ISERink

Module 5

ISERink Introduction

- Purpose
  - Provide a safe learning environment
  - Provide a way for students to get direct access to technology, which helps learning
    - While avoiding expense of schools obtaining and operating additional equipment
  - Provide a means for students to prepare and defend an IT environment at the IT-Olympics cyber defense competition (CDC).

Assumptions

- Students have access to computers at school and/or at home.
- These computers can access the Internet
- Internet access is reliable and is a broadband service
- Computers have Microsoft’s remote desktop client software installed.

Intended Uses

- Hands-on activities
- Cyber Defense Competition
- Not:
  - Online shopping
  - Personal uses of social media
  - Doing homework for your regular classes
  - Doing anything else that may require to you use a username and password or download materials you do not want others to have.

Playground Limitations

- Multiple schools are sharing the same VM server.
- VM server resources are fixed.
- No resource limits have been established
  - Any team consuming too many resources will be restricted
- Idle (running but not being actively used) VMs consume resources
  - 35 running VMs are too many

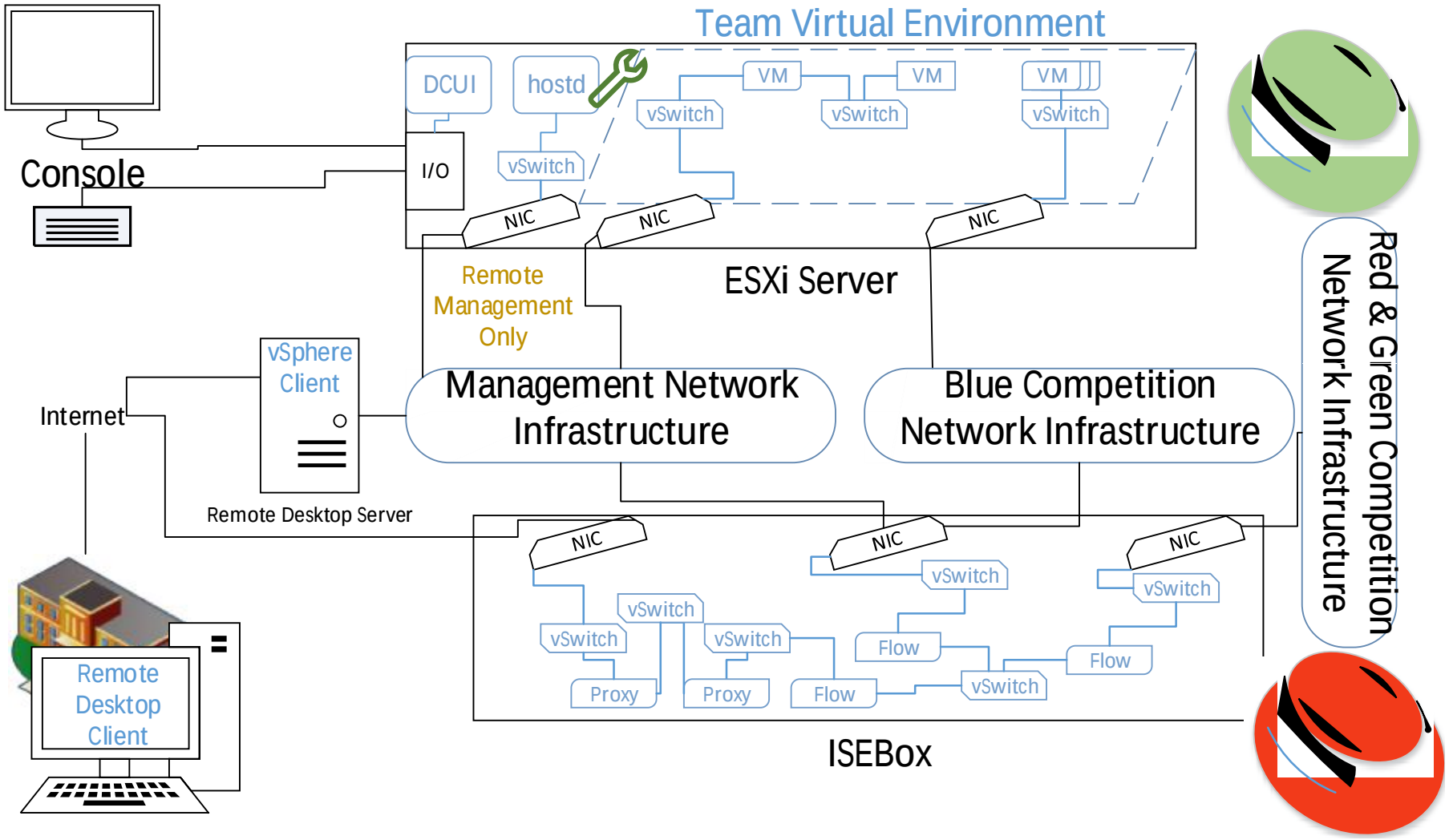
ISERink Limitations

- VM environment is common for all students of a team
  - Team members will need to coordinate naming of systems, IP addressing, network topology
  - It will not be practical for every student to be doing hands-on activities simultaneously
    - Depending on team size you may need to pair-up with a fellow student and take turns
    - Learn together and help each other avoid or correct mistakes

ISERink Limitations

- Consider OS resource consumption
  - Newer OS versions tend to be bigger consumers than their predecessors
  - Feature rich OS types Windows tend to be bigger consumers than simpler OS types like Linux
  - Isolating services can provide good security, but the tradeoff is resource consumption.
    - Heavy-weight OS types like Windows Server 2012 should be highly leveraged – use them for many services

ISERink Architecture



Functional Orientation

- ISERink features worth understanding
  - Inbound Access
  - Virtual Networking
  - Virtual Machine Internet Access
  - Operational Control of VMs
  - Mechanics of VM construction

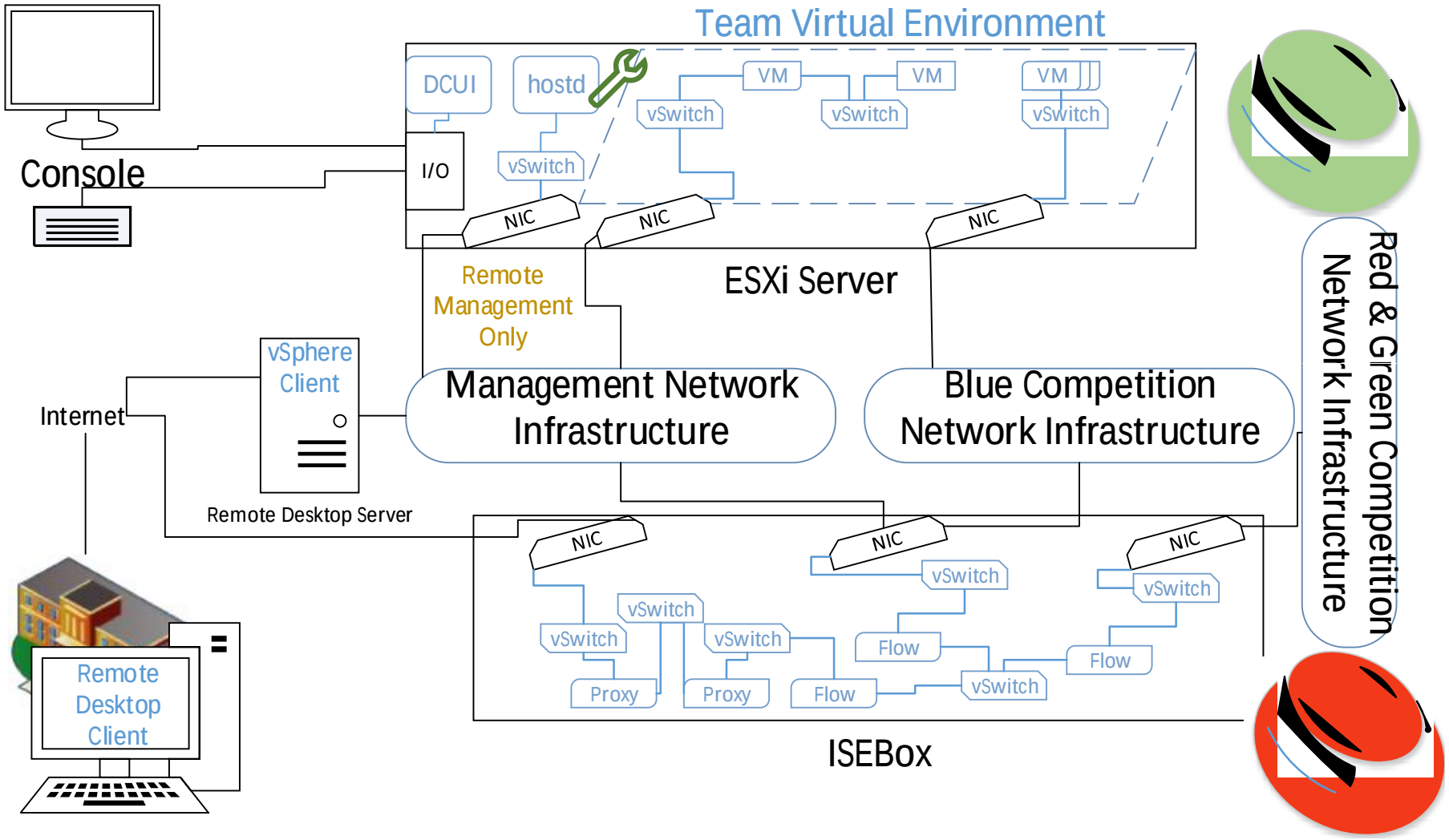
Inbound Access

- Requires Internet connectivity
- Requires use of Microsoft's Remote Desktop Client
  - Standard Windows accessory
  - Available for Macintosh
- Two management options
  - vSphere to manage virtual environment and access a VM's console
  - Remote connections to VMs

Inbound Access

- Management options available by remote desktop connection to remote desktop server.
  - vSphere client is installed on server
  - Remote connections to VMs will require
    - Starting the remote desktop client or other appropriate client available on the remote desktop server
    - Knowing VMs ip address or DNS name
    - VM is connected to a vswitch that is connected to the management network switch

ISERink Architecture



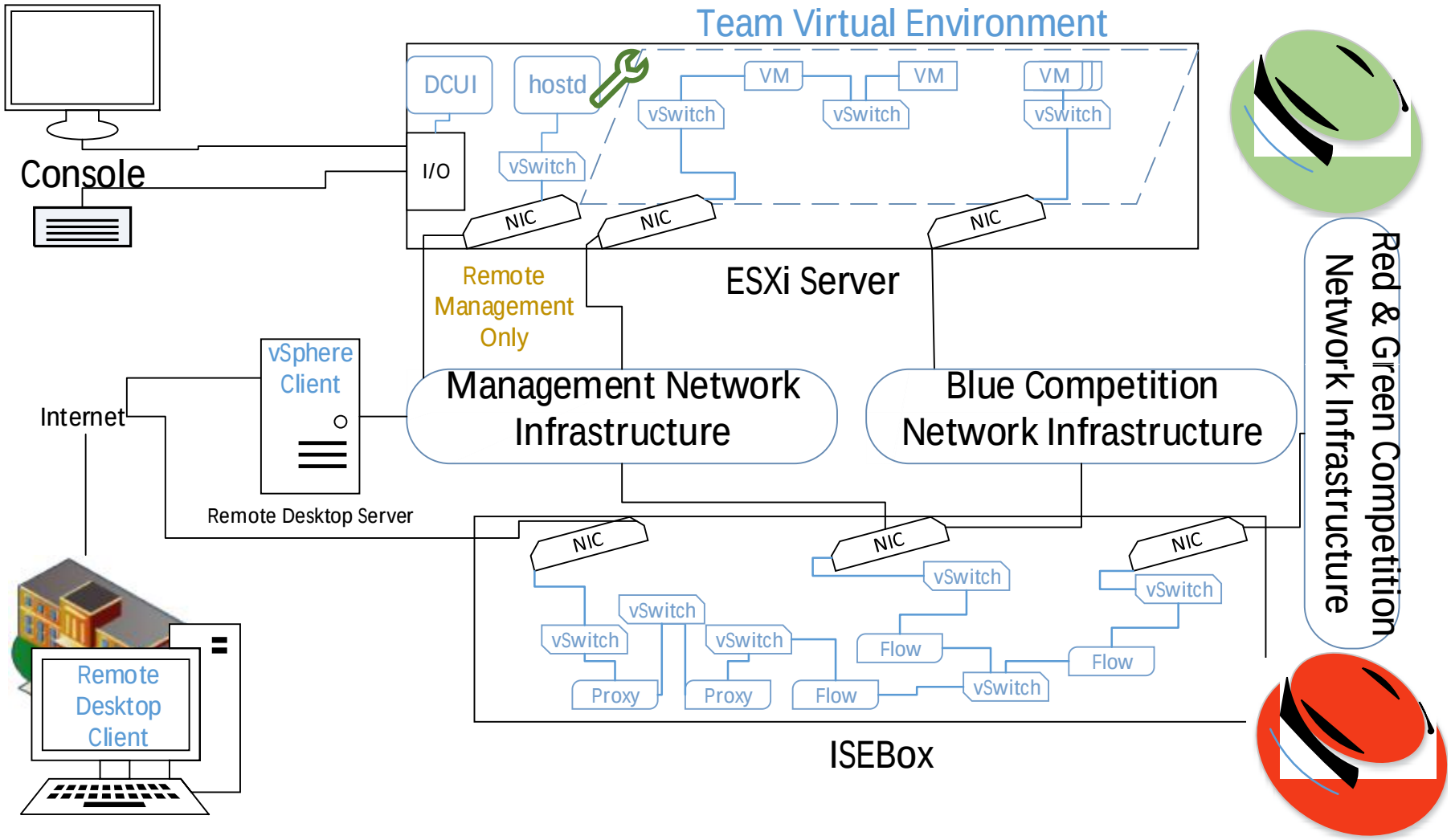
Virtual Networking

- VMs attached to a common switch share a communication channel
  - You will need:
    - The VMs must be in the same IP subnet
    - Know the IP address or DNS host name of destination
- No virtual routers exist
  - Routing function is provided by a VM assigned two virtual NICs
  - OS must be configured to forward packets from one NIC to the other
  - Correct routing table is needed

Virtual Networking

- VMs can reach the outside of the virtual environment if they are attached to a switch that is attached to an actual NIC.
  - Without a path to an actual NIC, network traffic will not leave the ESXi platform.
  - Pay attention to which network the NIC is attached. This affects addressing and routing.
- VM assignment to switch(es) requires vSphere client

ISERink Architecture



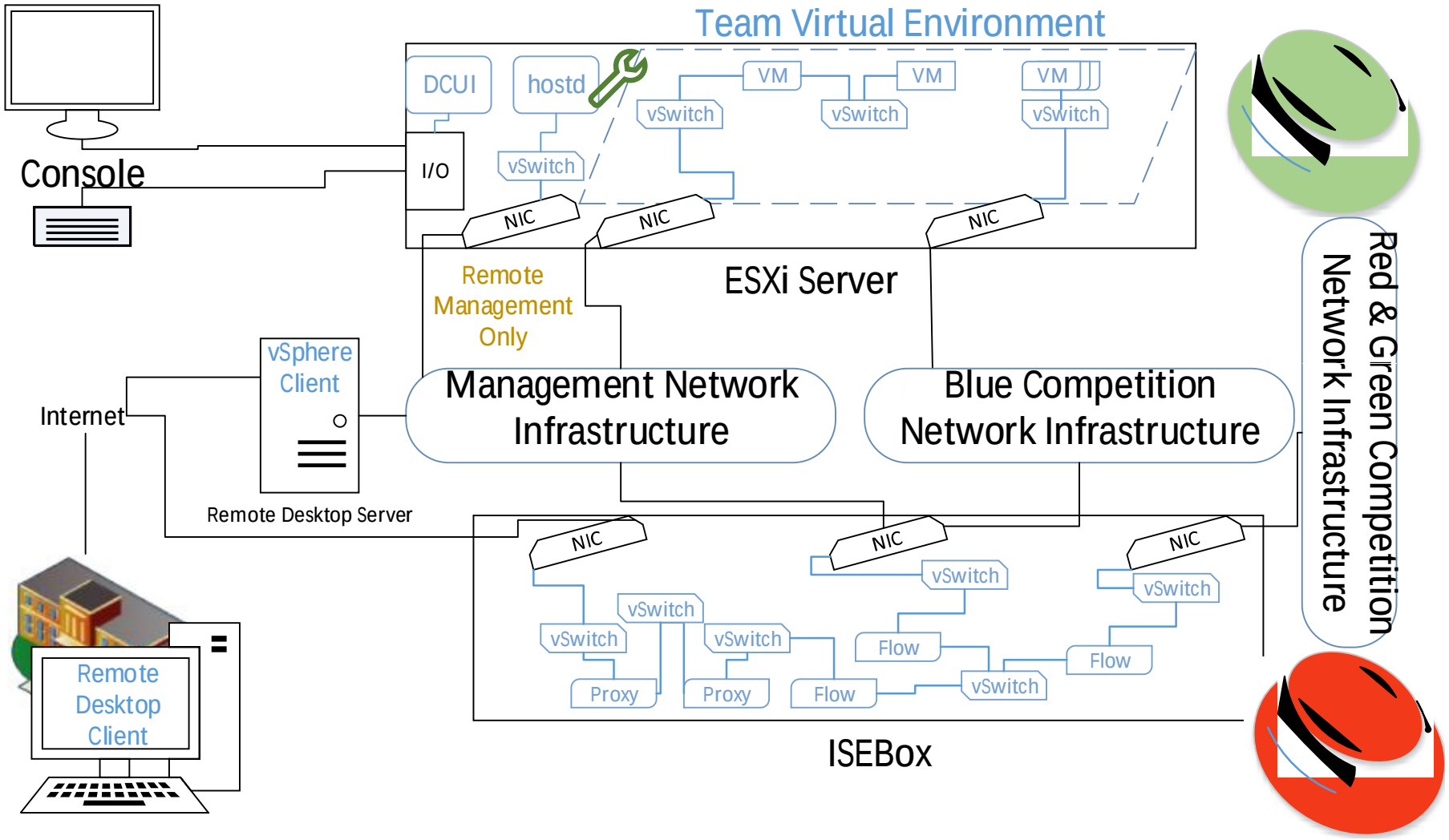
[Content Notes] To be developed

- Virtual switch creation and assignment demo segment is needed

VM Internet Access

- In the playground, VMs cannot send network traffic directly to the Internet
- The remote desktop protocol (RDP) NIC is not a generic way out for VMs.
  - Only RDP sessions destined to the RDP server will succeed
- A VM direct traffic through the Blue Competition network to reach the Internet
  - This path is protected by a pair of proxies

ISERink Architecture



VM Internet Access

- Proxies are not transparent – browsers on VMs need to know about the inside proxy.
  - The IP address of the inside proxy is
  - Names of Internet sites will be resolved by proxies
- Internet services supported by the proxies are:
  - HTTP, HTTPS, FTP

VM Operational Control

- The “power switch” of a VM is managed from the vSphere client
  - Start/Running typically means the OS is either booting or is operational
  - Suspend/Resume– not your typical power option – the VM is not running or a running VM will be stopped but all the temporary operating information will be saved. Operational information will be restored when VM resumes.
  - Stop/Stopped means the VM is not functioning. This is like turning the power off. An operational VM will simply stop functioning. Be careful, many OS types should be shutdown using OS commands.

[Content Notes] To be developed

- Provide screenshot or demo segment showing VM power status and controls

VM Construction

- Basic ingredients
  - vSphere client
  - OS installation media
    - CDs/DVDs
    - Image files of CDs/DVDs, common called ISOs
  - Resource commitments
    - Memory, CPU, disk space, network
  - Machine name (OS requirement)
  - Networking configuration details (OS requirement)
  - Password for administrator account (OS requirement)
  - Or, an existing VM can be duplicated

[Content Notes] To be developed

- Demonstrate vSphere client initial sequence of building a VM
- Stop segment after OS ISO is starting to boot

Getting Started

- Here are a few details you need
  - You first connect to the RDP server.
    - Its name is ….
  - Use the remote desktop client on your computer to connect
  - vSphere client installed on RDP server
    - Start it and connect to the system given to your teacher.
  - You need to authenticate to the RDP server and ESXi system. See your teacher for account information.

Account Explanation

- RDP and ESXi accounts are the same account – not just in name
  - RDP and ESXi share the same user directory
- Generic accounts are a bad security practice – no accountability, because more than one person is using it.
  - But, it simplifies account setup and management
- Password can be changed using RDP server