# Overview of tools and troubleshooting

- Network troubleshooting tools are standalone or integrated solutions that help network administrators identify the root cause of a network issue in order to fix it.
- These network troubleshooting tools range from simple command line based troubleshooting utilities to more comprehensive and robust solutions that allows for a systematic, efficient and proactive approach to network troubleshooting.

- There are many programs and utilities available for Windows and UNIX operating systems that allow us to sniff, capture, trace, and analyze packets that are exchanged between our computer and the Internet.
- **Sniffing** is a process of monitoring and capturing all data packets passing through given **network**. Sniffers are used by **network**/system administrator to monitor and troubleshoot **network traffic**. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.
- Some of these, such as Wireshark and Ping Plotter have graphical user interface (GUI);
- others, such as traceroute, nslookup, dig, ipconfig, and ifconfig, are network administration command-line utilities.
- Any of these programs and utilities can be a valuable debugging tool for network administrators.

- Some of the basic network troubleshooting tools are as follows:
- Ping
- Tracert/ Trace Route
- Ipconfig/ ifconfig
- Netstat
- Nslookup
- Pathping/MTR
- Route
- PuTTY

- One of the tools that a host can use to test the liveliness of another host is the ping program. The ping program can also measure the reliability and congestion of the router. Ping can calculate the round-trip time.
- The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination.
- It can find the IP addresses of all the routers that are visited along the path. The program is usually set to check for the maximum of 30 hops (routers) to be visited.
- ipconfig is a console application program of some computer operating systems that displays all current TCP/IP network configuration values.
- **ifconfig**(interface configuration) command is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.

- The network statistics ( **netstat** ) command is a networking tool **used for** troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network. Both incoming and outgoing connections, routing tables, port listening, and usage statistics are common **uses for** this command.
- **nslookup** is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping .
- The PathPing command is a command-line network utility supplied in Windows 2000 and beyond that combines the functionality of ping with that of tracert. It is used to locate spots that have network latency and network loss.
- Route is a command used to view and manipulate the IP routing table

- PuTTY  is a free and open-source terminal emulator, serial console and network file transfer application. It supports several network protocols, including SCP, SSH, Telnet, rlogin, and raw socket connection.
- The echo request  and the echo reply pair of messages are used by a host or a router to test the liveliness of another host or router.
- The timestamp request and the timestamp reply pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.

# An introduction to Network Analyzers

# Network Analysis and Sniffing

- Process of capturing, decoding, and analyzing network traffic
  - Why is the network slow
  - What is the network traffic pattern
  - How is the traffic being shared between nodes
- Also known as
  - traffic analysis, protocol analysis, sniffing, packet analysis etc.

# Network Analyzer

- A combination of hardware and software tools that can detect, decode, and manipulate traffic on the network

- Available both free and commercially
- Mainly software-based (utilizing OS and NIC)
  - Also known as *sniffer*
  - A program that monitors the data traveling through the network *passively*

- Common network analyzers
  - Wireshark / Ethereal
  - Windump
  - Etherpeak
  - Dsniff
  - And much more….

# Network Analyzer

## Components

- Hardware
  - Special hardware devices
    - Monitoring voltage fluctuation
    - Jitter (random timing variation)
    - Jabber (failure to handle electrical signals)
    - CRC and Parity Errors
  - NIC Card
- Capture driver
  - capturing the data
- Buffer
  - memory or disk-based
- Real-time analyser
  - analyzing the traffic in real time; detecting any intrusions
- Decoder
  - making data readable

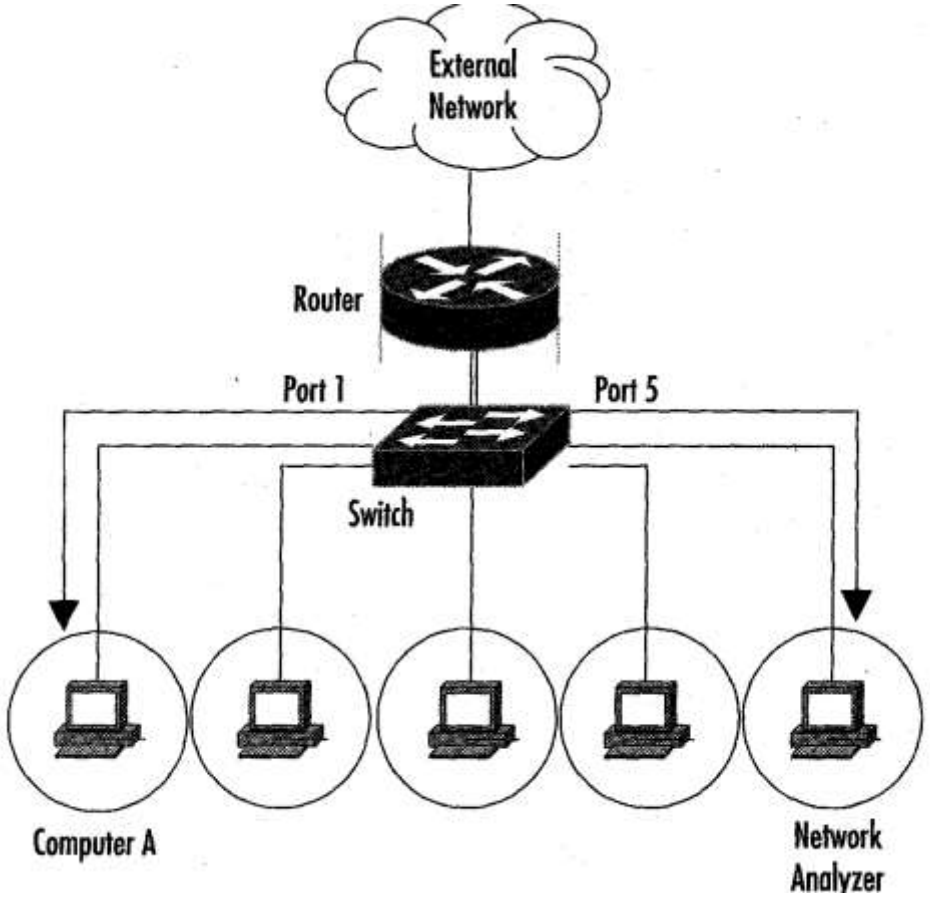
# Who Uses Network Analyzers

- System administrators
  - Understand system problems and performance
- Malicious individuals (intruders)
  - Capture cleartext data
  - Passively collect data on vulnerable protocols
    - FTP, POP3, IMAP, SMATP, rlogin, HTTP, etc.
    - Capture VoIP data
  - Actively break into the network (backdoor techniques)

# Basic Operation

- Ethernet traffic is broadcasted to all nodes on the same segment
- Sniffer can capture all the incoming data when the NIC is in ***promiscuous*** mode:
  - Default setup is ***non-promiscuous*** (only receives the data destined for the NIC)
  - Remember: a hub receives all the data!
- If switches are used the sniffer must perform **port spanning**
  - Also known as port mirroring
  - The traffic to each port is mirrored to the sniffer

# Port Monitoring



# Protecting Against Sniffers

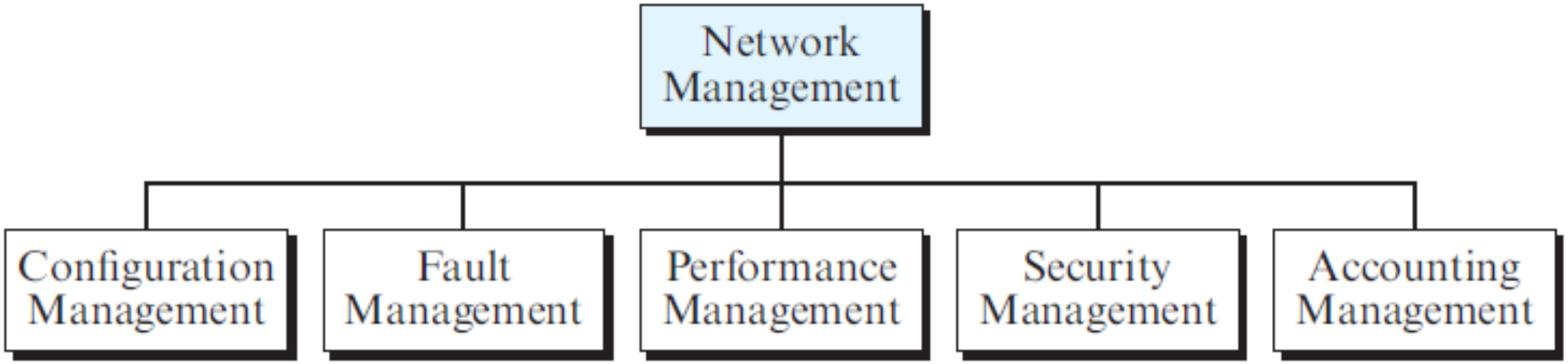
- Using switches can help
- Use encryption
  - Making the intercepted data unreadable
  - Note: in many protocols the packet headers are cleartext!
- VPNn use encryption and authorization for secure communications
  - VPN Methods
    - Secure Shell (SSH)
    - Secure Sockets Layer (SSL)
    - IPsec

# What is Wireshark?

- Formerly called ***Ethereal***
- An open source program
  - free with many features
- Decodes over 750 protocols
- Compatible with many other sniffers
- Supports command-line and GUI interfaces

- Wireshark captures live packet data from a network interface and displays them with detailed protocol information.
- Wireshark, however, is a passive analyzer.
- It only "measures" things from the network without manipulating them; it does not send packets on the network or do other active operations.
- Wireshark is not an intrusion detection tool either. It does not give warning about any network intrusion.
- It, nevertheless, can help network administrators or network security engineers figure out what is going on inside a network and to troubleshoot network problems.
- In addition to being an indispensable tool for network administrators and security engineers, Wireshark is a valuable tool for protocol developers, who may use it to debug protocol implementations,
- and a great educational tool for computer networking students who can use it to see details of protocol operations in real time.

# Configuration Management



- A large network is usually made up of hundreds of entities that are physically or logically connected to each other.
- These entities have an initial configuration when the network is set up, but can change with time.
- Desktop computers may be replaced by others; application software may be updated to a newer version; and users may move from one group to another.
- The configuration management system must know, at any time, the status of each entity and its relation to other entities.
- Configuration management can be divided into two subsystems: reconfiguration and documentation.

# Reconfiguration

- Reconfiguration can be a daily occurrence in a large network. There are three types of reconfiguration: hardware reconfiguration, software reconfiguration, and user-account reconfiguration.
- Hardware reconfiguration covers all changes to the hardware.
- For example, a desktop computer may need to be replaced. A router may need to be moved to another part of the network. A subnetwork may be added or removed from the network.
- All of these need the time and attention of network management.
- In a large network, there must be specialized personnel trained for quick and efficient hardware reconfiguration.
- Unfortunately, this type of reconfiguration cannot be automated and must be manually handled.

- Software reconfiguration covers all changes to the software. For example, new software may need to be installed on servers or clients. An operating system may need updating.
- Fortunately, most software reconfiguration can be automated. For example, an update for an application on some or all clients can be electronically downloaded from the server.
- User-account reconfiguration is not simply adding or deleting users on a system. We must also consider the user privileges, both as an individual and as a member of a group.
- For example, a user may have both read and write permission with regard to some files, but only read permission with regard to other files.
- User-account reconfiguration can be, to some extent, automated.

# Documentation

- The original network configuration and each subsequent change must be recorded meticulously.
- This means that there must be documentation for hardware, software, and user accounts.
- Hardware documentation normally involves two sets of documents: maps and specifications.
- Maps track each piece of hardware and its connection to the network.
- There can be one general map that shows the logical relationships between subnetworks.
- There can also be a second general map that shows the physical location of each subnetwork.
- For each subnetwork, then, there is one or more maps that show all pieces of equipment.

- There must be a set of specifications for each piece of hardware connected to the network.
- These specifications must include information such as hardware type, serial number, vendor (address and phone number), time of purchase, and warranty information.
- All software must also be documented. Software documentation includes information such as the software type, the version, the time installed, and the license agreement.
- Most operating systems have a utility that allows user account documentation.
- The management must make sure that the files with this information are updated and secured.
- Some operating systems record access privileges in two documents; one shows all files and access types for each user; the other shows the list of users that have access to a particular file.