ICS Security

Zoning

Objectives

- Discuss the concept of network zoning using the Purdue Model.
- Learn how to create network zones using segmentation.
- Demonstrate how hackers can take advantage of improperly segmented networks and intercept secure communications.
- Demonstrate how network segmentation restricts a hacker’s ability to intercept secure communications.

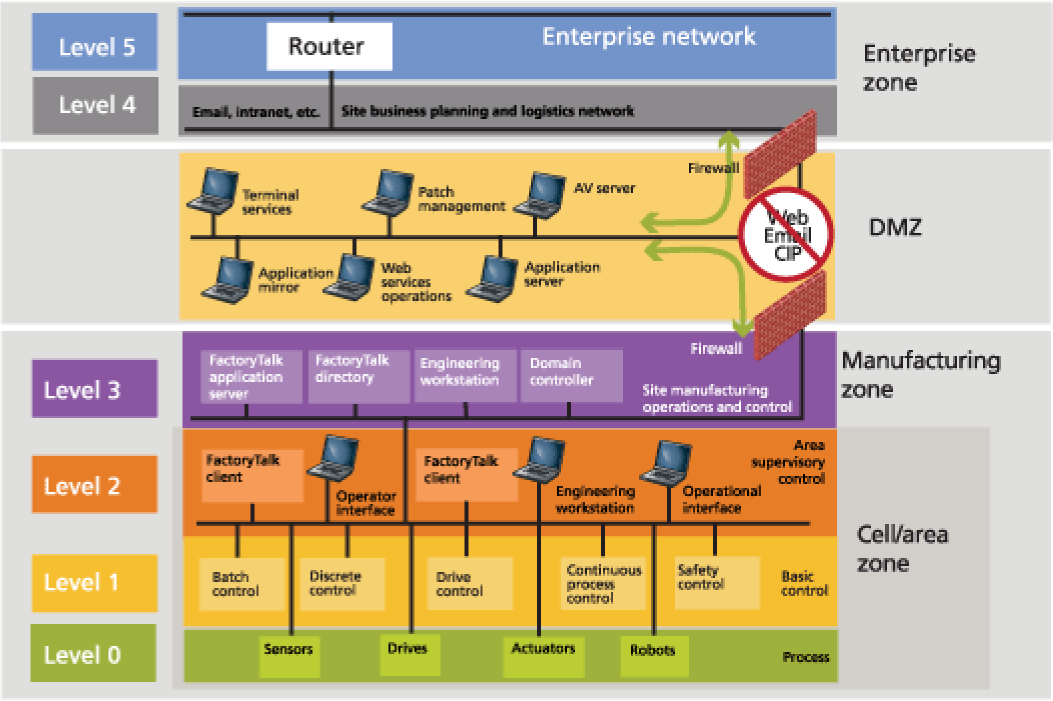
Purdue Model

- Purdue Enterprise Reference Architecture (PERA)
  - Part of ICS99 – Industrial Automation and Control Systems Security
- Separates systems into four zones and six levels

Purdue Model

Enterprise Security Zone

Manufacturing Zone



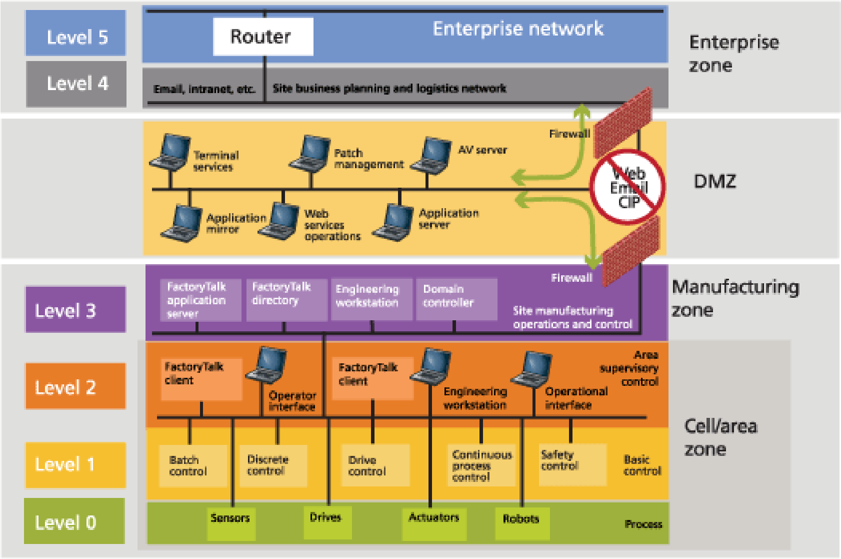
Industrial Demilitarized Zone

Cell/Area Zone

Purdue Model

- Enterprise Security Zone
  - Levels 4 and 5
  - Contains traditional IT services (Email, Enterprise Resource Planning (ERP), File Sharing, etc)

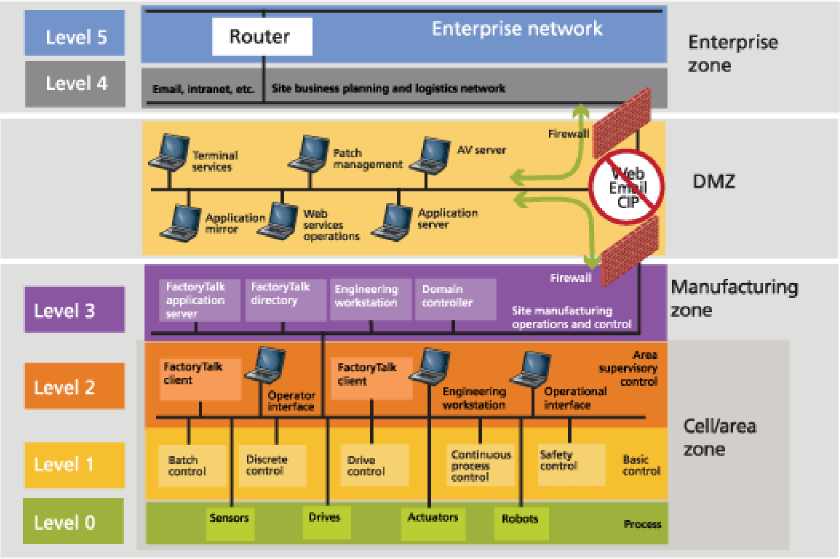
Enterprise Security Zone



Purdue Model

- Industrial Demilitarized Zone
  - Sits between levels 3 and 4
  - This zone provides common services needed by both traditional IT and industrial systems (databases, web servers, etc)
  - This zone contains security devices such as firewalls

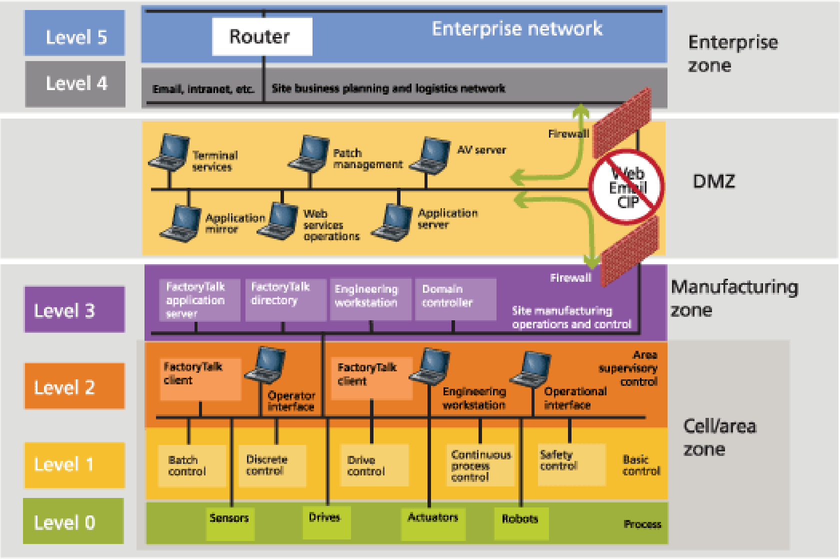
Industrial Demilitarized Zone



Purdue Model

- Manufacturing Zone
  - Contains level 3
  - This zone houses systems such as historians, OPC servers and engineering workstations

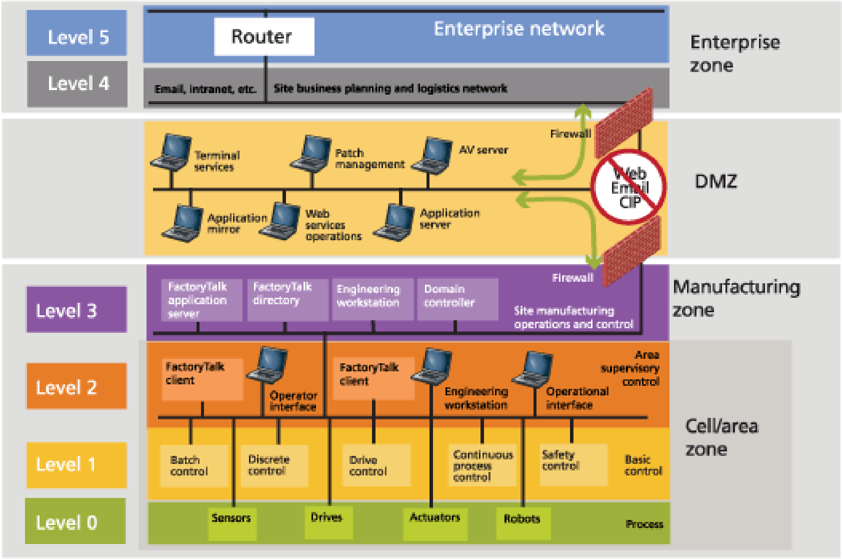
Manufacturing Zone



Purdue Model

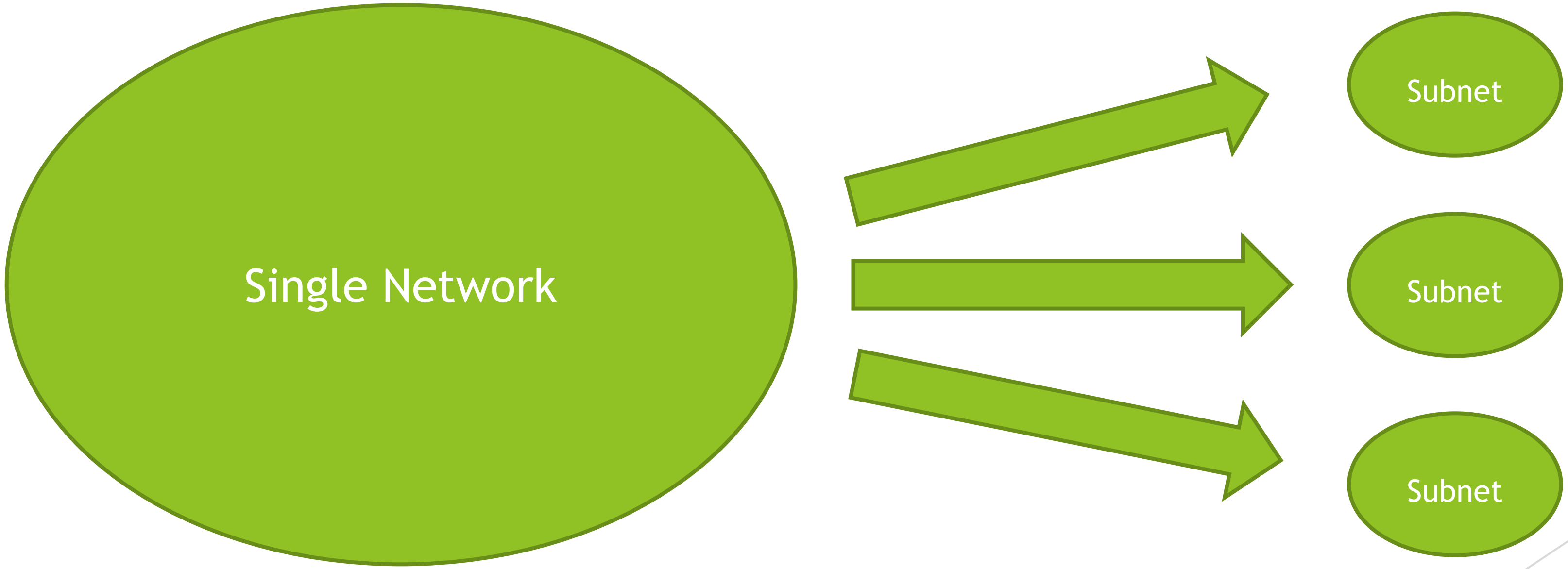
- Cell/area Zone
  - Contains levels 0, 1 and 2
  - This zone contains operator HMI devices, PLCs, sensors and electrical controls

Cell/Area Zone



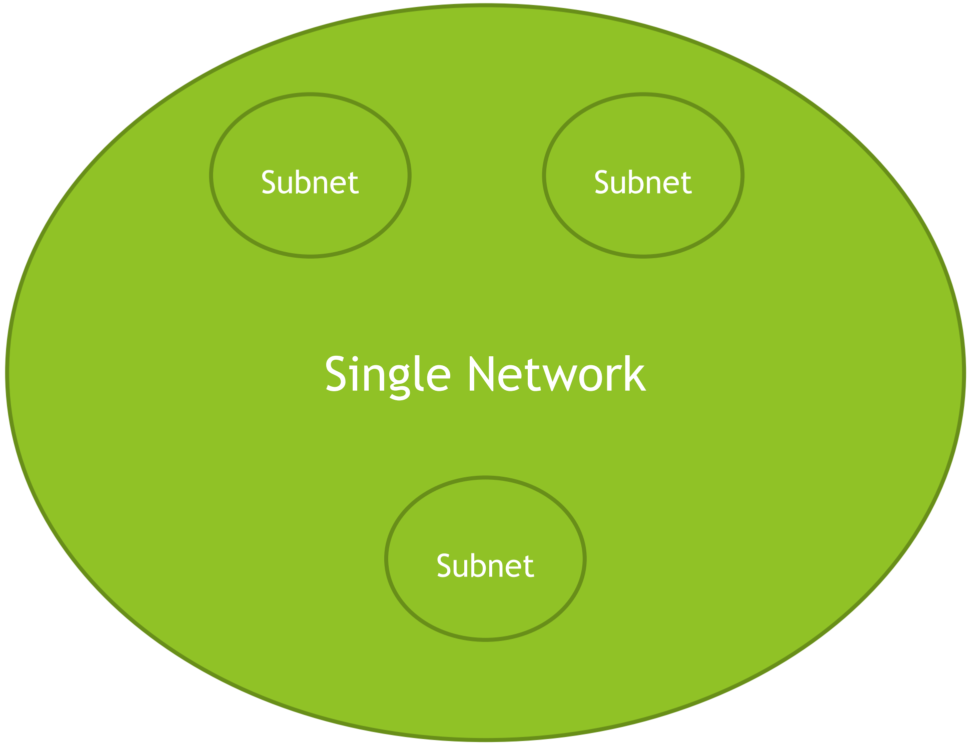
Network Segmentation

- Network segmentation occurs when a computer network is split into multiple subnets or segments
- Network segmentation can be done by physically separating a large network into smaller subnetworks



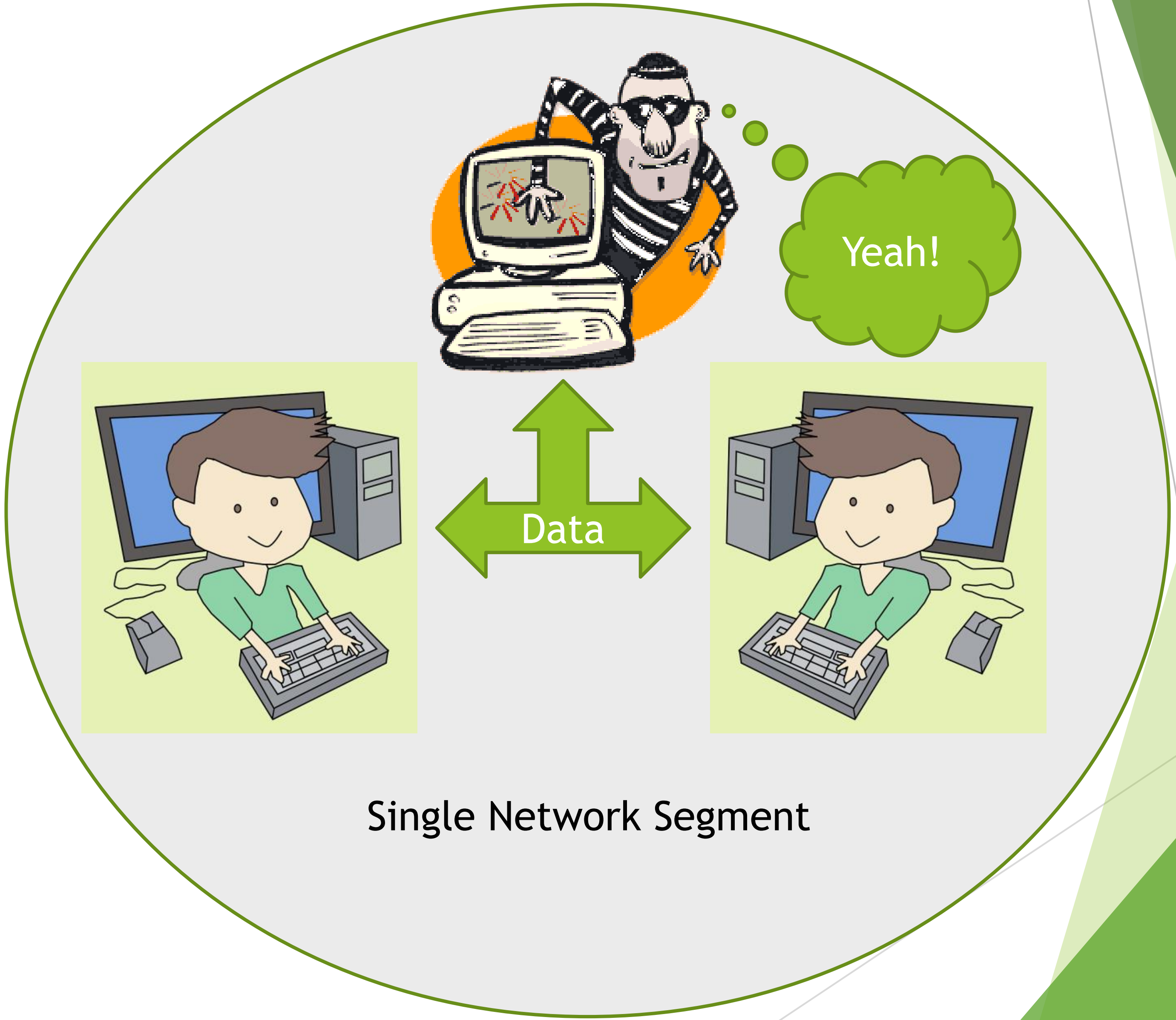
Network Segmentation

- Network segmentation can be done by logically separating a large network into smaller subnetworks using virtual LANs (VLANs)



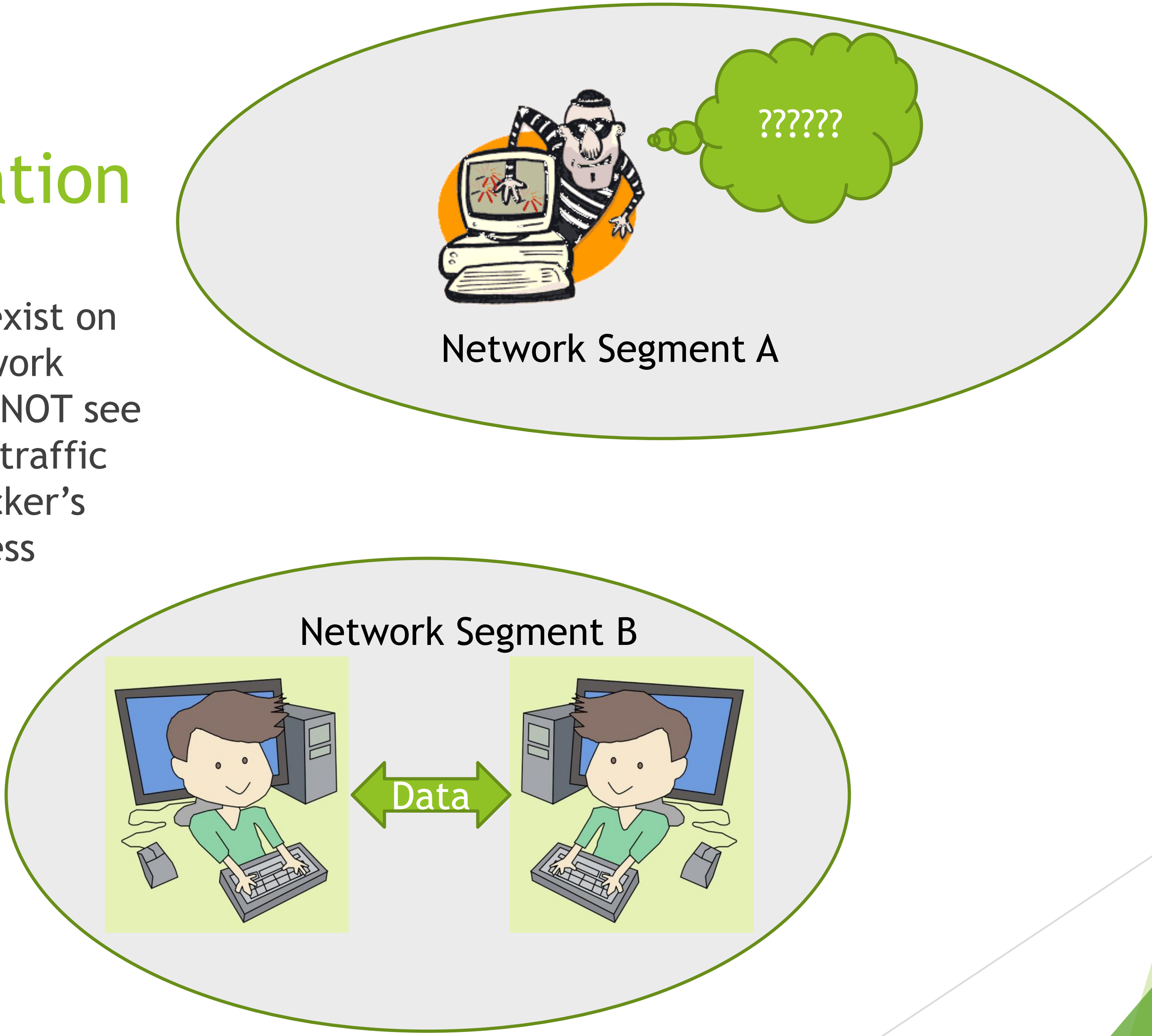
Network Segmentation

- Devices that exist on the same network segment CAN see one another's traffic potentially allowing a hacker to access sensitive data



Network Segmentation

- Devices that exist on different network segments CANNOT see one another's traffic blocking a hacker's ability to access sensitive data



??????

Network Segment A

Network Segment B

Data

For More Information

- For further information go to https://www.nl.northweststate.edu/camo or contact:
  - Tony Hills – thills@northweststate.edu – 419-267-1354
  - Sarah Stubblefield – sstubblefield@northweststate.edu – 419-267-1512
  - Mike Kwiatkowski – mkwiatkowski@northweststate.edu – 419-267-1231

Made possible through support from the National Science Foundation (NSF) award number 1800929