Network Security

Objective: The objective of this workshop is to examine the key concepts, protocols and the policies involved in establishing and maintaining security for a network, and building an understanding and familiarity with their operation. Device and network infrastructure security is examined with a focus on different layers to establish a robust, stable and secure network and protect the data and processes that occur in the network.

.

Introduction to Networking-

- Brief history of computers and networks
- What is a LAN?
- What is a WAN?
- When do you use a LAN?
- When do you use a WAN?

Understanding the OSI Reference Model-

- Understanding each of the seven layers
- Using the OSI Reference model in network design and troubleshooting
- Mapping equipment and protocols to the appropriate layers

Common Topologies and Connection Options-

- Star Topology
- Tree Topology

- Mesh Topology
- Wireless Topology
- Network Cabling option
- Network Architecture
- Types of cables
- Connection rates and Terminology

Understanding Networking Protocols Including IPv4 and IPv6-

- IPv4 (formerly known as TCP/IP)
- Planning for your addressing need
- Choosing the right protocols for your network
- Understanding an IP address and subnet mask
- What is the default gateway
- Configuring IP addresses on your network
- IP Version 6 (IPv6)
- Address Resolution Protocol (ARP)
- WAN protocols
- Tunneling protocols
- Security protocols

Network Security-

- Physical security
- Passwords
- The "run-as" command in Windows 8 and Server 2012
- Port scanning
- Baseline security analyzer
- Windows Server 2012 Security Configuration Wizard
- Classification of Firewalls
- Understanding encryption, including PKI and SSL/TLS