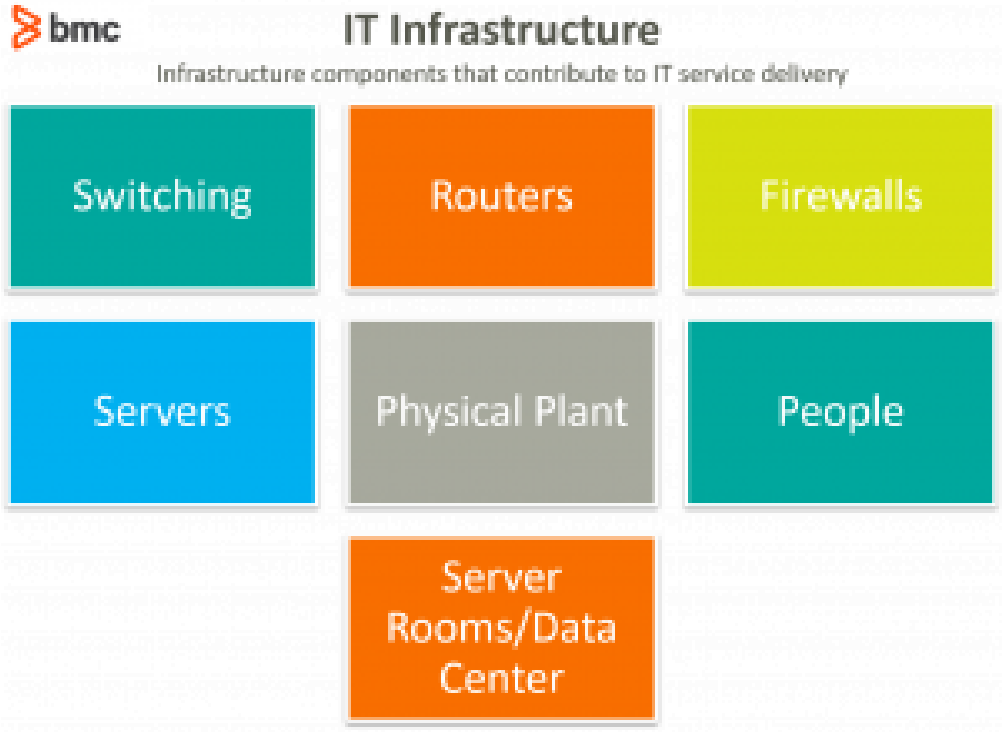
IT INFRASTRUCTURE AND COMPONENTS: AN INTRODUCTION

IT Infrastructure

I like to think of infrastructure as everything from wall jack to wall jack. Thinking of infrastructure in this manner enables effective conversations with those who are less familiar with the various components.

The term IT infrastructure is defined in ITIL as a combined set of hardware, software, networks, facilities, etc. (including all of the information technology related equipment) used to develop, test, deliver, monitor, control, or support IT services. Associated people, processes, and documentation are not part of IT Infrastructure.



Switching

A network switch is the device that provides connectivity between network devices on a Local Area Network (LAN). A switch contains several ports that physically connect to other network devices - including other switches, routers and servers. Early networks used bridges, in which each device "saw" the traffic of all other devices on the network. Switches allow two devices on the network to talk to each other without having to forward that traffic to all devices on the network.

Routers

Routers move packets between networks. Routing allows devices separated on different LANs to talk to each other by determining the next "hop" that will allow the network packet to eventually get to its destination.

If you have ever manually configured your IP address on a workstation, the default gateway value that you keyed in was the IP address of your router.

Firewalls

Firewalls are security devices at the edge of the network. The firewall can be thought of as the guardian or gatekeeper.

A set of rules defines what types of network traffic will be allowed through the firewall and what will be blocked.

In the simplest version of a firewall, rules can be created which allow a specific port and /or protocol for traffic from one device (or a group of devices) to a device or group of devices. For example: if you want to host your own web server and limit it to only web traffic, you would typically have two firewall rules that look something like this:

Source	Destination	Port / Protocol	Description
any	10.1.1.100	80 / http	Web traffic in
any	10.1.1.100	443/ https	Secure web traffic in

The source is the originating device. In this case, any means 'allow any computer to communicate'. Destination is the specific IP address of your internal web server. Port/Protocol defines what type of traffic is allowed from the source to the destination. Most firewall devices allow for a description for each rule that have no effect on the rule itself. It is used only for notes.

Firewall devices can get complicated quickly. There are many different types of firewalls which approach managing traffic in different ways. Detailed firewall capabilities and methods are beyond the scope of this post.

Servers

A network server is simply another computer, but usually larger in terms of resources than what most people think of. A server allows multiple users to access and share its resources. There are several types of servers, with the following being among the most common:

- A file server provides end users with a centralized location to store files. When configured correctly, file servers can allow or prevent specific users to access files.
- A directory server provides a central database of user accounts that can be used by several computers. This allows centralized management of user accounts which are used to access server resources.
- Web servers use HTTP (Hyper Text Transfer Protocol) to provide files to users through a web browser.
- There are also application servers, database servers, print servers, etc.

Physical Plant

The physical plant is all of the network cabling in your office buildings and server room/data center. This all too often neglected part of your infrastructure usually is the weakest link and is the cause of most system outages when not managed properly. There are two main types of cabling in the infrastructure: CAT 5/6/7 and fiber optic. Each type of cabling has several different subtypes, depending on the speed and distance required to connect devices.

People

By the strict ITIL definition, people are not considered part of the network infrastructure. However, without competent, well-qualified people in charge of running and maintaining your infrastructure, you will artificially limit the capabilities of your organization. In larger organizations, there are specialty positions for each of the areas mentioned in this article. In smaller organizations, you will find that the general systems administrator handles many of the roles.

Server Rooms / Data Center

The server room, or data center (in large organizations), can be thought of as the central core of your network. It is the location in which you place all of your servers, and it usually acts as the center of

most networks.

Infrastructure Software

This is perhaps the most “gray” of all infrastructure components. However, I consider server operating systems and directory services (like MS Active Directory) to be part of the infrastructure. Without multi-user operating systems, the hardware can't perform its infrastructure functions.

Additional Resources