



Incident Containment

CYBER INCIDENT RESPONSE

Incident Containment

- Perform this as quickly as possible
- Isolate the issue
- Stop the spread of the incident



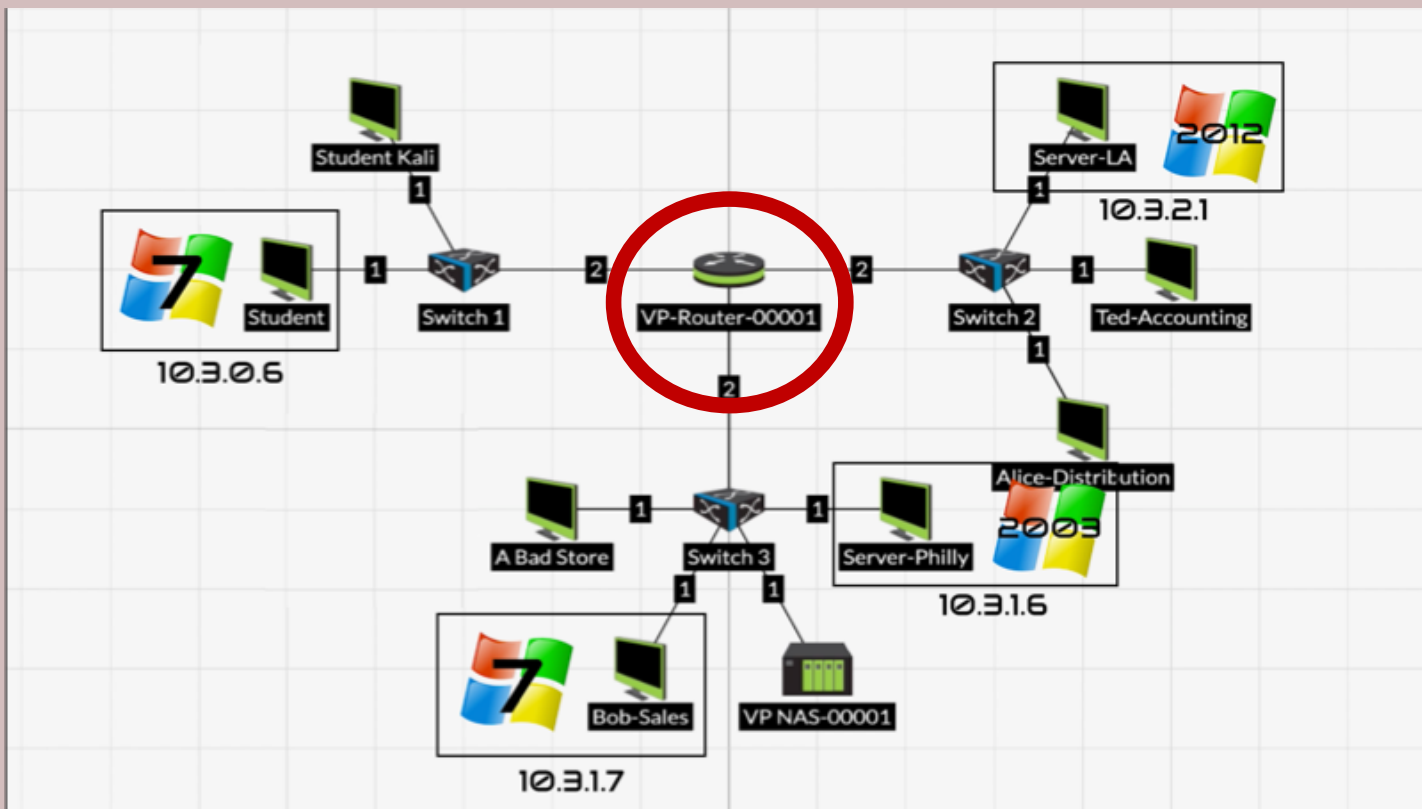
Containment Considerations

- Containment isn't perfect...
it is quick and dirty
- Can cause some loss of business functionality
- Coordinate with stakeholders before you take actions



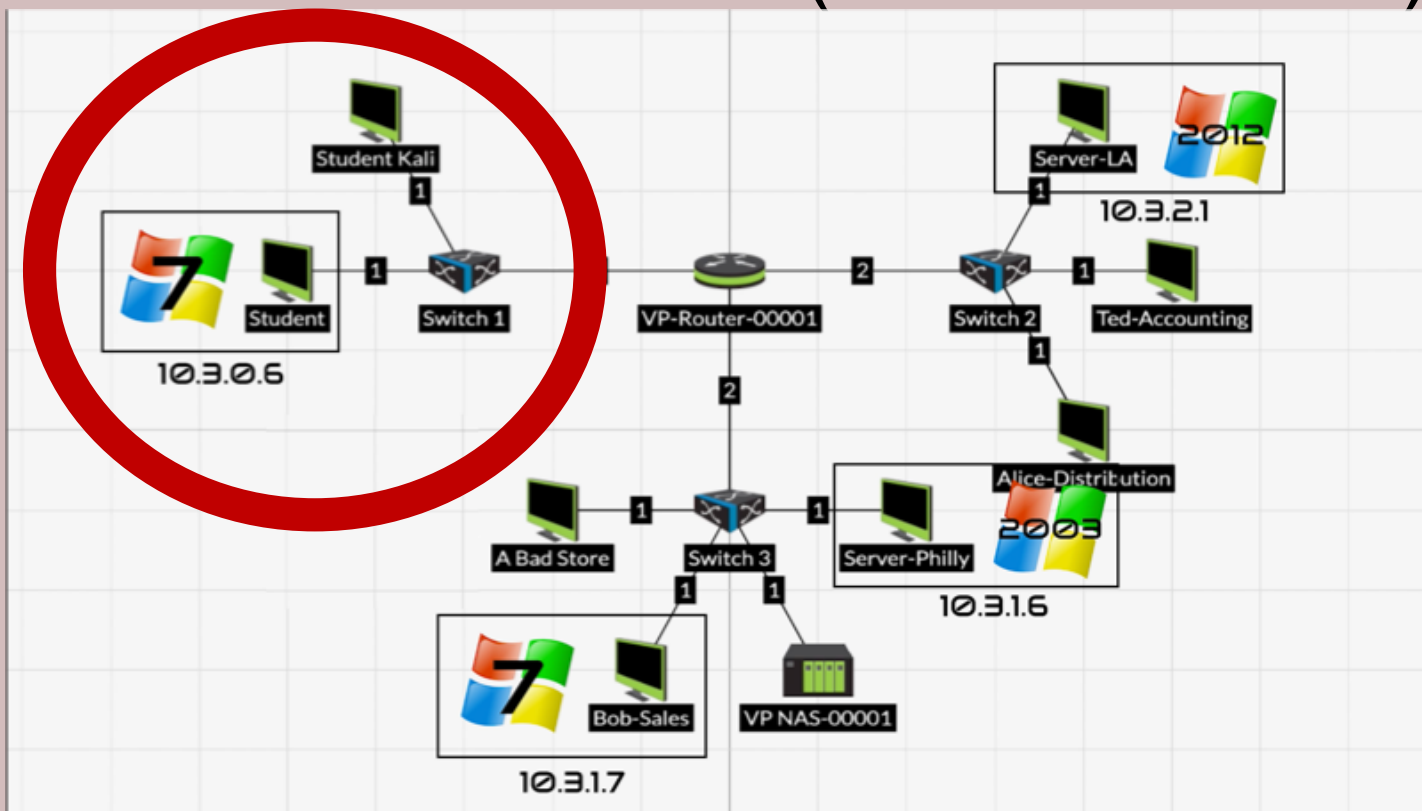
Segmentation

- Proactive strategy to prevent spread from one part of network to another



Isolation or Removal

- Remove a system from your network and directly connect to internet
- Remove the attacker (disconnect PC)



Objective of Containment

- Limit the damage to the organization
- Provide incident handlers an opportunity to collect evidence and repair issue
- Maintain and operate services for your customers to use



Identifying Attackers

- Do you need to identify the attacker?
- Is there a good business reason why?
- Attackers cover their tracks well, and identifying them can take a lot of time and resources, where your goal is simply to minimize business impact...
- Law enforcement has a different viewpoint on this, though...

