

creation of a simple network configuration.IP addressing.Monitoring of a network.Analysis of traffic.Use of sniffers for the analysis of network packets.

Abdullayeva Nargiza

Network Configuration Procedures

Network software installation takes place along with the installation of the operating system software. At that time, certain IP configuration parameters must be stored in appropriate files so they can be read at boot time.

The procedure is a matter of creating or editing the network configuration files. How configuration information is made available to a machine's kernel depends on whether these files are stored locally (**local files** mode) or acquired from the network configuration server (**network client** mode).

Parameters supplied during network configuration are:

IP address of each network interface on every machine

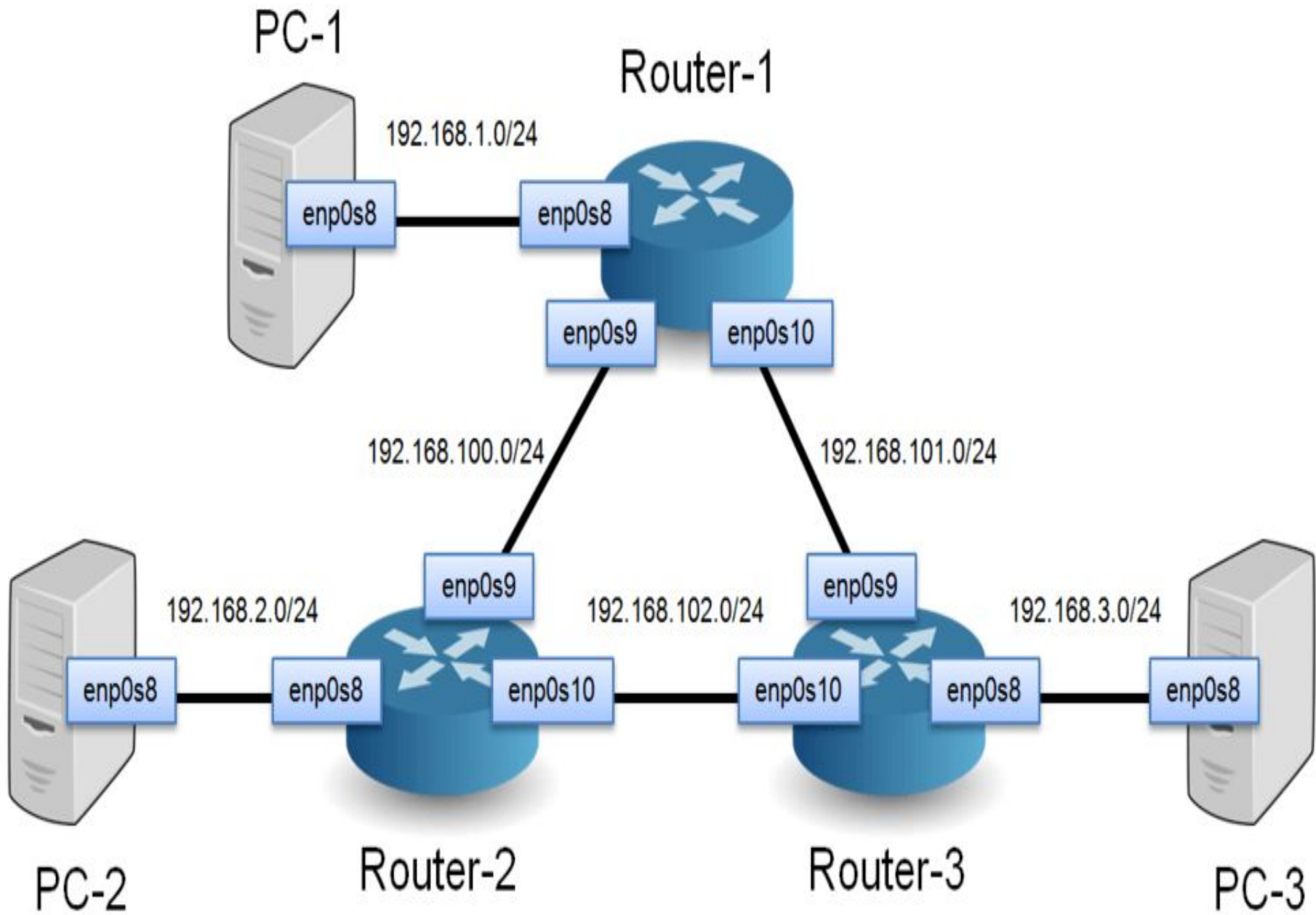
Host names of each machine on the network. You can type the host name in a local file or a name service database.

NIS, NIS+, or DNS domain name in which the machine resides, if applicable





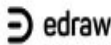


Default router addresses. You supply this only if you have a simple network topology with only one router attached to each network, or your routers don't run routing protocols such as the Router Discovery Server Protocol (RDISC) or the Router Information Protocol (RIP). (See "[Routing Protocols](#)" for more information about these protocols.)

Subnet mask (required only for networks with subnets)

This chapter contains information on creating and editing local configuration files. See the [Solaris Naming Administration Guide](#) for information on working with name service databases.



Best Network Design Tools

		Free Trial?		Top Features		What You Need to Know
SolarWinds Network Topology Mapper		14-Day	Auto-discovery	Multi-layer integration	Multiple export formats	With a range of sophisticated utilities, including automated network discovery, this is an enterprise-grade network design tool.
CADE		Free Tool	Multiple export formats	Locking/unlocking function	Support for multiple diagrams	This free network design tool offers advanced functionality, with predefined blocks and multiple export formats.
Dia		Free Tool	Large library of objects	Cisco-based network elements	Open source	A simple open source program with an impressive library of objects.
Microsoft Visio		None	AutoCAD support	Automatic chart generation	In-app commenting	This popular network design tool supports collaboration and is highly flexible.
EDraw		15-Day	Sharing capabilities	Web version	Multiple export formats	This all-in-one diagramming application has multiple versions, including a web-based version.
Diagram Designer		Free Tool	Advanced pocket calculator	Graph plotter	Compressed file format support	This free tool offers advanced utilities, including a sophisticated pocket calculator and graph plotter.
Network Notepad		Free Version	Multiple versions	Add-ons available	Grouping and locking utilities	This tool comes in multiple versions, with a freeware edition available, with support for a number of useful add-ons.

How to Configure a Host for Local Files Mode

Use this procedure for configuring TCP/IP on a machine that runs in local files mode. Become superuser and change to the `/etc` directory.

Type the host name of the machine in the file `/etc/nodename`.

For example, if the name of the host is `tenere`, type `tenere` in the file.

Create a file named `/etc/hostname.interface` for each network interface.

(The Solaris installation program automatically creates this file for the primary network interface.) Refer to "[/etc/hostname.interface File](#)" for details. If you are using IPv6, see "[IPv6 Network Interface Configuration File](#)".

Type either the interface IP address or the interface name in each `/etc/hostname.interface` file.

For example, create a file named `hostname.ie1`, and type either the IP address of the host's interface or the host's name.

Edit the `/etc/inet/hosts` file to add:

- IP addresses that you have assigned to any additional network interfaces in the local machine, along with the corresponding host name for each interface.
- The Solaris installation program has already created entries for the primary network interface and loopback address.
- IP address or addresses of the file server, if the `/usr` file system is NFS mounted.

- Type the host's fully qualified domain name in the `/etc/defaultdomain` file.
- For example, suppose host `tenere` was part of the domain `deserts.worldwide.com`. Therefore, you would type: `deserts.worldwide.com` in `/etc/defaultdomain`. See ["/etc/defaultdomain File"](#) for more information.
- Type the router's name in `/etc/defaultrouter`.
- See ["/etc/defaultrouter File"](#) for information about this file.
- Type the name of the default router and its IP addresses in `/etc/inet/hosts`.
- Additional routing options are available. Refer to the discussion on routing options in ["How to Configure Hosts for Network Client Mode"](#). You can apply these options to a local files mode configuration.
- If your network is subnetted, type the network number and the netmask in the file `/etc/inet/netmasks`.
- If you have set up a NIS or NIS+ server, you can type netmask information in the appropriate database on the server as long as server and clients are on the same network.
- Reboot each machine on the network.

ip addressing

- An **Internet Protocol address (IP address)** is a numerical label assigned to each device connected to a [computer network](#) that uses the [Internet Protocol](#) for communication.^{[1][2]} An IP address serves two main functions: host or network interface [identification](#) and location [addressing](#).

Introduction

- This document provides basic information needed in order to configure your router for routing IP, such as how addresses are broken down and how subnetting works. You learn how to assign each interface on the router an IP address with a unique subnet. There are examples included in order to help tie everything together.

Prerequisites

Requirements

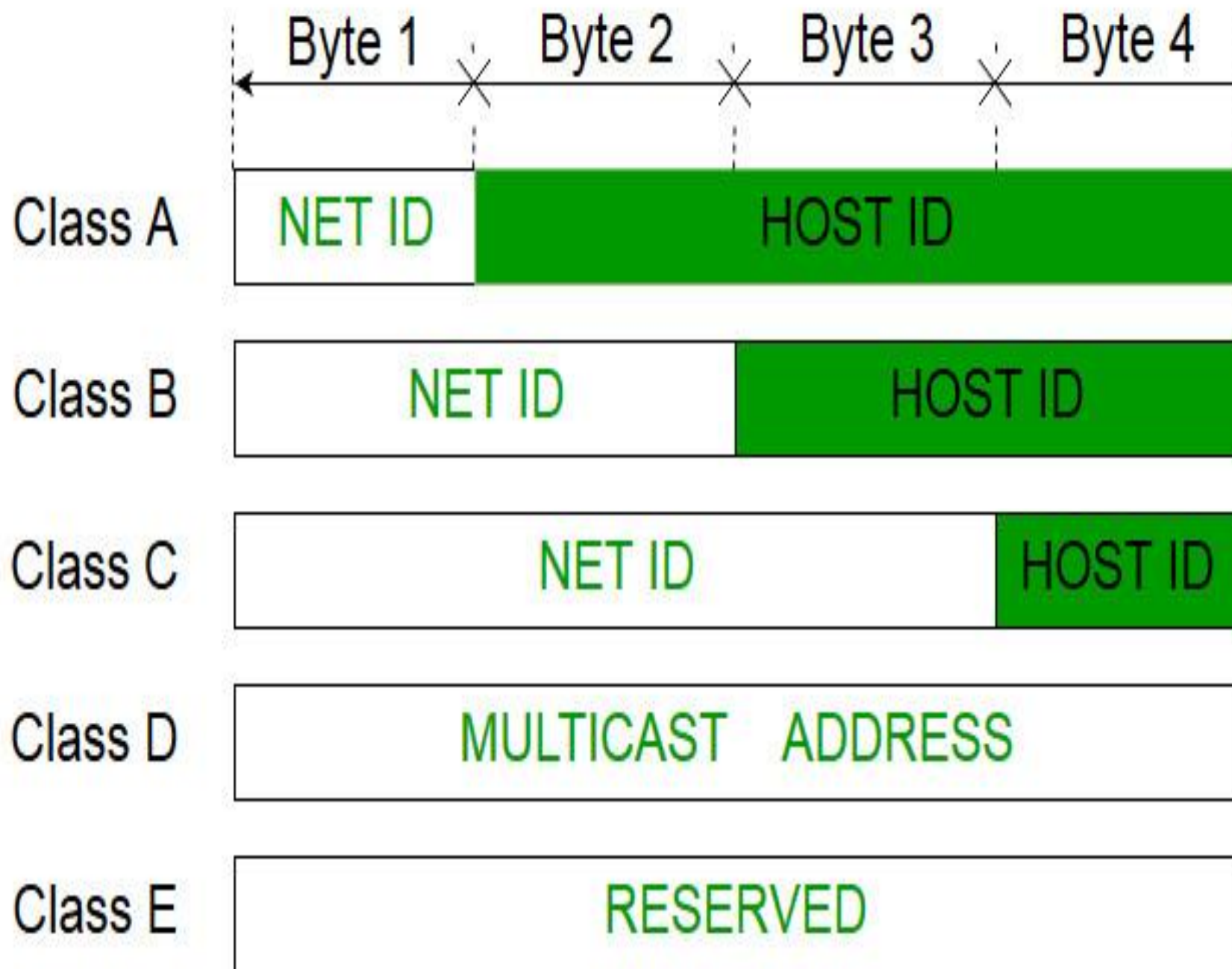
Cisco recommends that you have a basic understanding of binary and decimal numbers.

Components Used

- This document is not restricted to specific software and hardware versions.
- The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

- **Additional Information**

- If definitions are helpful to you, use these vocabulary terms in order to get you started:
- **Address** - The unique number ID assigned to one host or interface in a network.
- **Subnet** - A portion of a network that shares a particular subnet address.
- **Subnet mask** - A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.
- **Interface** - A network connection.
- If you have already received your legitimate address(es) from the Internet Network Information Center (InterNIC), you are ready to begin. If you do not plan to connect to the Internet, Cisco strongly suggests that you use reserved addresses from [RFC 1918](#) .



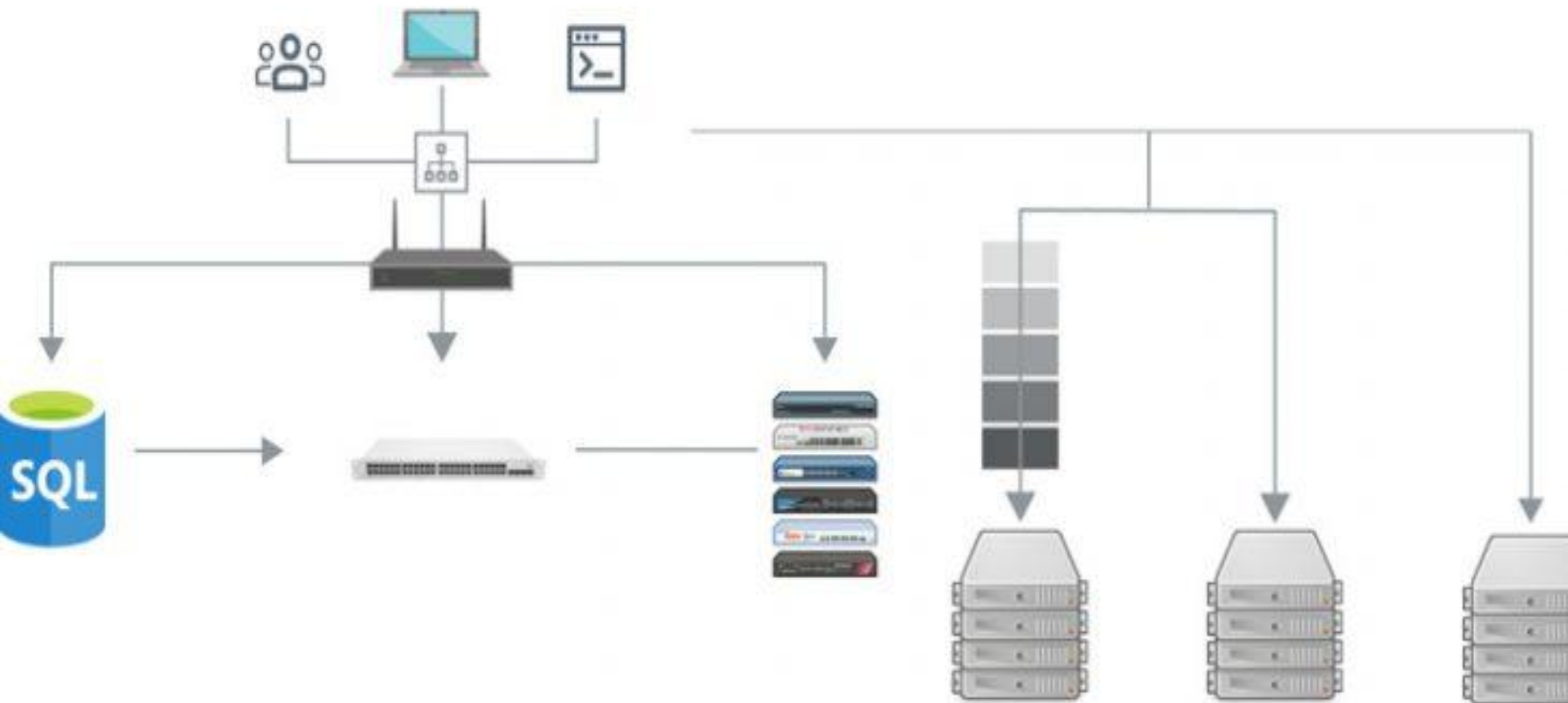
Private addresses

- Early network design, when global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be globally unique. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.
- Computers not connected to the Internet, such as factory machines that communicate only with each other via [TCP/IP](#), need not have globally unique IP addresses. Today, such private networks are widely used and typically connect to the Internet with [network address translation](#) (NAT), when needed.
- Three non-overlapping ranges of IPv4 addresses for private networks are reserved.^[8] These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry. Any user may use any of the reserved blocks. Typically, a network administrator will divide a block into subnets; for example, many [home routers](#) automatically use a default address range of *192.168.0.0* through *192.168.0.255* (*192.168.0.0/24*).

Network monitoring is the use of a system that constantly monitors a [computer network](#) for slow or failing components and that notifies the [network administrator](#) (via [email](#), [SMS](#) or other alarms) in case of outages or other trouble. Network monitoring is part of [network management](#).

- Monitoring the essentials.
- Faulty network devices impact network performance. This can be eliminated through early detection and this is why continuous monitoring of network and related devices is essential. In effective network monitoring, the first step is to identify the devices and the related performance metrics to be monitored. The second step is determining the monitoring interval. Devices like desktops and printers are not critical and do not require frequent monitoring whereas servers, routers and switches perform business critical tasks but at the same time have specific parameters that can be selectively monitored.

Network Monitoring Tools and Software



Monitoring interval.

- Monitoring interval determines the frequency at which the network devices and its related metrics are polled to identify the performance and availability status. Setting up monitoring intervals can help to take the load off the network monitoring system and in turn, your resources. The interval depends on the type of network device or parameter being monitored. Availability status of devices have to be monitored the least interval of time preferably every minute. CPU and memory stats can be monitored once in every 5 minutes. The monitoring interval for other metrics like Disk utilization can be extended and is sufficient if it is polled once every 15 minutes. Monitoring every device at the least interval will only add unnecessary load to the network and is not quite necessary.

Protocol and its types.

- When monitoring a network and its devices, a common good practice is to adopt a secure and non-bandwidth consuming [network management](#) protocol to minimize the impact it has on network performance. Most of the network devices and Linux servers support SNMP(Simple Network Management Protocol) and CLI protocols and Windows devices support WMI protocol. SNMP is one of the widely accepted [network protocols](#) to manage and monitor network elements. Most of the network elements come bundled with a [SNMP agent](#). They just need to be enabled and configured to communicate with the network management system (NMS). Allowing SNMP read-write access gives one complete control over the device. Using SNMP, one can replace the entire configuration of the device. A network monitoring system helps the administrator take charge of the network by setting SNMP read/write privileges and restricting control for other users.

Traffic analysis

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in [communication](#), which can be performed even when the messages are [encrypted](#).^[1] In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of [military intelligence](#), [counter-intelligence](#), or [pattern-of-life analysis](#), and is a concern in [computer security](#).

Traffic analysis tasks may be supported by dedicated computer software programs. Advanced traffic analysis techniques may include various forms of [social network analysis](#)

The most effective, advanced network traffic analysis solutions include the following key features:

- **Broad Visibility:** Whether the network communications in question are traditional TCP/IP style packets, virtual network traffic crossing from a vSwitch, traffic from and within cloud workloads, API calls to SaaS applications, or serverless computing instances, NTA tools have the ability to monitor and analyze a broad variety of communications in real-time.
- **Encrypted Traffic Analysis:** With [over 70 percent of web traffic encrypted](#), organizations need an accessible method for decrypting their network traffic without disrupting data privacy implications. NTA solutions deliver on this challenge by enabling security professionals to uncover network threats by analyzing the full payload without actually peeking into
- **Entity Tracking:** NTA products offer the ability to track and profile all entities on a network, including the devices, users, applications, destinations, and more. Machine learning and analytics then attribute the behaviors and relationships to the named entities, providing infinitely more value to organizations than a static list of IP addresses.

- **Comprehensive Baseline:** To keep up with ever-changing modern IT environments, NTA solutions track behaviors that are unique to an entity or a small number of entities in comparison to the bulk of entities in an environment. The underlying data is available immediately and NTA machine learning baselines evolve in real-time as behaviors change. Also, with entity tracking capabilities, NTA baselines are even more comprehensive as they can understand the source and destination entities, in addition to traffic patterns. For instance, what might be normal for a workstation is not normal for a server or IP phone or camera.
- **Detection and Response:** Because NTA tools attribute behaviors to entities, ample context is available for detection and response workflows. This means security professionals no longer need to sift through multiple data sources such as DHCP and DNS logs, configuration management databases and directory service infrastructure in an attempt to gain comprehensive visibility. Instead, they can quickly detect anomalies, decisively track them down, determine the root cause and react accordingly.

use of sniffers for the analysis of network packets

Network Management

Network Monitoring

- **■ Packet sniffer** This tool allows you to collect all the data that is being transmitted to and from the endpoints on the network. The advantage of collecting individual packets is that you will have an insight and detailed inspection of how certain traffic is being transmitted.
- **■ Event logs** Logs are records of events that have occurred and actions that were taken. Many systems will provide logs that will give automated information on events that have occurred, including accounts that were used to log on, activities performed by users and by the system, and problems that transpired. On many systems, the logs may be simple text files that are saved to a location on the local hard drive or a network server. In other cases, the system will provide a specific tool for viewing the information.

Password lists Password lists should contain all the passwords used to perform administrative or maintenance tasks on the network. This includes passwords for

- Administrative and administrator account for servers and workstations.
- Setup and [configuration utilities](#) on computers and other devices.
- Administrative features in software.
- Files, such as those containing other passwords or documentation containing procedures.
- **Notification documentation** Notification documentation includes contact information for specific people in an organization, their roles, and when they should be called. The contact information included in notification documentation should provide several methods of contacting the appropriate person. [Notification procedures](#) should also include contact information for certain outside parties who are contracted to support specific systems.

Benefits of Packet Sniffing

