

**NIS/CpE 691CE**

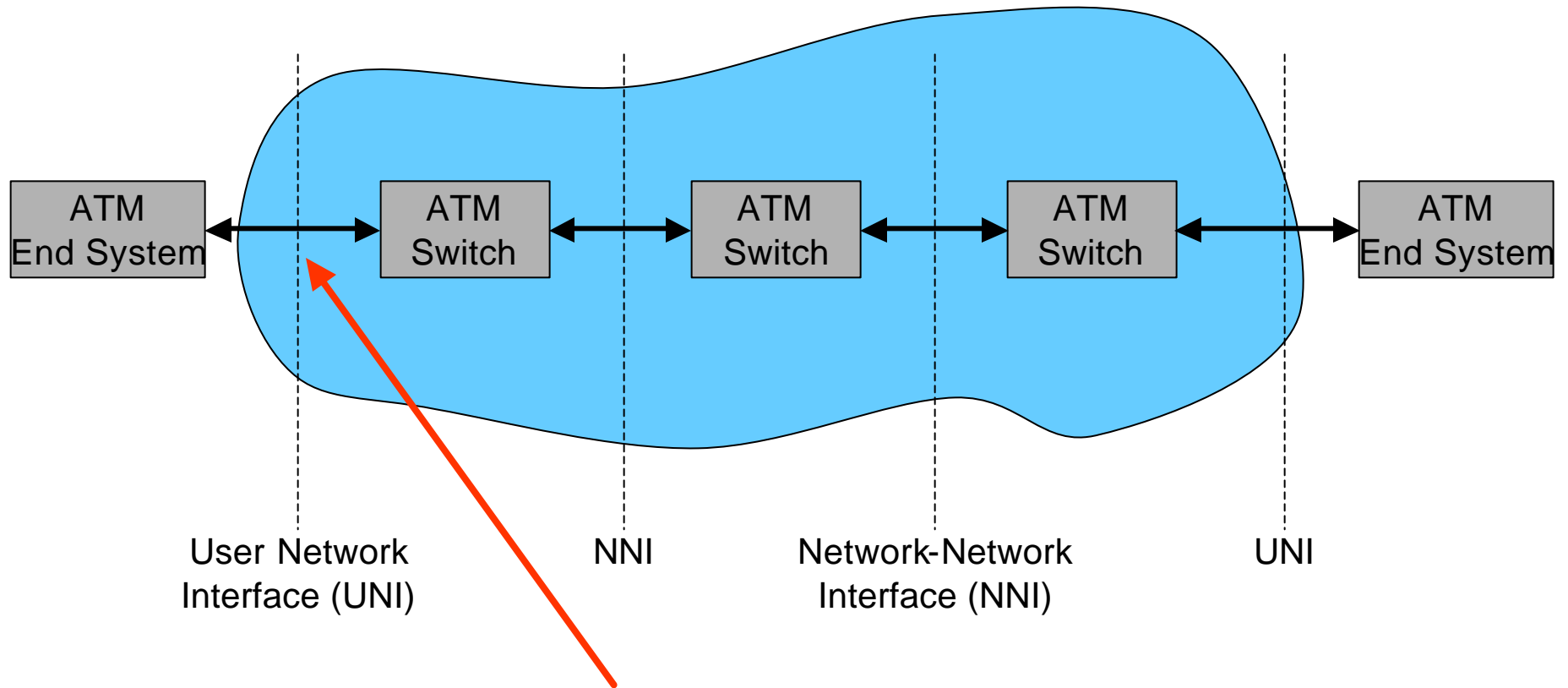
**Information System Security**

**Class 8 – 11/4/02**

# Tonight's Topic

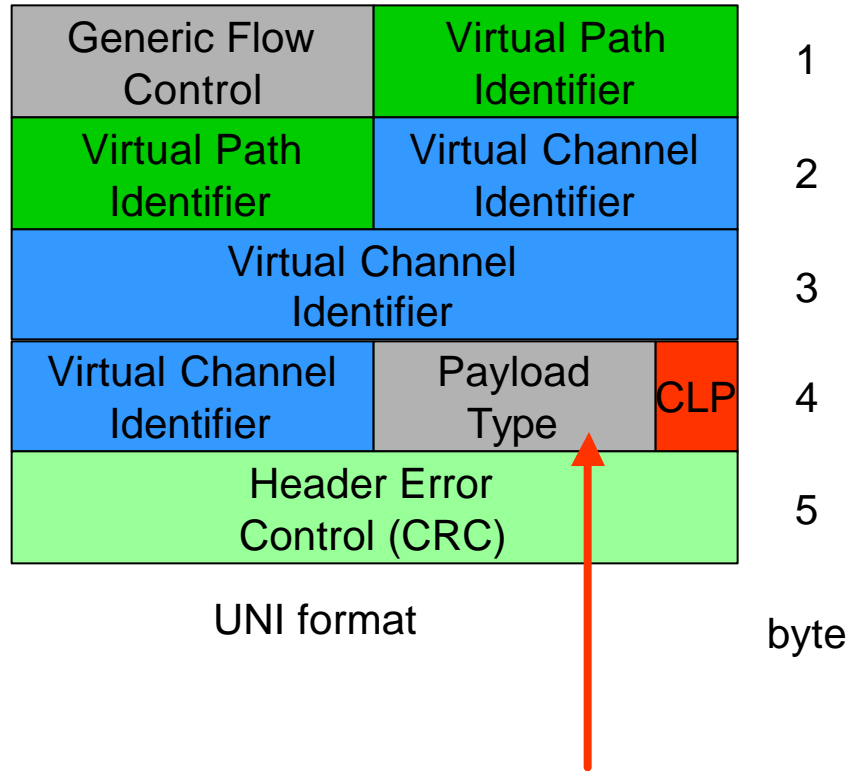
- Review of Vulnerabilities
- Synthesizing Attacks (Ghosh 6.3.3)

# ATM Vulnerabilities - 1



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

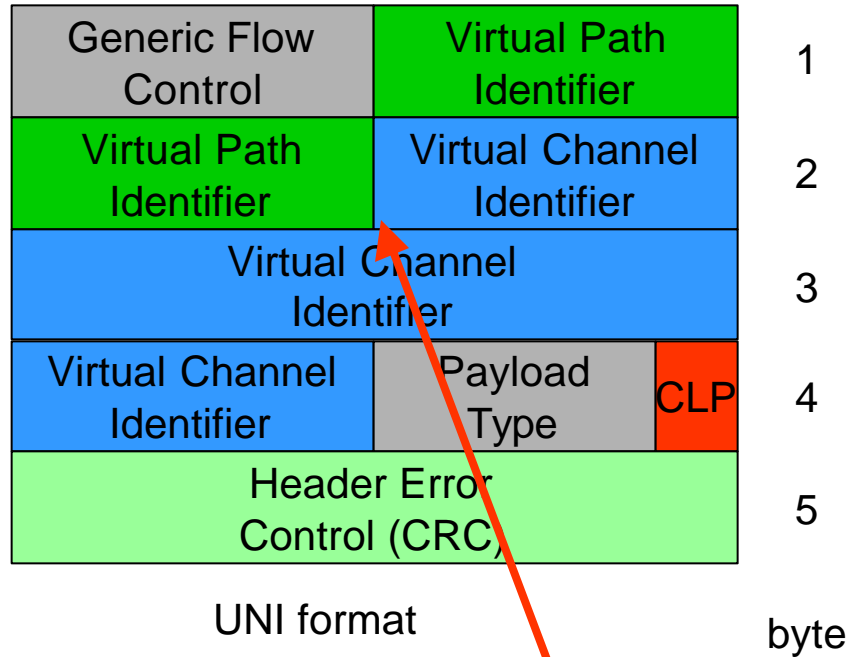
# ATM Vulnerabilities - 2



## In-band Signaling

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

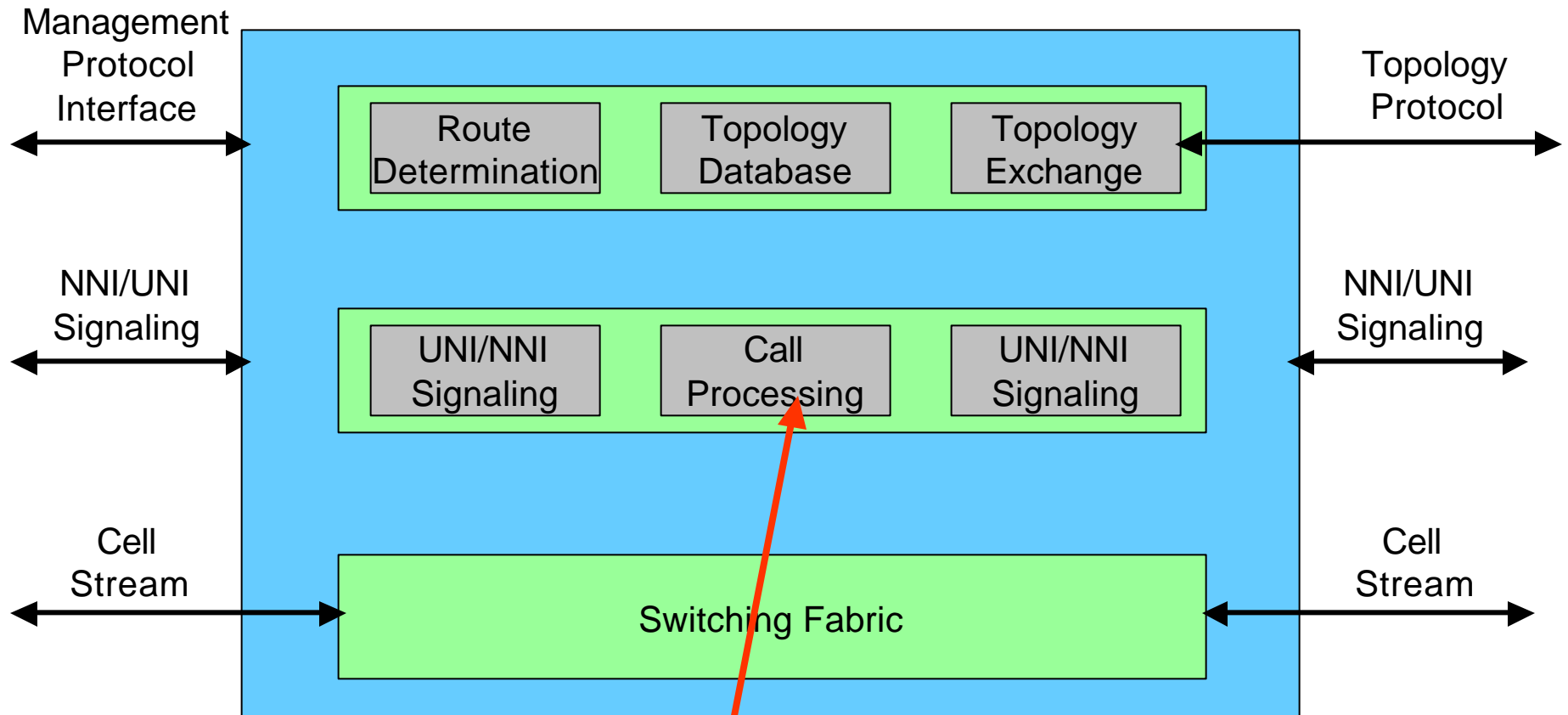
# ATM Vulnerabilities - 3



## VPI/VCI based switching

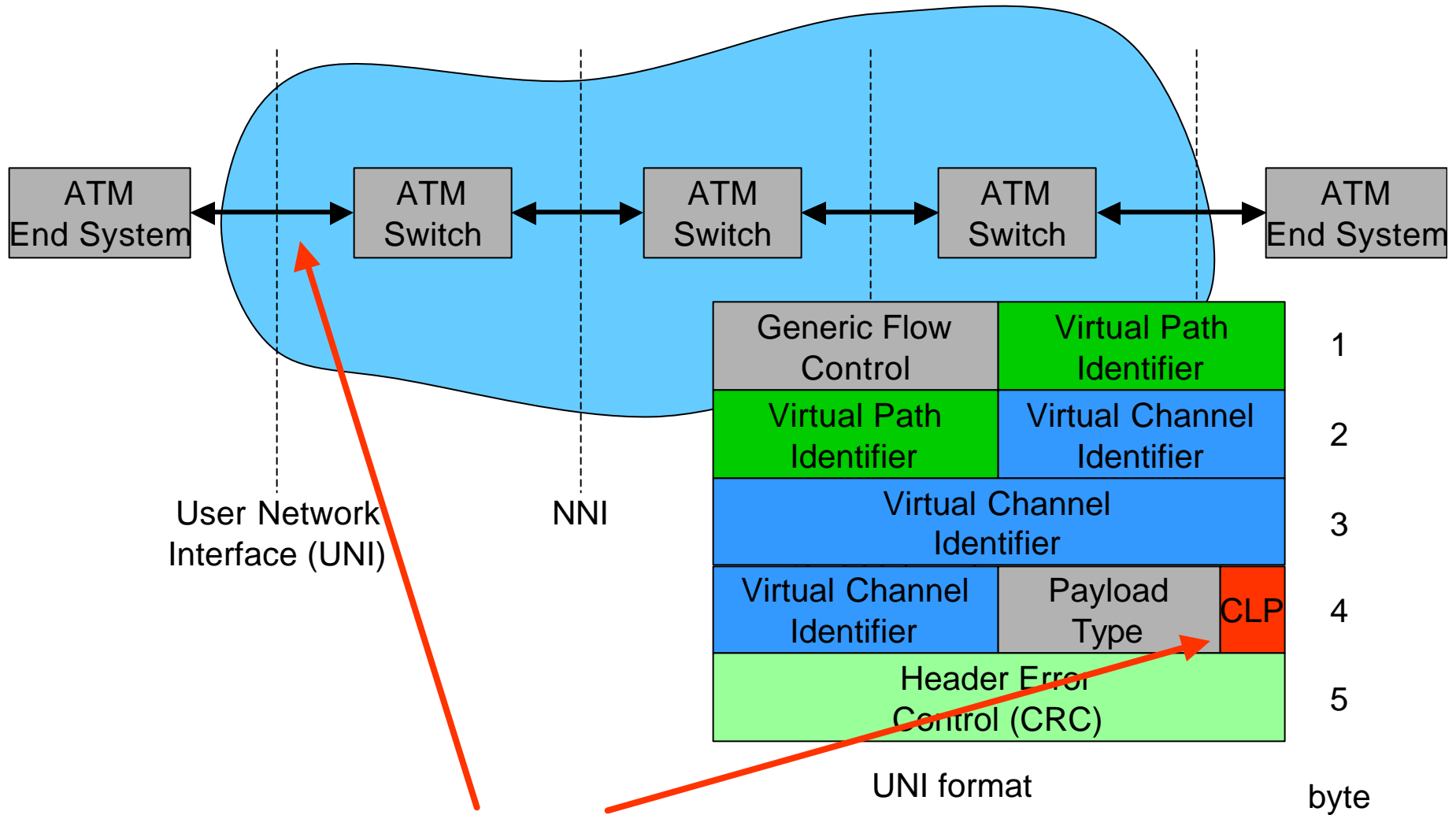
- Can they be manipulated by end user as in IP forgery?

# ATM Vulnerabilities - 4



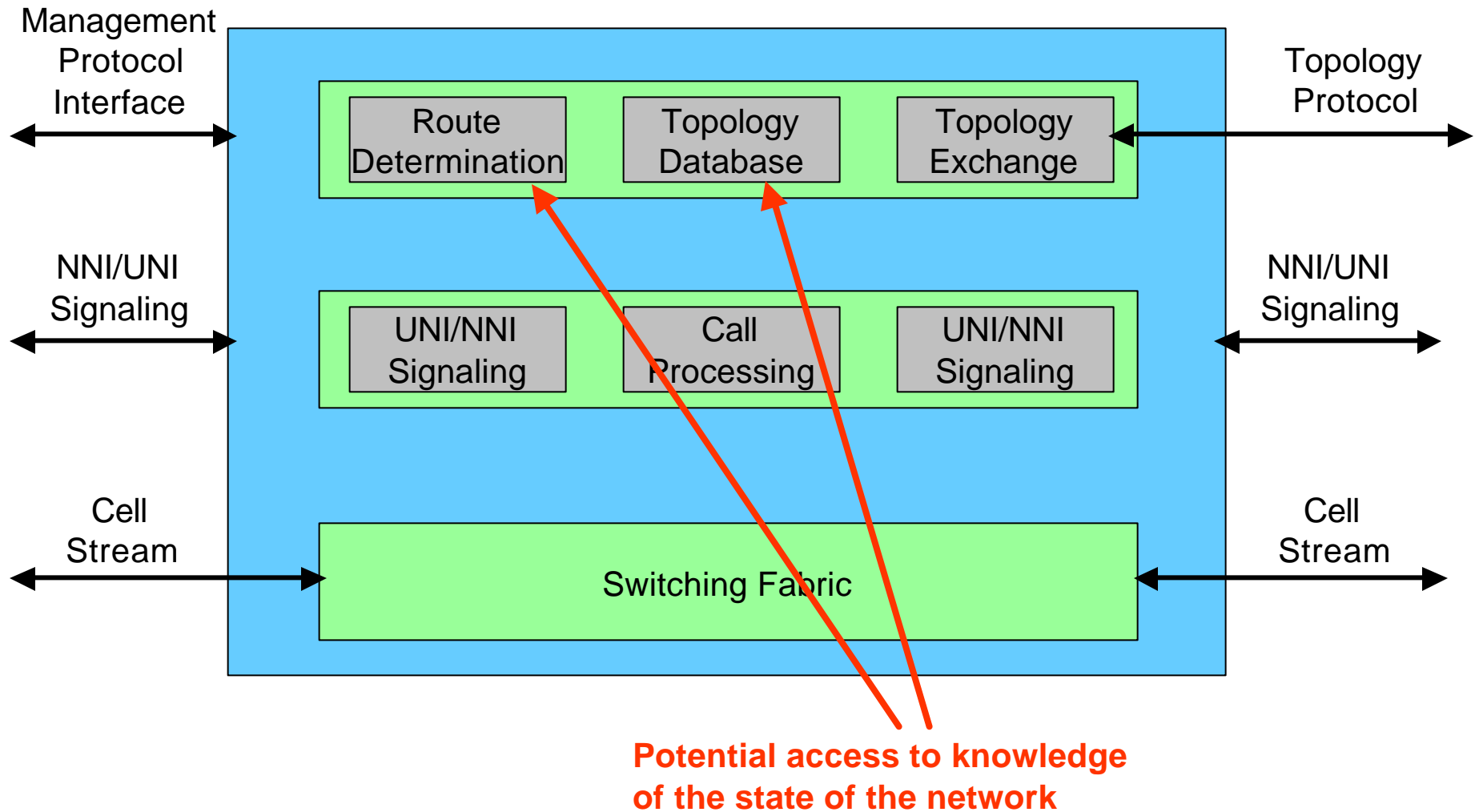
**Call processing is critical function and subject to attack**

# ATM Vulnerabilities - 5

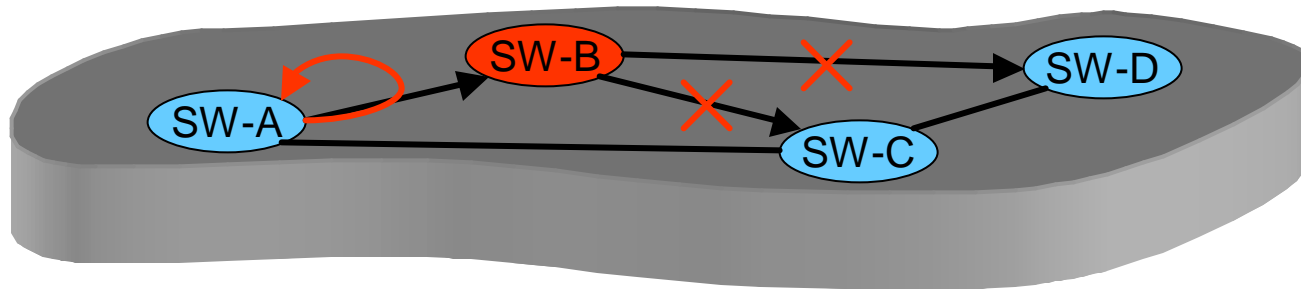


**Imprecise traffic control, trusting interface, and no internal network checking of network usage**

# ATM Vulnerabilities - 6

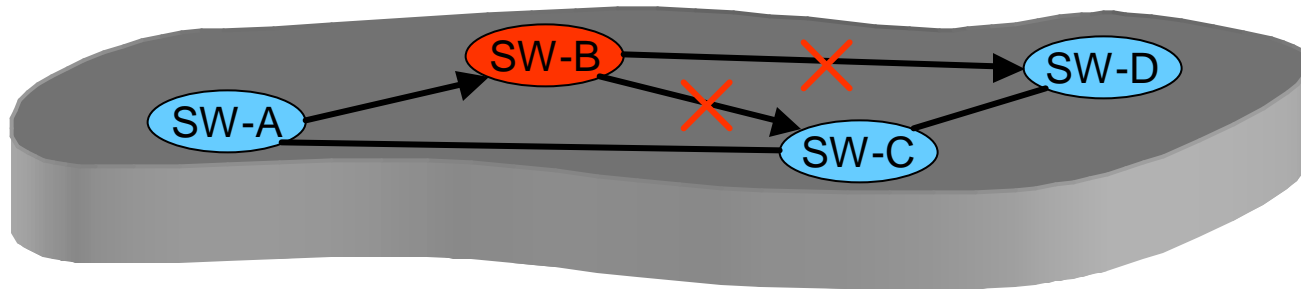


# Attack 1 - Denial of Service



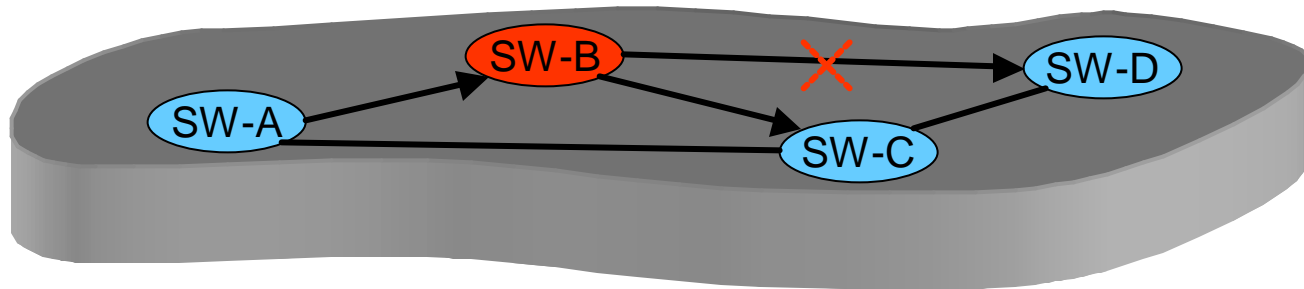
- Switch B is under the perpetrator's control, rejects SETUP requests, claims lack of resources
  - Blanket rejections of all SETUPS may be detectable.
    - Refinement: Reject subset of SETUP requests
      - All those originating at a specific switch
      - All those destined for a specific switch
- Sometimes call SETUP requests are rejected for true lack of resources
- Attack detection metric needs to measure local and network-wide statistics to see pattern shifts:
  - Number of call requests, number successful, number rejected

## Attack 2 - Indirect Denial of Service



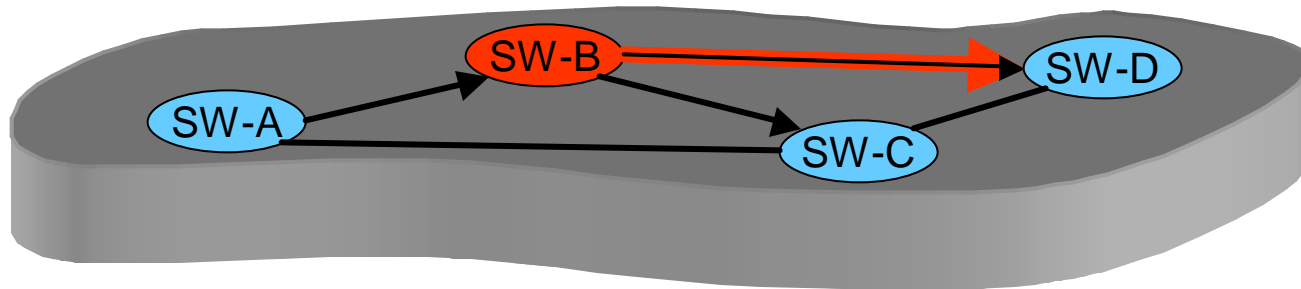
- Switch B is under the perpetrator's control, *accepts* SETUP requests, and allows origination point under attack to think call is proceeding
  - Compromised switch does not forward the SETUP request to the destination
  - All traffic sent on call is discarded by compromised switch
- Compromised switch may select particular sources and destinations to attack
- Metrics focus on call attempts vs. successfully established calls; bandwidth utilization across all network links

# Attack 3 - Cell Loss



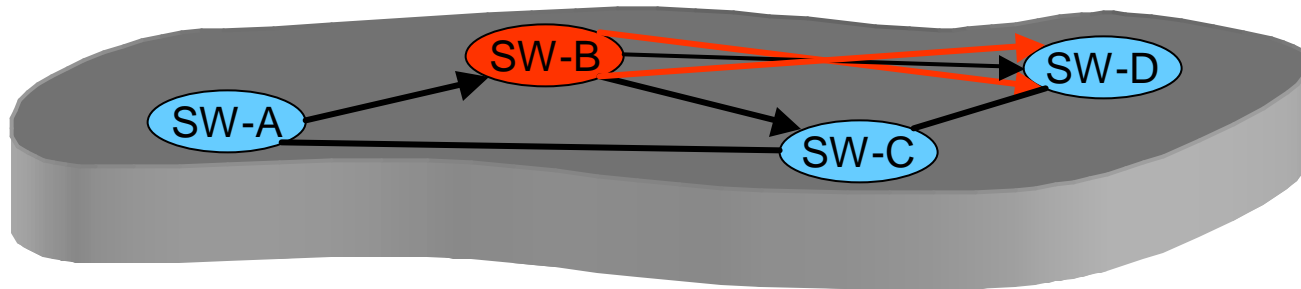
- Switch B is under the perpetrator's control, *allows* call establishment to proceed
  - Compromised switch discards traffic cells for attacked switches
- Refinements:
  - Drop traffic cells randomly
  - Drop traffic cells periodically
- Knowing the traffic monitoring procedures of network will help avoid detection
- Understanding the type of traffic being interfered with can help, too (e.g., drop one cell from each IP packet)
- Metrics focus on number of cells leaving source, arriving at destination, and dropped by network.

# Attack 4 - Bogus Traffic



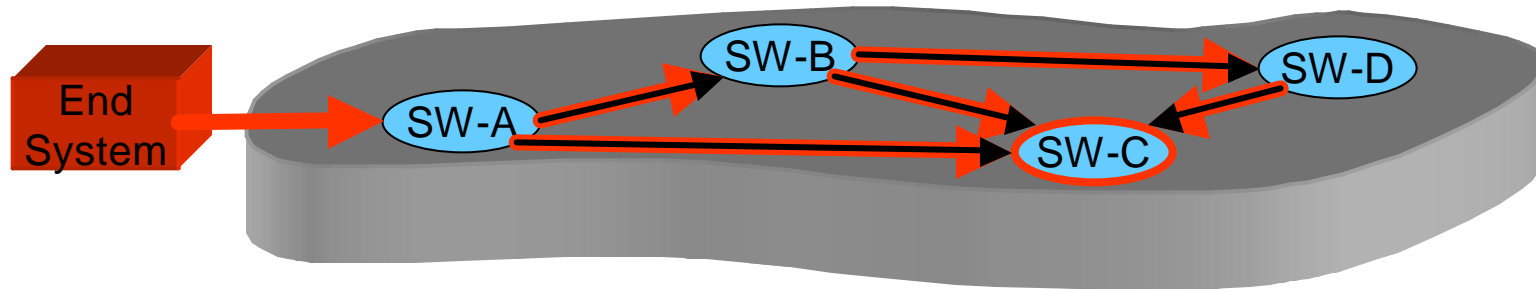
- Switch B is under the perpetrator's control, generates fictitious ATM cells, mixes them with authentic cells and transmits them on established channels
- Traffic controls are only used at UNI, not NNI - ATM network trusts its peers.
- Switches do not check traffic content or rate relative to negotiated rate.
- Overutilization causes cell loss of legitimate cells, which may cause erroneous cell assembly at destination or cause retransmission requests.
- Metrics focus on number of cells leaving source, arriving at destination, and dropped by network, on a per channel basis.

# Attack 5 - Misdirected Traffic



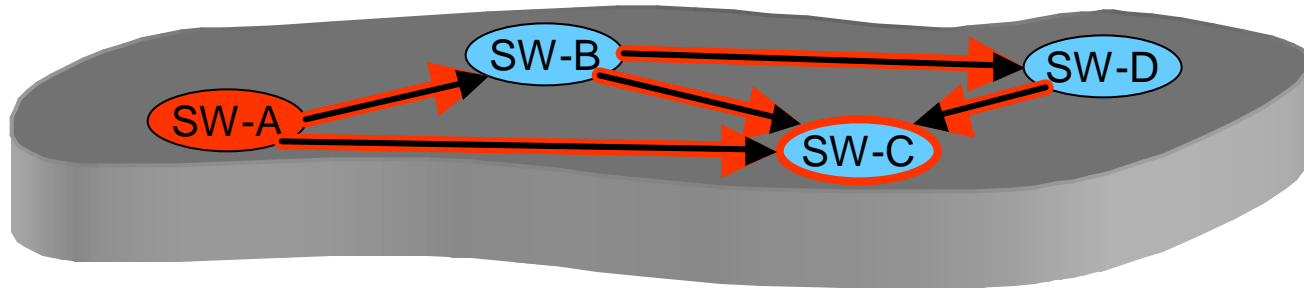
- Switch B is under the perpetrator's control, relaying active calls between one or more switches under attack. Switch B diverts cells between active channels
- No traffic is created or destroyed, so simple traffic volume metrics won't work.
- Bandwidth is consumed improperly, traffic along some routes will increase, causing heavier load than planned, missing traffic may lead to retransmission requests, extra cells in some channels may cause data corruption and retransmission requests.
- Metrics focus on number of cells leaving source, arriving at destination, and dropped by network, on a per call basis.

## Attack 6.1 - Bogus Calls - From a User



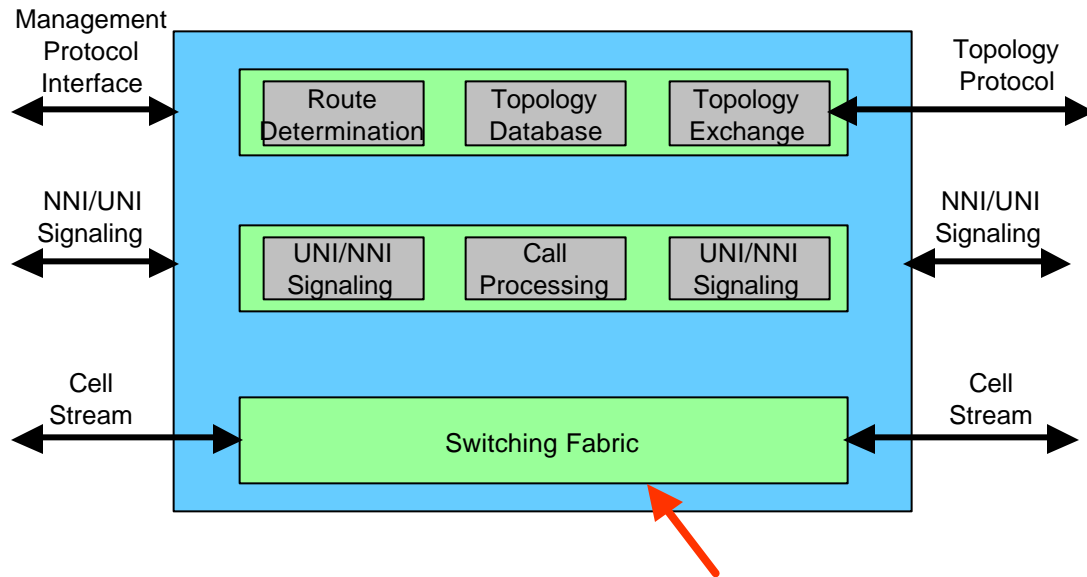
- User End System signals across UNI, making a large number of call setup requests
- User must know node identifiers used in system
  - But, user cannot influence routing of calls to destination

## Attack 6.2 - Bogus Calls - From a Node



- Compromised node signals across NNI, making a large number of call setup requests
- Attacker probably knows network internals, including node identifiers used in system
- Attacker **can** influence routing of calls to destination, picking routes to maximize effect or minimize detection. Focused overload can be created at destination node with little observable impact on individual links.
- Variation A: Small number of calls, each requesting large amount of bandwidth
- Variation B: Large number of calls, each requesting small amount of bandwidth
- Metrics focus on bandwidth availability of each link, calls initiated at each node, and number of successful calls at each node.

# Attack 7 - Reduction in Buffers



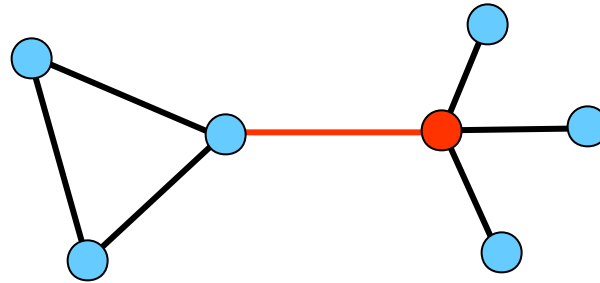
- Attacker controlling a node artificially reduces the available buffer
- Cell loss probability increases, cell delay may increase
- Attacker could also simulate reduction in buffer by generating bogus cells (as in Attack 4)
- Metrics focus on cell statistics (transmitted, received, dropped) and traffic cell delays

# Attacks 8 & 9 - Complex Attacks

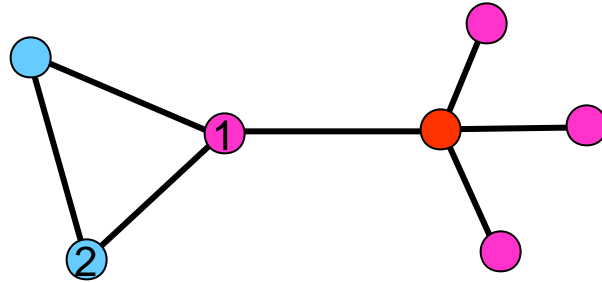
- Attempt to break network into disjoint subnetworks
- Definitions:
  - Severity: measure of degree of disconnection of network - number of pairs of nodes that are isolated into subnetworks
  - Sensitive node: Node that, if isolated from the rest of the network, brings about maximum reduction in network connectivity
  - Sensitive link: Link that could bring about maximum reduction in network connectivity

# Attacks 8 & 9 - Complex Attacks

- Attempt to break network into disjoint subnetworks
- Definitions:
  - Severity: measure of degree of disconnection of network - number of pairs of nodes that are isolated into subnetworks
  - Sensitive node: Node that, if isolated from the rest of the network, brings about maximum reduction in network connectivity
  - Sensitive link: Link that could bring about maximum reduction in network connectivity

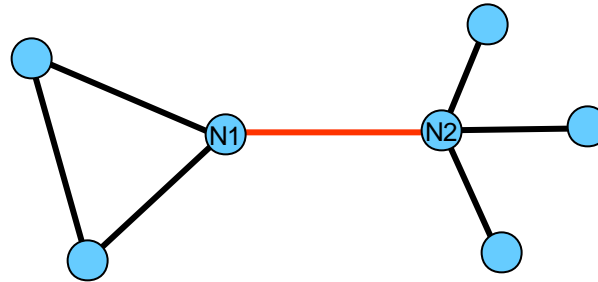


# Attack 8 - Focused Attack on Node



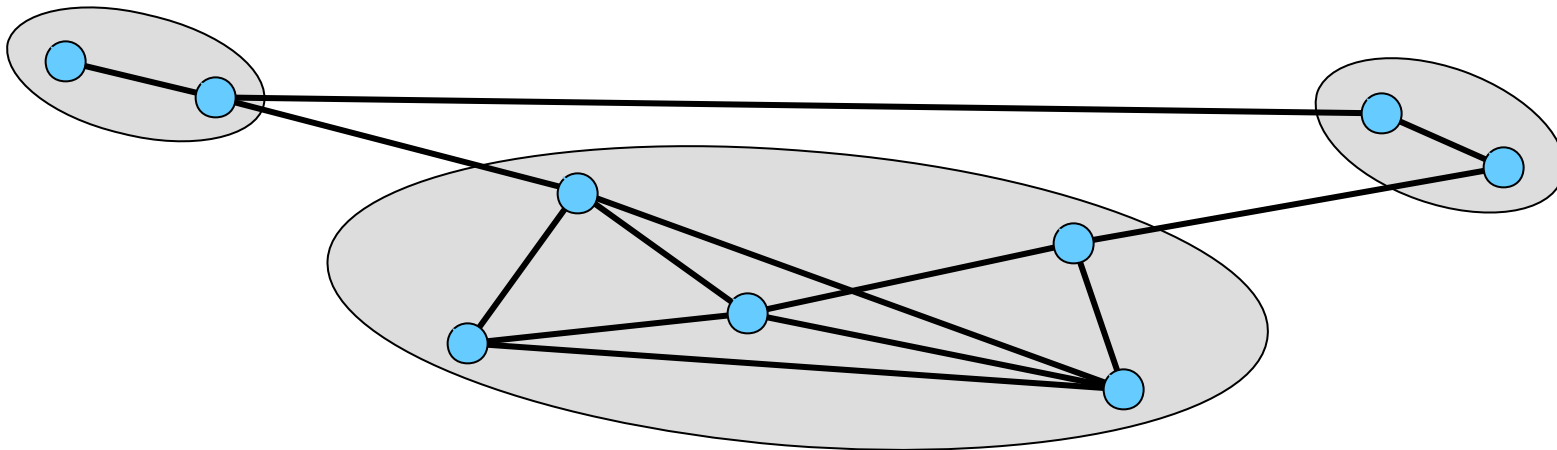
- Consume sufficient resources of the target node to deny service to/from the node
  - VPI/VCI channels
  - Buffer space
  - Link bandwidth from attacked node
- Establish bogus calls to all neighbors of attacked node
- Attacking node may be directly connected (as 1) or indirectly connected (2)
  
- Metrics focus on number of call requests, particularly with routes through the node under attack.

# Attack 9 - Focused Attack on Link



- If attacked node is in call routing path thru link under attack, SETUP can be rejected by attacker, SETUP can be accepted, but blocked, or cells on active calls can be dropped
- Attacker can initiate bogus calls to N2 with N1 in route over as many paths as possible
- Attacker can generate traffic reports that give impression that N1-N2 link is broken - other switched will avoid that link
- Damage to N1-N2 connectivity may cause other overload conditions at nodes N1 and N2
- Metrics focus on call requests, call rejections for entire network and usage of N1-N2 link

# Representative ATM Network for Attack Simulation



- Limited number of nodes to allow reasonable run time simulations
- Variety of interconnections to allow various attack scenarios
  - Two layer hierarchical network
  - Subnetworks include gateway nodes (interfaces with peer nodes in other subnetworks)
- Link delays representative of CONUS network
- Simulation network run on distributed Linux PC systems