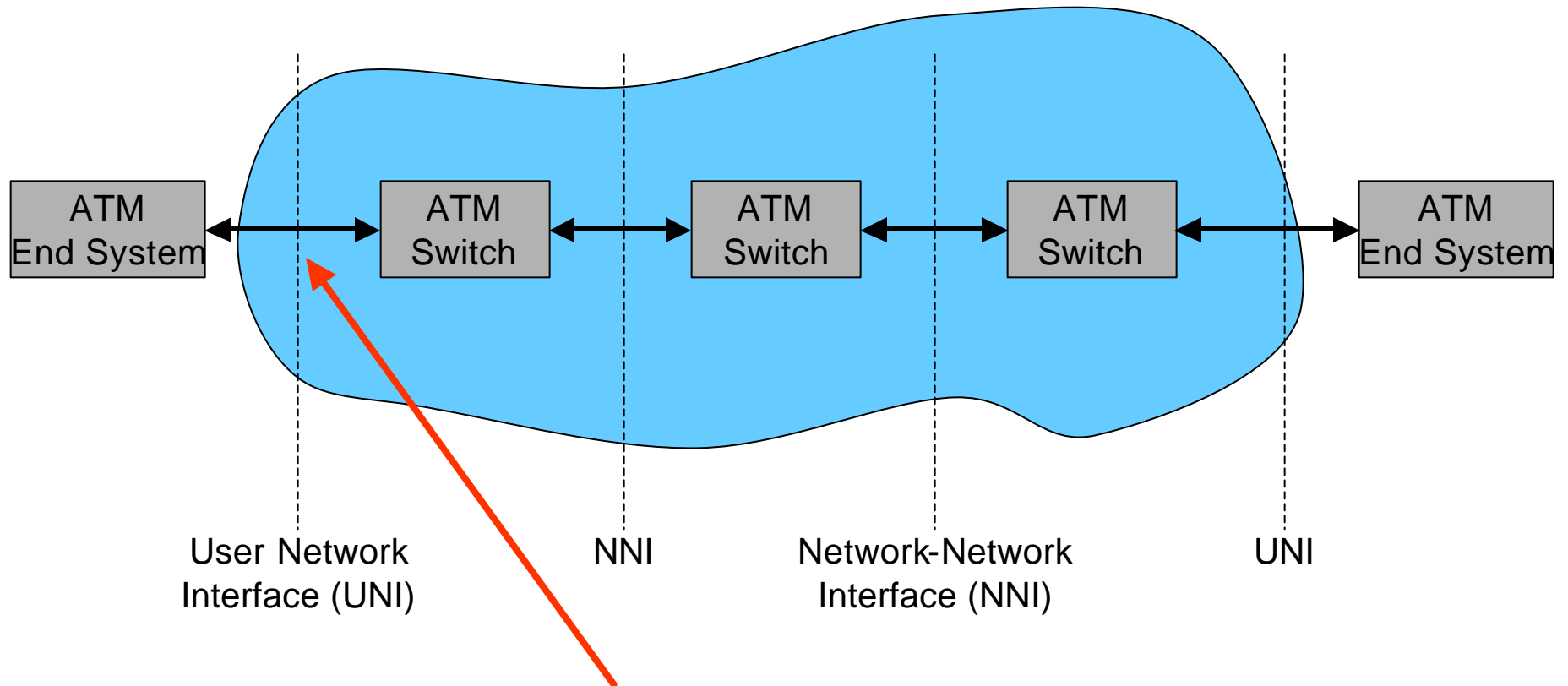
# ATM Call Release



# Layered ATM Network

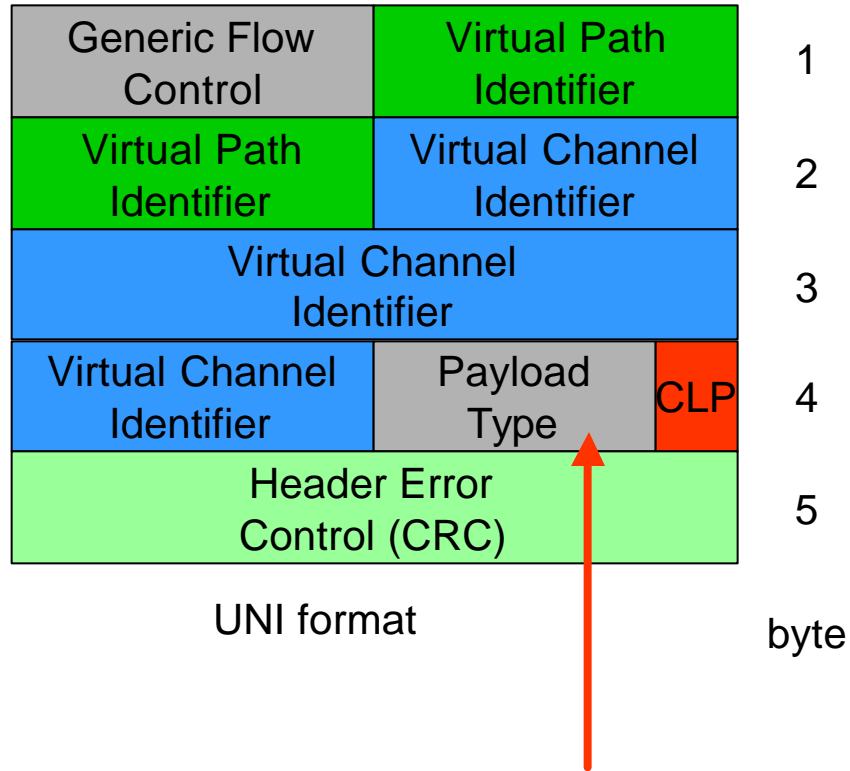


# ATM Vulnerabilities - 1



- Unrestricted User Interactions with UNI**
- Multiple call requests
  - Unrestricted QoS parameters

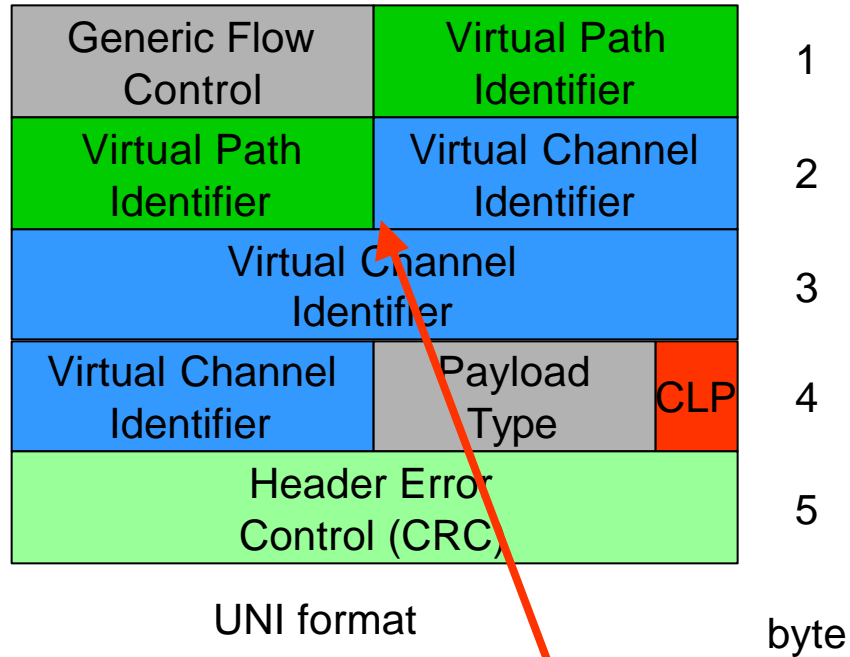
# ATM Vulnerabilities - 2



## In-band Signaling

- User traffic and call control share buffers
- Signaling can be manipulated to unknown ends

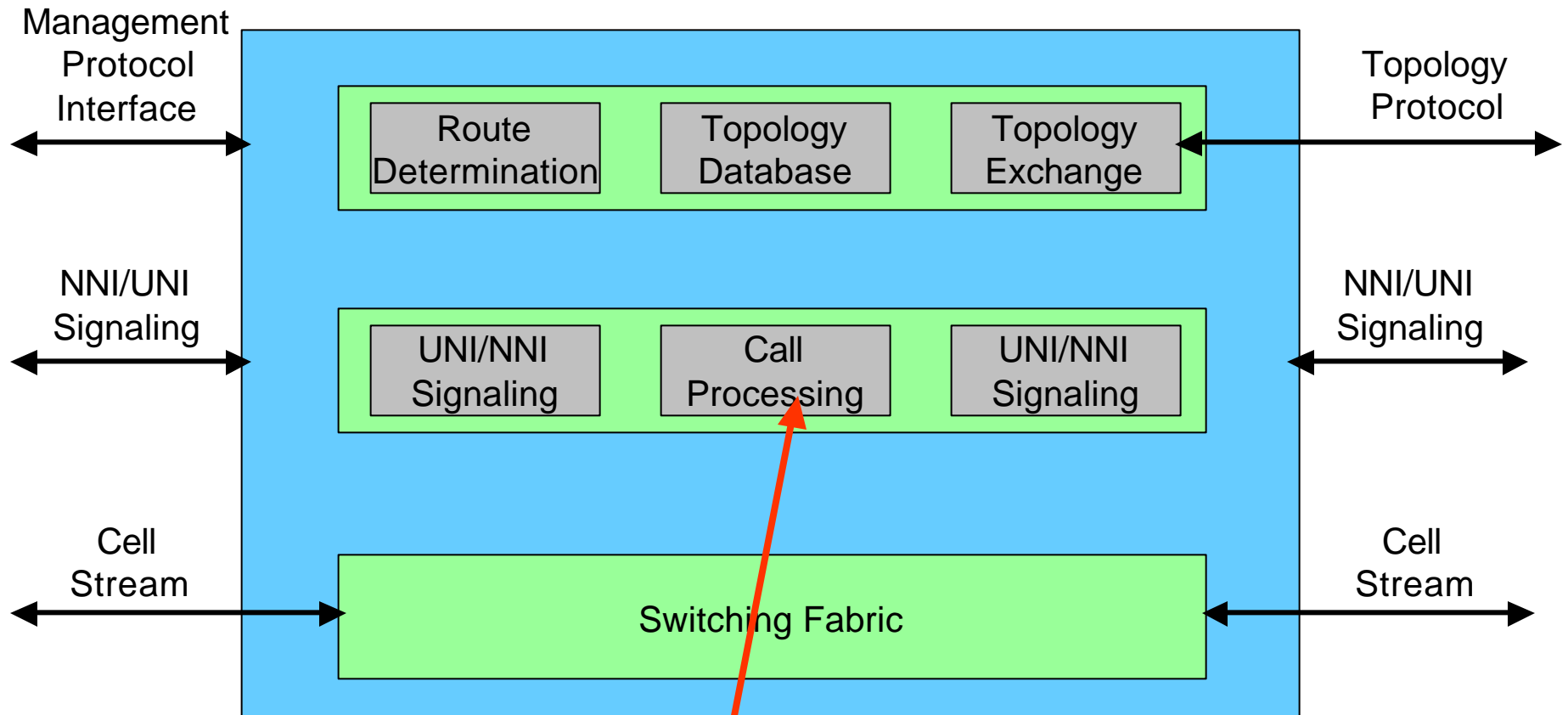
# ATM Vulnerabilities - 3



## VPI/VCI based switching

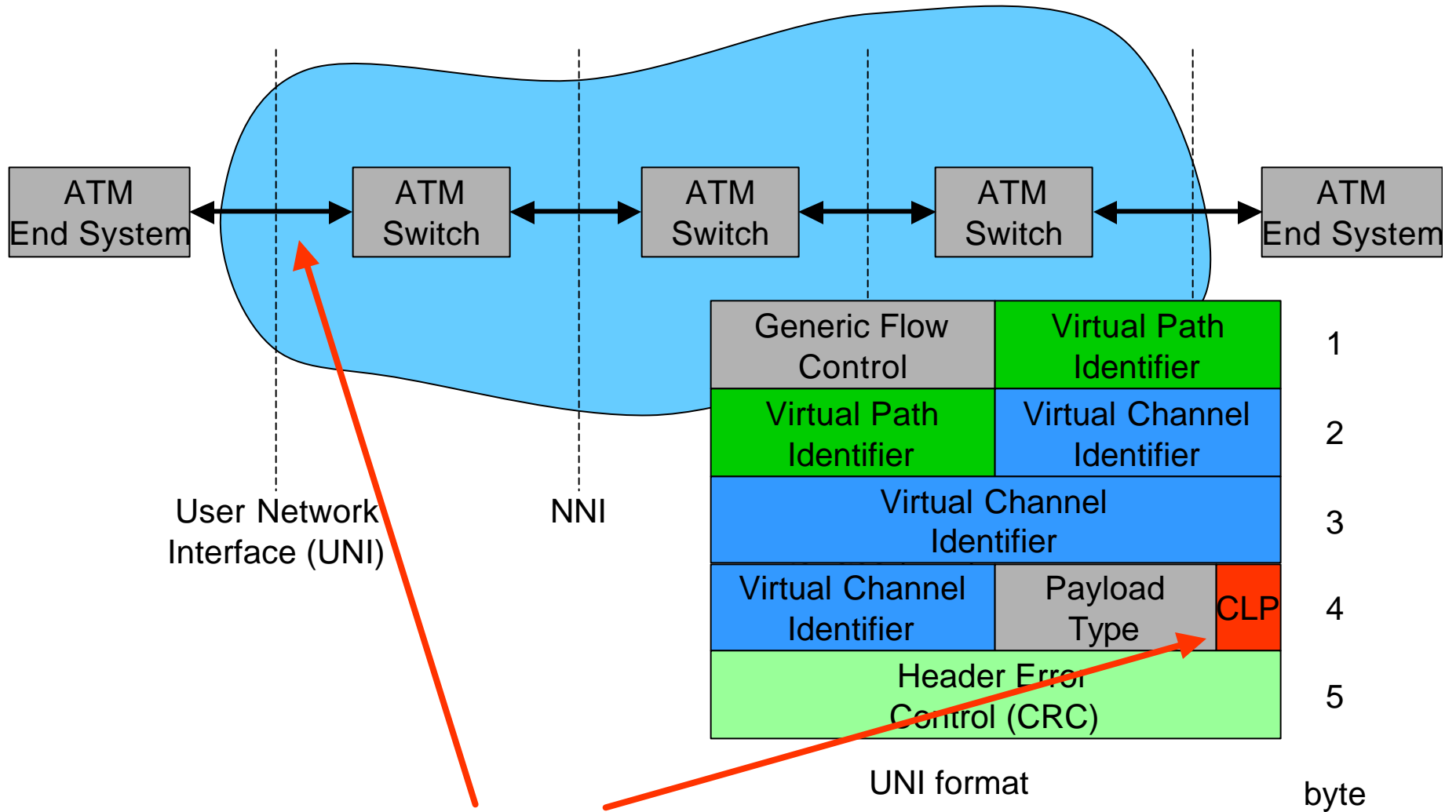
- Can they be manipulated by end user as in IP forgery?

# ATM Vulnerabilities - 4



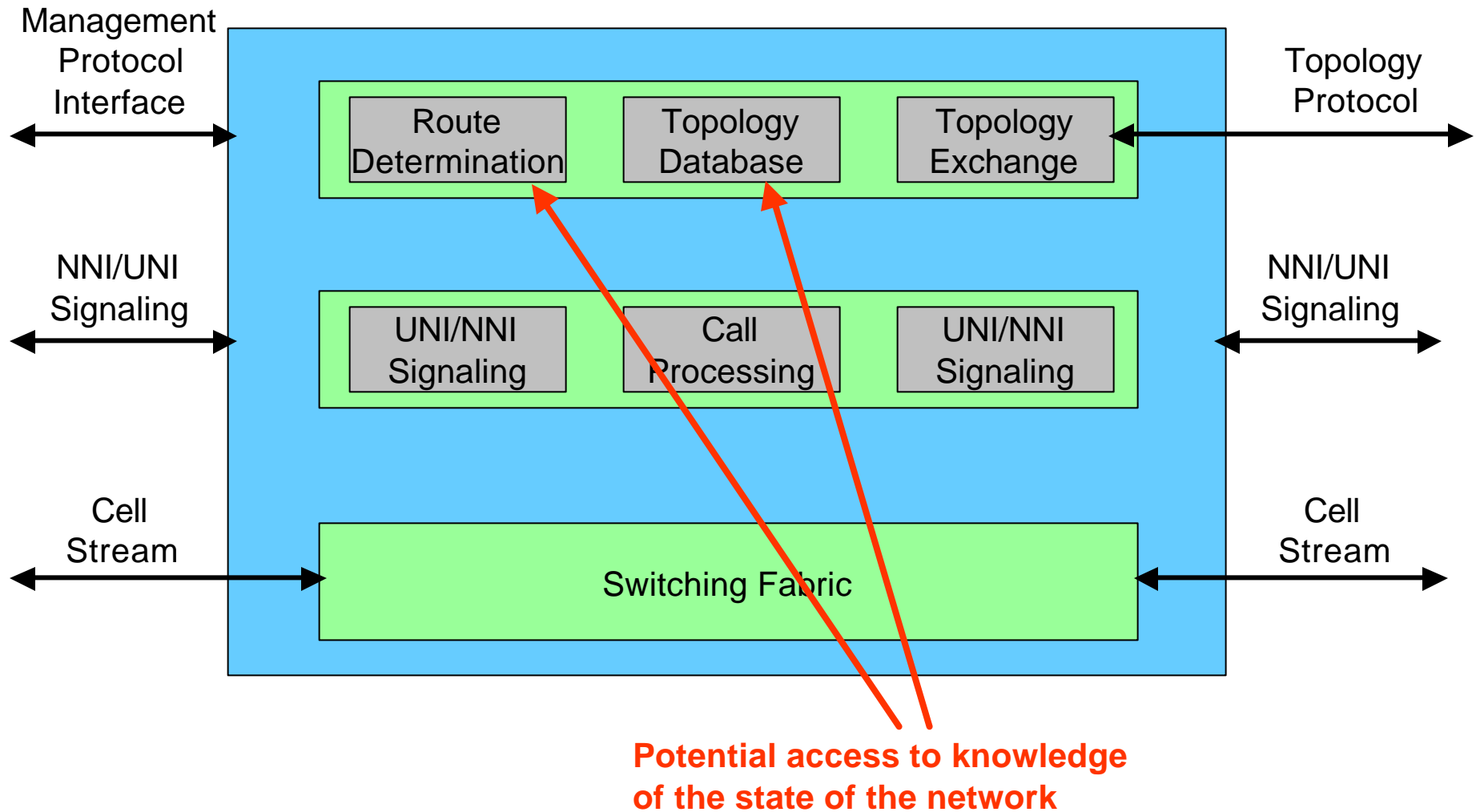
**Call processing is critical function and subject to attack**

# ATM Vulnerabilities - 5

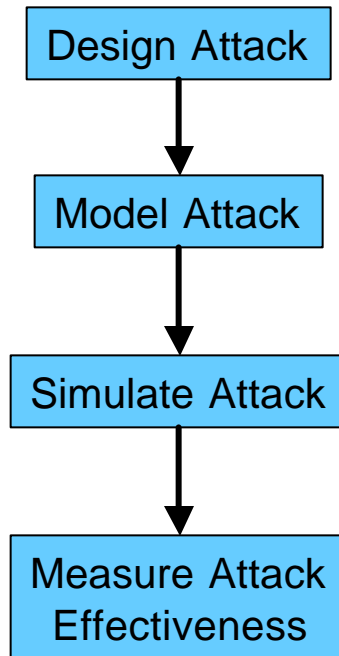


**Imprecise traffic control, trusting interface, and no internal network checking of network usage**

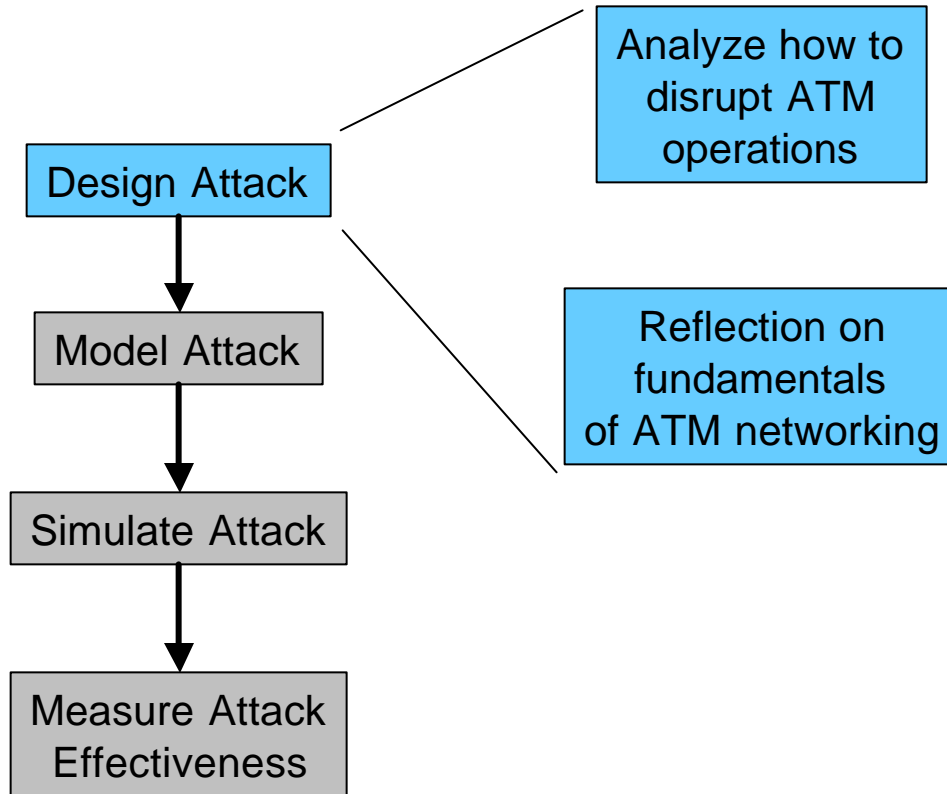
# ATM Vulnerabilities - 6



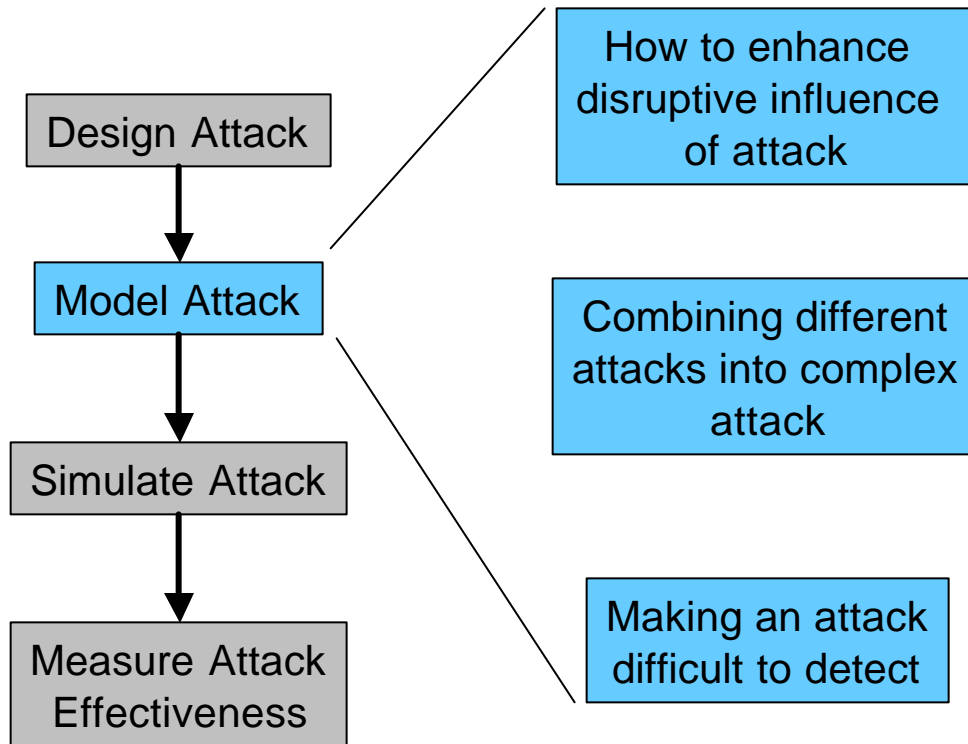
# Attack Modeling Methodology



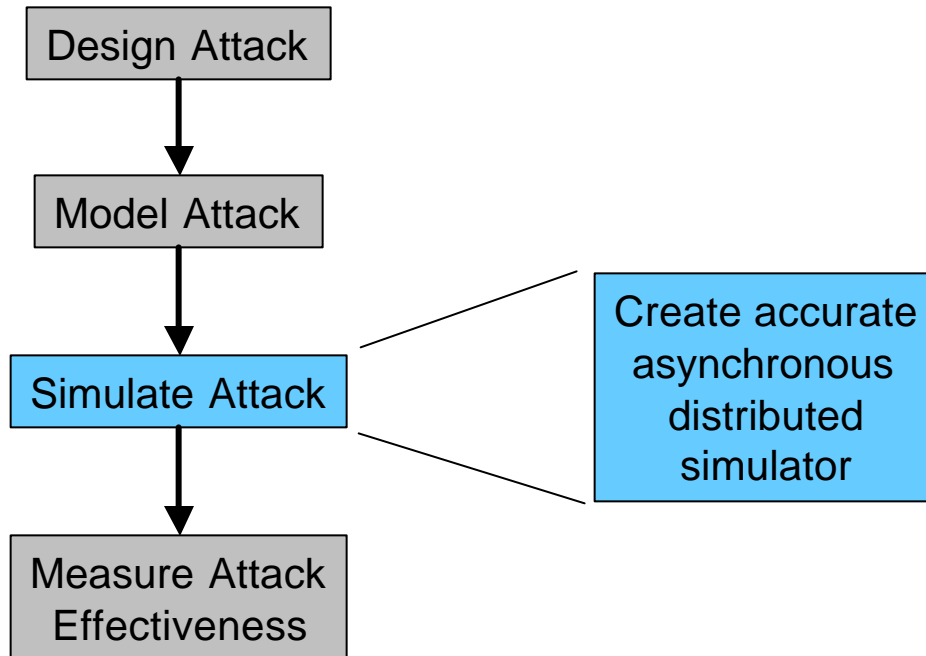
# Attack Modeling Methodology



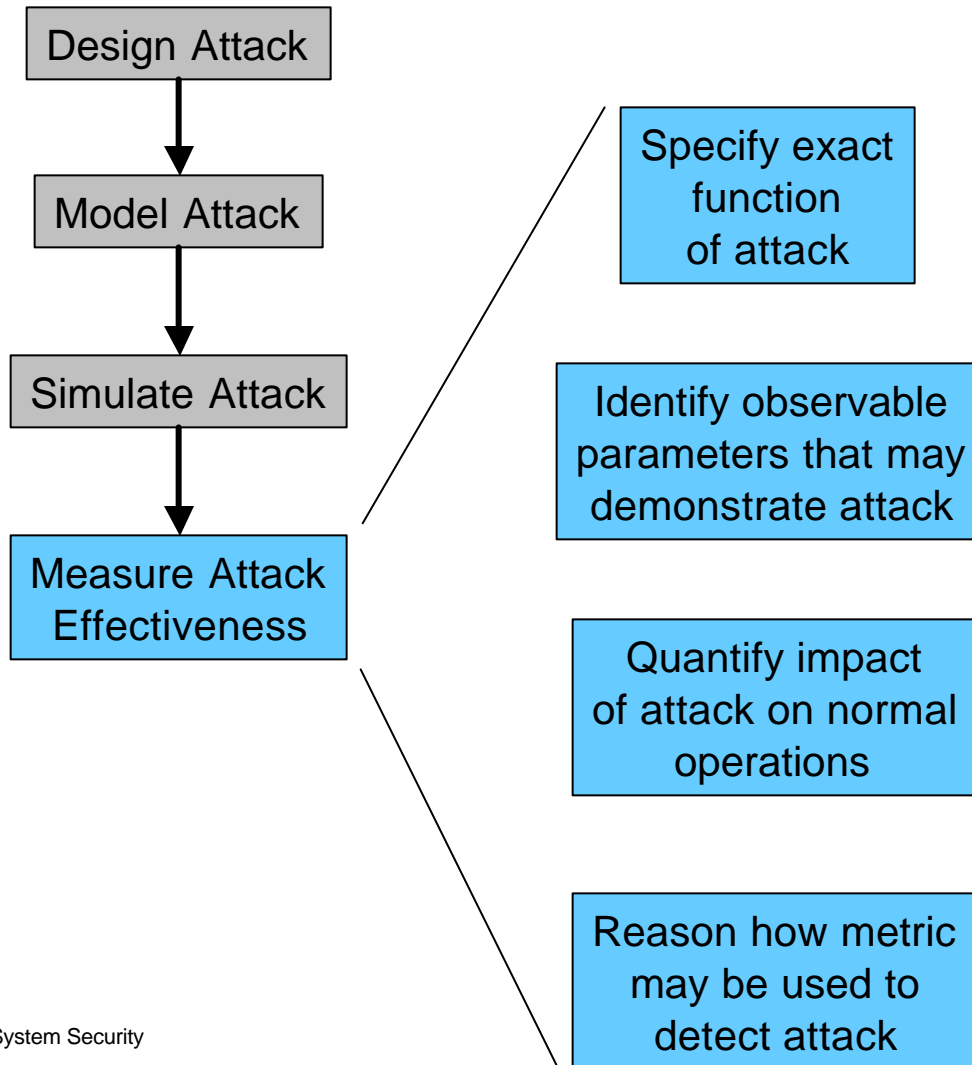
# Attack Modeling Methodology



# Attack Modeling Methodology



# Attack Modeling Methodology



# Homework 7 - due 11/4/02

- ref: Ghosh, p. 156, Problem 5:
- In-band signaling was a significant vulnerability for the long distance voice toll network: Sufficient details of the signaling network protocol were published in the Bell System Technical Journal to enable hackers to build devices to simulate internal signaling from the outside of the network. Do one of the following exercises (do both for extra credit):
  - (A) Research the signaling protocol that replaced in-band signaling and describe some of its early vulnerabilities
  - (B) Other than the threat of toll-evasion, there was a significant national security threat related to the use of the in-band signaling protocol. Research this other threat and describe how it was perpetrated.