

# NETWORK ADMINISTRATION AND SECURITY

## NETWORK ADMINISTRATION

*Network administration* normally includes the deployment, monitoring and maintaining the networks as well as *configuring devices such as* routers, switches, firewalls, servers and other services.

Other tasks includes in the job description of a network administrator are:-

- Network IP addressing, creating VLANs, VPNs
- Configuring switching and routing protocols,
- Configuring Authentication, Authorization and Auditing (AAA) of the directory services
- Backups and restoration procedures
- User support
- Monitoring the network i.e. logs and audit trails
- Fixing hardware and software problems
- Maintaining an inventory of network assets
- Troubleshooting and fixing network problems

### 1. MAINTENANCE OF THE NETWORK RESOURCES

It also includes the *maintenance of the network resources*, such as hosts, servers, communication links, and printer settings, settings of personal computers, virus protection servers and providing the server access to the client computers. Some of the tasks here are:-

#### ***a) Managing Group Policy Objects (GPOs)***

Systems administrators use GPOs to configure settings for multiple users and computers. After configuration of the settings, an Admin need to think about issues such as GPO maintenance. For example, there is need to have a backup of these configurations just in case something happens to the servers.

The main tool you'll use for managing GPOs is the *Group Policy Management Console* (GPMC), we will see and use it during the practical. You can use this console to back up, restore, import, copy, and migrate. You can also use this console to delegate GPO management tasks.

### ***b) Monitoring servers***

Monitoring a server using data collector sets, alerts, and events enables you to keep an eye on the server's performance and configuration. Although effective monitoring is unlikely to stop a server from ever experiencing problems, it often provides warning signs about developing problems, giving you a chance to resolve them before they cause a service disruption.

During the practical we will learn how to manage alerts, monitor events, and perform network monitoring.

## **2. MONITORING OF THE NETWORK SERVICES**

It also includes the *monitoring of the network services* such as performance, audit trails, server alerts. Their work can also include the maintenance of the network authorization as well as network backup systems.

Admins are also responsible for providing network management functions such as providing network/system support services; they ensure that the network is used efficiently, and they also ensure prescribed service-quality objectives are met. Some of the tasks here are:-

### ***a) Performing network monitoring***

*Network monitoring* enables you to track how a computer interacts with the network. Through network monitoring, you can determine which services and applications are using specific network interfaces, which services are listening on *specific ports*, and the *business* of traffic that exists.

There are two primary tools through which you can perform network monitoring on computers running Windows Servers

- Resource Monitor
- Message Analyzer

We will get more details during the practical

### ***b) Configuring and monitoring audit reports***

We have audit policies in a Group Policy Object (GPO) in the windows servers and Admins can configure these *audits policies*. These policies are many so the Administrators pick what they are interested in as we will see.

## **3. TROUBLESHOOTING**

Network specialists also work on network security and design, particularly *troubleshooting* network related problems.

### ***a) LAN & Network Troubleshooting***

Troubleshooting the local area network means *identifying and sorting out network problems* for getting the *optimized performance*. In order to troubleshoot the problem in the LAN, it is important to monitor the LAN to identify the problems. LAN monitoring can be accomplished with the network management computer or general network sniffers. *Protocol Analyzer* provides various LAN troubleshooting solutions over the TCP/IP networks.

LAN/TCP/IP troubleshooting can often be tricky and the troubleshooting scenarios includes finding duplicate IP addresses on the network computers, misconfigured network applications, non-optimized network devices, low service performance, cabling problems, faulty LAN cards and network switches, viruses and spyware attacks, misconfigured firewall, security issues, DNS/DHCP problems, proxy server's settings and overloading of the network servers with the number of software applications.

The problems in the Local Area Network can be caused by a number of reasons thus the importance of understanding the LAN infrastructure, network hardware, software, user access rights and preferences and the major configurations of the network.

The best practice is to make inventory of all the resources of your LAN such as number of workstations, software installed and network hardware.

### **BEFORE YOU START TROUBLESHOOTING**

Before you do anything, before you touch anything else:

1. Write *down a list of everything* that has changed. Chances are high your problem lies with the change or a side-effect of the change.
2. Think it through first - running around doing things with no plan is a recipe for another disaster.
3. be methodical. Start at one place and work slowly out from there. Test each step and *MAKE NO ASSUMPTIONS*. Check everything.

#### FIRST THINGS TO LOOK OUT

1. Know the NORMAL look of *LEDs*, flashing light and other indicators are. We typically look at these indicators only when something is NOT working and then assume they are telling us things that they probably are not.
2. Use elimination method to get rid of possible errors, e.g. using another network cable, a laptop etc.

#### ***b) Diagnosing Network Problems***

To diagnose a network problem you just start to verify the connections from a known starting point (your PC) moving progressively further into the network until you find the problem:

#### **Always start with your own PC (If it regularly fails).**

Issue a *ping* to your own PC (get it's address here). If this fails restart your PC and try the failing operation again.

Check with someone else in the office - if you are the only person having the problem you have already isolated it to your PC or its wiring. Now you only have to find it - in all cases it is not a remote network problem.

1. Restart your PC - 90% of all problems disappear after the boot.
2. Check the link LEDs on your PC LAN card (if it has any).
3. Check your cabling.

#### NOW CHECK YOUR LOCAL NETWORK.

- Your local PC is OK - someone else has same problem.
- Ping the local router (its address is the Default Gateway IP that you get here). If this fails we may have a problem with the local LAN or the router.

- Now you have to move from your desk.
- Find your router and Hub/Switch check the LED displays. If they are not normal remove and immediately replace the power connection or switch the unit OFF then ON.
- Go back to your PC and retry to ping your local router and then repeat the failing operation.

### WHAT IS PING AND WHAT DOES IT DO?

'Ping' (actually its full name is 'ICMP Echo request') is a simple command that may be issued from the DOS Command Prompt (*Start/Run/cmd/OK*). Ping tells you if you can, or cannot, contact an IP address (another device). Ping sends a small message to another computer which causes the receiver to echo back the same message (the message pings forward and backward). Ping is the simplest and most useful diagnostic tool to become familiar with and well worth a few minutes experimentation. To use Ping;

1. Run a command prompt (sometimes called a 'DOS box') (Start->Programs->Command Prompt (MSDOS) or Start->run enter command -> OK
2. Type:
3. Ping xxx.xxx.xxx.xxx

Where xxx.xxx.xxx.xxx is the IP address that you want to check followed by ENTER. You can also use a URL with a ping:

Ping www.sitename.com (domain name)

For this format to work the DNS service must be contactable and working.

4. If ping works (you have successfully sent a message to the remote computer and received a response) you should get up to 4 replies of the form:
5. Reply from xxx.xxx.xxx.xxx: bytes=32 time=yys TTL=zz

Where xxx.xxx.xxx.xxx is the IP address that is responding, yys is the time (yy) in milliseconds (ms) that the ping took and zz can be used to calculate the number of routers that it passed through on its journey.

6. If the Ping fails you will see a message like:

Request timed out (connection or routing error)

OR

Host unreachable (routing error)

OR

Network unreachable (routing error)

### **Check the remote network.**

Your local router is OK - we can reach it and its LEDs are normal.

Issue a *tracert* command to 64.58.76.176 (www.yahoo.com) NOTE: always use the *-d* option with this command and you can abandon it using CTRL+C when you see two three consecutive rows of '\*'.  
Note the hop number of the first failure and contact your service provider.

### **What is a trace route (or tracert) command?**

A *tracert* (or trace route) command tells you all the routers between your PC and the place you want to trace to (can be either an IP address or a URL e.g. www.yahoo.com)

To run a tracert command:

1. Click start->programs->Command Prompt (or Start->run enter **cmd** then OK)
2. Enter:
3. tracert www.xxx.xxx.xxx -d' (or www.yahoo.com -d)

Replace the IP address with the one you want or use the URL of the site if you know it. **NOTE:**

The -d in the command line stops a DNS lookup and speeds up the command considerably.

4. tracert outputs the following display:

5. x xx xxx xxxxx ee. ee. ee. ee

### **Where:**

**x** is the hop number starting from 1

**xx** is the time in milliseconds that the first attempt took to reach the site. Asterisk means it timed out.

**xxx** is the time in milliseconds that the second attempt took to reach the site. Asterisk means it timed out.

xxxx is the time in milliseconds that the third attempt took to reach the site. Asterisk means it timed out.

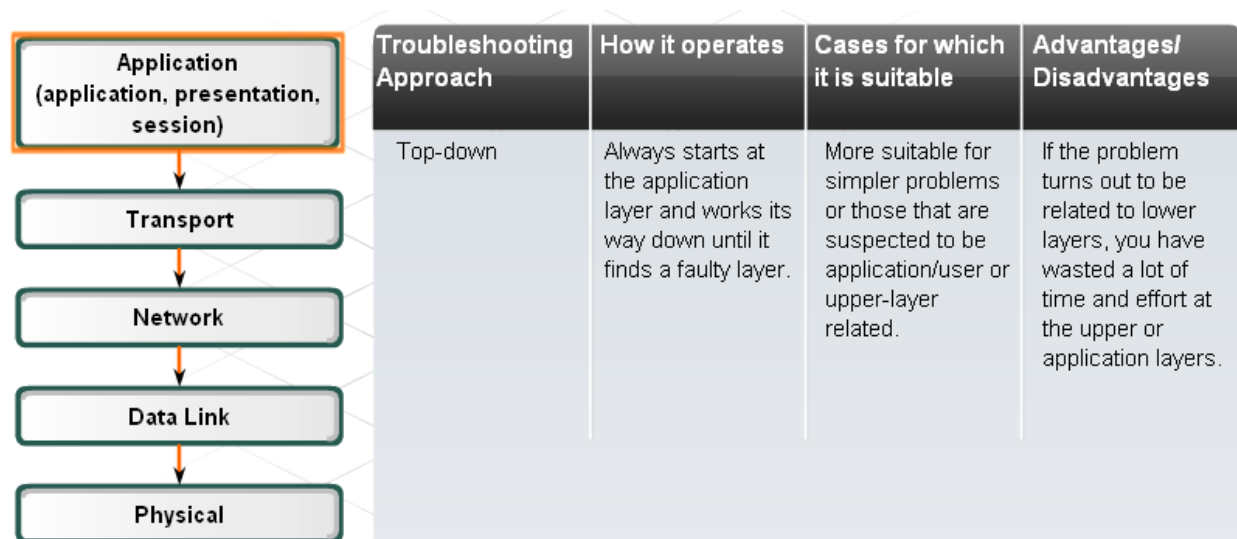
ee.ee.ee.ee is the IP address of the router at this hop number.

### *c) Approaches to Structured Troubleshooting*

There are several different structured troubleshooting techniques available, including:

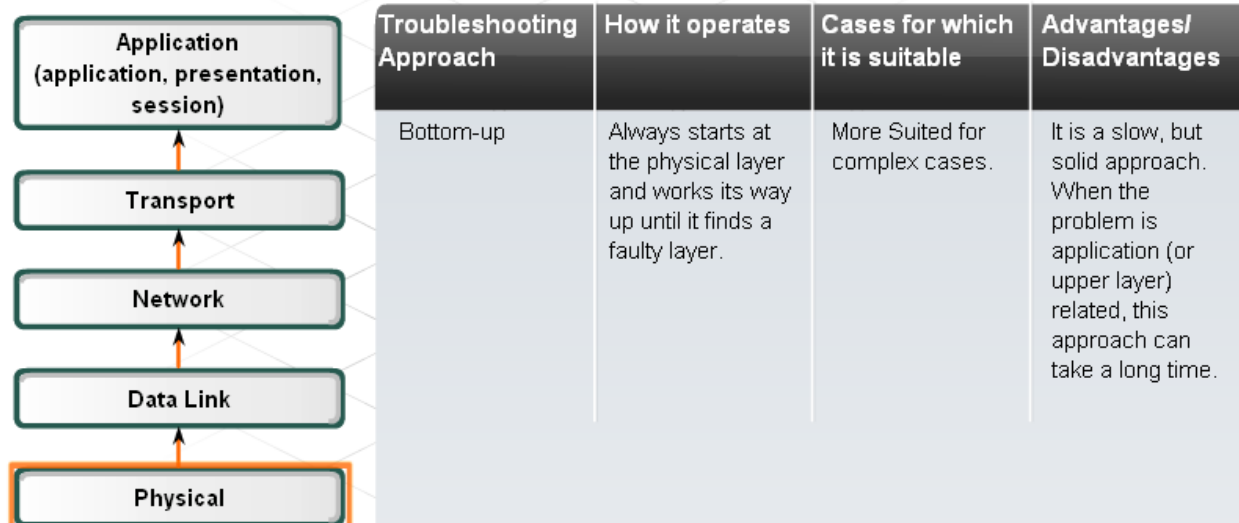
#### *a) Top-down*

Top-down starts with the application layer and works down. It looks at the problem from the point of view of the user and the application. Is it just one application that is not functioning, or have all applications failed? For example, can the user access various web pages on the Internet, but not email? Do other workstations have similar issues?



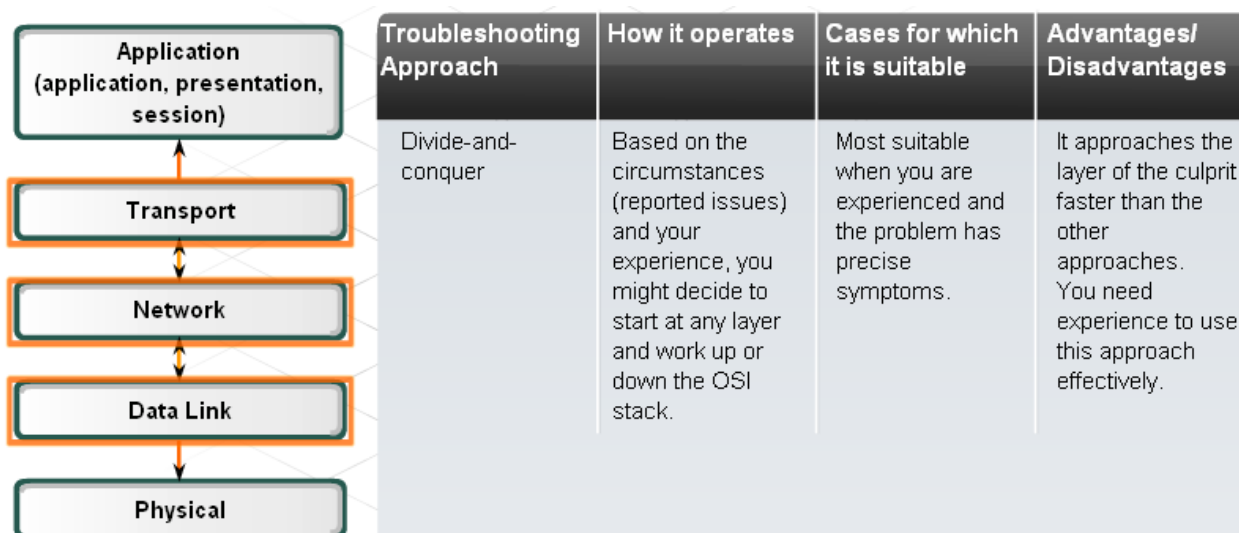
#### *b) Bottom-up*

Bottom-up starts with the physical layer and works up. The physical layer is concerned with hardware and wire connections. Have cables been pulled out of their sockets? If the equipment has indicator lights on, are they on or off?



### c) Divide-and-conquer

Bottom-up starts with the physical layer and works up. The physical layer is concerned with hardware and wire connections. Have cables been pulled out of their sockets? If the equipment has indicator lights, are they on or off?



All of these structured approaches assume a layered concept of networking. An example of a layered approach is the OSI model, in which every function of communication is broken down into seven distinct layers. Using this model, a troubleshooter can verify all functionality at each layer until the problem is located and isolated.















The structure of these approaches makes them ideally suited for the *novice* troubleshooter. More experienced individuals often bypass structured approaches and rely on instinct and experience. They may use less structured techniques such as trial and error or substitution.

As computer networks expands, more computer support specialist and system administrators may be able to connect to the customers remotely using modems, laptops, emails and the internet to provide the support to the end users. Systems and network administrators can also *administer and configure the servers remotely*.

The main job description of a network administrator is to *maintain LAN* and connect computers in the same office building. You could even maintain the vast servers, which host the websites and these servers are called web servers.

Being a network administrator you must have a *good knowledge of computer hardware*, software and the network devices such as router, switches, hubs, modems and NIC cards. Additionally, you will have to constantly update yourself with the latest advancements and updates in this field by taking certification courses by Microsoft

 <b>Microsoft Certified: Azure Administrator Associate</b> Requirements: Exam AZ-104 Azure administrators implement, manage, and monitor an organization's Microsoft Azure environment.	 <b>Microsoft Certified: Azure for SAP Workloads Specialty</b> Requirements: Exam AZ-120 Architects or engineers for Azure for SAP Workloads partner with cloud administrators, cloud database administrators, and clients to implement solutions.	 <b>Microsoft Certified: Azure Virtual Desktop Specialty</b> Requirements: Exam AZ-140 Candidates for the Azure Virtual Desktop Specialty certification are Microsoft Azure administrators with subject matter expertise in planning, delivering, and managing virtual desktop experiences and remote apps, for any device, on Azure.
 <b>Microsoft Certified: Azure Stack Hub Operator Associate</b> Requirements: Exam AZ-600 Candidates for the Azure Stack Hub Operator Associate certification are Azure administrators or Azure Stack Hub operators who provide cloud services to end users or customers from within their own datacenter using Azure Stack Hub.	 <b>Microsoft 365 Certified: Messaging Administrator Associate</b> Requirements: Exam MS-203 Microsoft 365 messaging administrators deploy, configure, manage, troubleshoot, and monitor recipients, compliance, threat protection, and mail flow in hybrid and cloud enterprise environments.	 <b>Microsoft 365 Certified: Modern Desktop Administrator Associate</b> Requirements: Exam MD-100, MD-101 Modern desktop administrators deploy, configure, secure, manage, and monitor devices and client applications in an enterprise environment.

 <p><b>Microsoft 365 Certified: Security Administrator Associate</b></p> <p><b>Requirements:</b> Exam <a href="#">MS-500</a></p> <p>Microsoft 365 security administrators proactively secure Microsoft 365 enterprise and hybrid environments, implement and manage security and compliance solutions, respond to threats, and enforce data governance.</p>	 <p><b>Microsoft 365 Certified: Enterprise Administrator Expert</b></p> <p><b>Requirements:</b> Exam <a href="#">MS-100</a>, <a href="#">MS-101</a></p> <p>Microsoft 365 enterprise administrators evaluate, plan, migrate, deploy, and manage Microsoft 365 services.</p>	 <p><b>Microsoft 365 Certified: Teams Administrator Associate</b></p> <p><b>Requirements:</b> Exam <a href="#">MS-700</a></p> <p>Microsoft Teams administrators manage Microsoft Teams to facilitate efficient and effective collaboration and communication in a Microsoft 365 environment.</p>
 <p><b>Microsoft Certified: Identity and Access Administrator Associate</b></p> <p><b>Requirements:</b> Exam <a href="#">SC-300</a></p> <p>The Microsoft identity and access administrator designs, implements, and operates an organization's identity and access management systems by using Azure AD. They manage tasks such as providing secure authentication and authorization access to enterprise applications.</p>	 <p><b>Microsoft Certified: Information Protection Administrator Associate</b></p> <p><b>Requirements:</b> Exam <a href="#">SC-400</a></p> <p>The Microsoft information protection administrator plans and implements controls that meet organizational compliance needs. This person is responsible for translating requirements and compliance controls into technical implementation. They assist organizational control owners to become and stay compliant.</p>	 <p><b>Microsoft 365 Certified: Teams Voice Engineer Expert</b></p> <p><b>Requirements:</b> Exam <a href="#">MS-720</a></p> <p>Microsoft Teams voice engineers plan, design, configure, maintain, and troubleshoot an integrated communications solution at an organization.</p>

Others certifications for Network Administrators are:

### *CISCO*

- CCNA – Routing and Switching
- CCNP – Routing and Switching
- CCNA- Security
- CCDA – Cisco Certified Design Associate.
- CCENT – Cisco Certified Entry Networking Technician.

### *HUAWEI*

- HCIA
- HCIP
- HCIE

We have Security, Datacom, Routing & Switching, storage