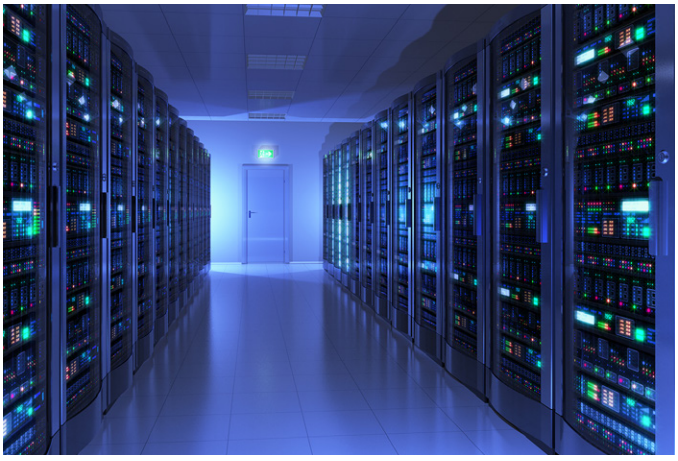
MISSISSIPPI STATE UNIVERSITY

DASI

Netmapper Project

CHALLENGE

The Netmapper Project helps with the problem of network complexity and reproducibility. In this age of the Internet-of-Things, even a small business network can get complicated over a short period of time. Networks today are much larger than just computers connected together and can contain multiple routers, VPNs, firewalls, switches, printers/FAX/copy machines, wireless devices, NAS storage boxes and computers. In addition to all of the above devices, the network may contain devices with different operating systems such as Windows and Linux. Whether this network is administered in-house or is out-sourced, it can be very difficult to keep track of what is attached to it and what effect attaching something new to the network will have. Netmapper can scan these devices, determine connectivity and operating system type, and in some cases even log in to the device to determine what services and software are installed on the device.



Netmapper, a tool to aid in determining network topology, visualization, and virtualization.

CURRENT PRACTICE

Networks are generally built by hand with an initial planning stage to resolve issues like IP address ranges, subnets, and connection to the outside world. Testing usually involves testing on the actual network since network virtualization is still fairly new. Parts of a network may be virtualized and tested such as a server or small subnet and there may be a small physical testbed.

TECHNICAL APPROACH

The Netmapper program can map out a network to show what devices are attached to the network and produce a visual roadmap of the network for an administrator to examine. Netmapper will also allow the administrator to save the network scan output. A difference check of a saved output can be compared against a later scan to see if there are any changes to the network over that period of time. The network scan can also be used to compare the live network against a duplicate virtual network to verify that they are equivalent. The Netmapper scan will not only identify what devices are on the network, it will also identify: server types, operating system types and installed software. This allows the administrator to build a duplicate virtual network that can be stressed and tested without making the live network unavailable to users.

IMPACT

The Netmapper program allows the administrator to understand how the network is put together and see where problems might be occurring in the network due to what is connected at or near that point. It can show where potential bottlenecks or weak points are located in the network and allow the administrator to design contingency plans for the network.

Netmapper allows the administrator to see what devices might have been added to or removed from the network. It also shows what devices are accessible on the network. If a device that was previously accessible is still present but no longer accessible to Netmapper, it could be indicative of a problem. If there is a new device on the network that is unknown, it should be identified and understood.

Network stressing might involve overloading the network with traffic or doing intrusion testing to see how it responds to a new set of firewall rules. It might also involve adding a new Domain Controller or DNS server to the network to see how it will respond. A virtual network allows the administrator to do this kind of testing without interfering with the users on the live network.

Contacts

Bob Reese
rbr@msstate.edu

Patrick Pape
pape@dasi.msstate.edu

Phillip Akers
pa19@msstate.edu