Network Scanning Software

by Sophia

WHAT'S COVERED

In this lesson, you will learn about software tools for network scanning.

Specifically, this lesson will cover the following:

1. Network Scanning

Network configuration is only the first step of network management. Networks aren't just "set it and forget it" entities! They require constant monitoring—and frequent configuration adjustments—to keep them running well and protect them from security threats.

Network monitoring involves both software and hardware tools. Here we begin our look at software tools that a network technician needs to be familiar with. Upcoming tutorials will address other software tools, as well as hardware tools.

1a. Setting Performance Baselines

Before you start monitoring a network, you must set baselines for it. A **baseline** is a standard level of performance of a certain device or the normal operating capacity for an entire network. For instance, a specific server's baseline describes norms for factors like how busy its processors are, how much of the memory it uses, and how much data usually goes through the network interface card (NIC) at a given time. Baselining is

important because you and your client need to know what “normal” looks like in order to detect problems before they develop into disasters.

A network baseline delimits the amount of bandwidth available and when. For networks and networked devices, baselines include information about the following four key components.

- Processor
- Memory
- Hard-disk (or other storage) subsystem
- Wired/wireless utilization

HINT

After everything is up and running, it’s a good idea to establish performance baselines on all vital devices and your network in general. To do this, measure things like network usage at three different strategic times to get an accurate assessment. For instance, peak usage usually happens around 8:00 a.m., Monday through Friday, or whenever time most people log in to the network at in the morning. After hours or on weekends is often when usage is the lowest. Knowing these values can help you troubleshoot bottlenecks or determine why certain system resources are more limited than they should be. Knowing what your baseline is can even tell you if someone’s complaints about the network running like a slug are really valid. You can use the network-monitoring software tools covered in this tutorial to establish baselines. Some server operating systems also come with their own software to help with network monitoring, which can help find baselines, perform log management, and even do network graphing as well so you can compare the logs and graphs at a later period of time on your network. It’s wise to re-baseline network performance at least once a year. And always pinpoint new performance baselines after any major upgrade to your network’s infrastructure.

BIG IDEA

Information from network scans is useful primarily when compared to baseline data collected when the network is running well.

TERM TO KNOW

Baseline

A standard level of performance against which future performance can be compared.

2. Network Scanners

Network scanner refers to a family of tools used to analyze our networks. This tutorial looks at the following five types of scanners.

- Packet sniffers
- Intrusion detection system/intrusion prevention system (IDS/IPS) software
- Port scanners

- Wi-Fi analyzers
- Bandwidth speed testers

TERM TO KNOW

Network Scanner

A family of tools used to analyze networks.

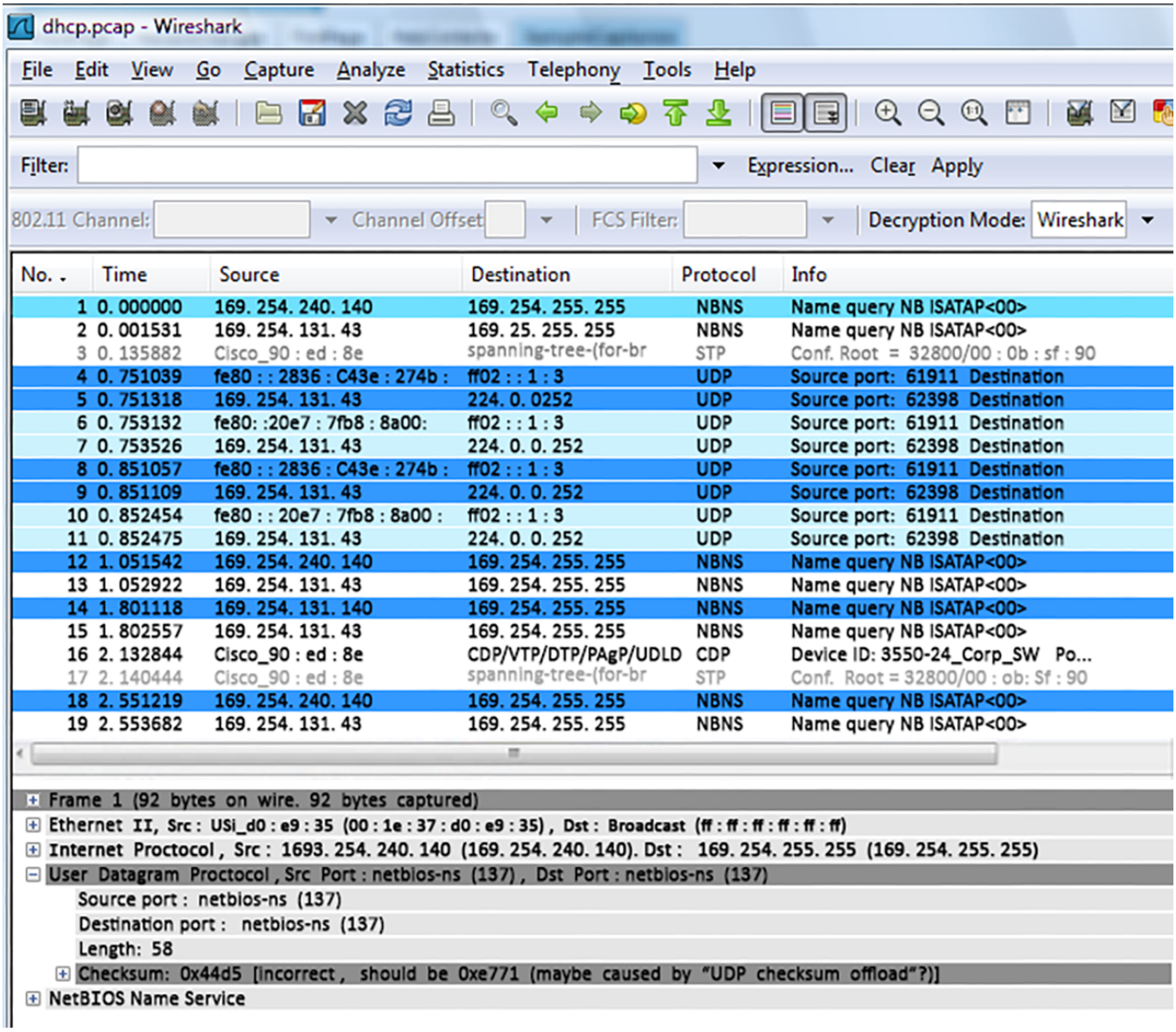
2a. Packet Sniffers

Unlike port scanners, **packet sniffers** (also called network monitors) actually look inside every packet on a network segment. The basic purpose of packet sniffers (or network analyzers) is to collect and analyze each individual packet that is captured on a specific network segment to determine if problems like bottlenecks, retransmissions, and security breaches are happening. Packet sniffers are a must-have for every network administrator to troubleshoot and find problems or security holes in a network. For example, you may discover that users are using an application on the network with usernames and passwords being sent unencrypted over the network.

You can also use packet sniffers to see if there is too much traffic on a segment, to see router or switch interfaces (referred to as interface monitoring), or even to see if a broadcast storm has been created by a bad NIC. These network analyzers can also show you top talkers and listeners on your network and provide packet flow monitoring. However, you can't use them to catch packets passing through routers.

DID YOU KNOW

One very useful free tool is Wireshark, which you can download from www.wireshark.org. It runs on Windows, macOS, Linux, and Unix platforms. It captures data on all interfaces easily, including wireless and virtual private network (VPN) connections, and looks at all traffic on the network segment. Notice in the following screenshot that Wireshark can identify both the IP addresses and the MAC addresses associated with any of the packets captured as well as the protocol in use.



Packet sniffers enable you to examine network traffic down to the details of individual packets. You can put the packet's header under the microscope; It contains vital information about the protocol being used to encapsulate it, plus the source and destination IP addresses. This is very valuable information. If you're seeing the speed of traffic on a specific segment grind to a crawl, one of the first things to look for is one IP address that's spewing tons of data. If that's the case, it could mean that you've got a failing network adapter, because a common symptom of a dying NIC is to become extremely "chatty" by sending out broadcast packets and clogging things to the point that legitimate traffic can't get through. It's like getting a deluge of junk mail and being forced to read every last bit of it; a broadcast packet is technically addressed to everyone, meaning that all the other NICs on the segment have to stop and read what's in it—not so good.

TERM TO KNOW

Packet Sniffer

A network scanner that looks inside every packet on a network segment to look for evidence of bottlenecks, retransmissions, and security breaches.

2b. Intrusion Detection and Prevention Systems

More expensive network sniffers can help find anomalies in your network, like a hack, and even alert you to these problems. However, for that level of monitoring, you'd be better off using a tool known as an IDS/IPS.

An **intrusion detection system (IDS)** detects unwanted attempts to manipulate network systems and/or environments. An IDS identifies, detects, and reports attempts of unauthorized access to the network as well as any suspicious activity, and it's the best software type for identifying an attack.

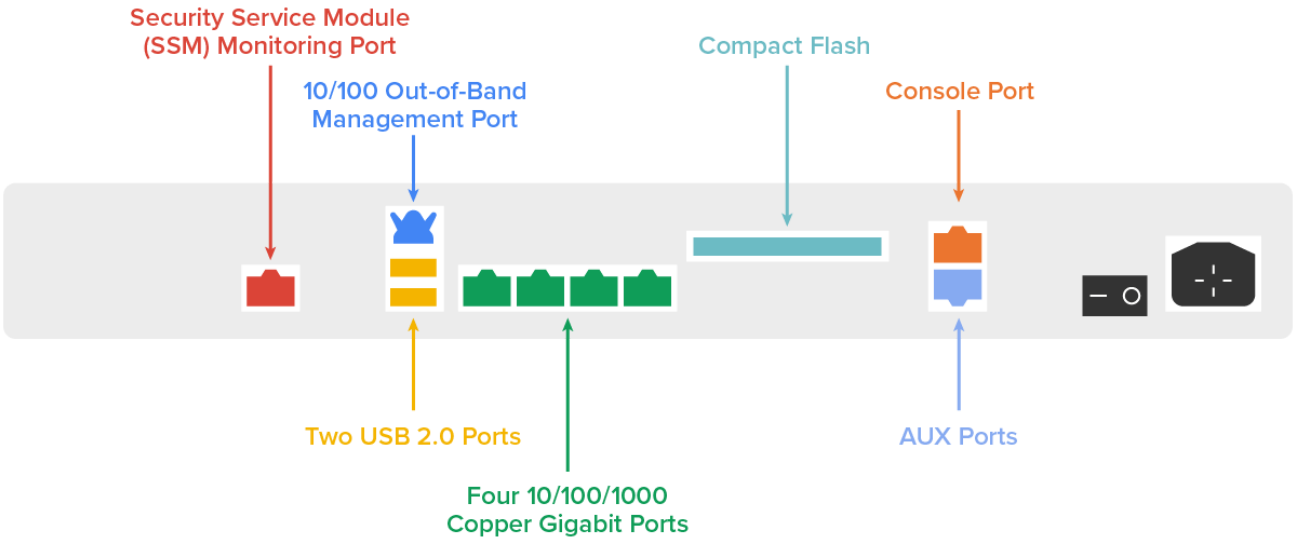
However, if you want to stop the attack in its tracks, you need to add an IPS device. An **intrusion prevention system (IPS)** is a system that monitors network and/or system activities for any strange or malicious behavior. It can react in real time to prevent and even block nasty activities. Unlike IDSs, which can identify an attack and report it, an IPS can stop the attack by shutting down ports or dropping certain types of packets.

Many IDS/IPS software packages are available, and some are free. Again, predictably, the best ones aren't free, and they can be a bit pricey. Most of these high-powered versions run on Linux or other proprietary hardware, but there are many IDS/IPS software applications available for Windows too.

DID YOU KNOW

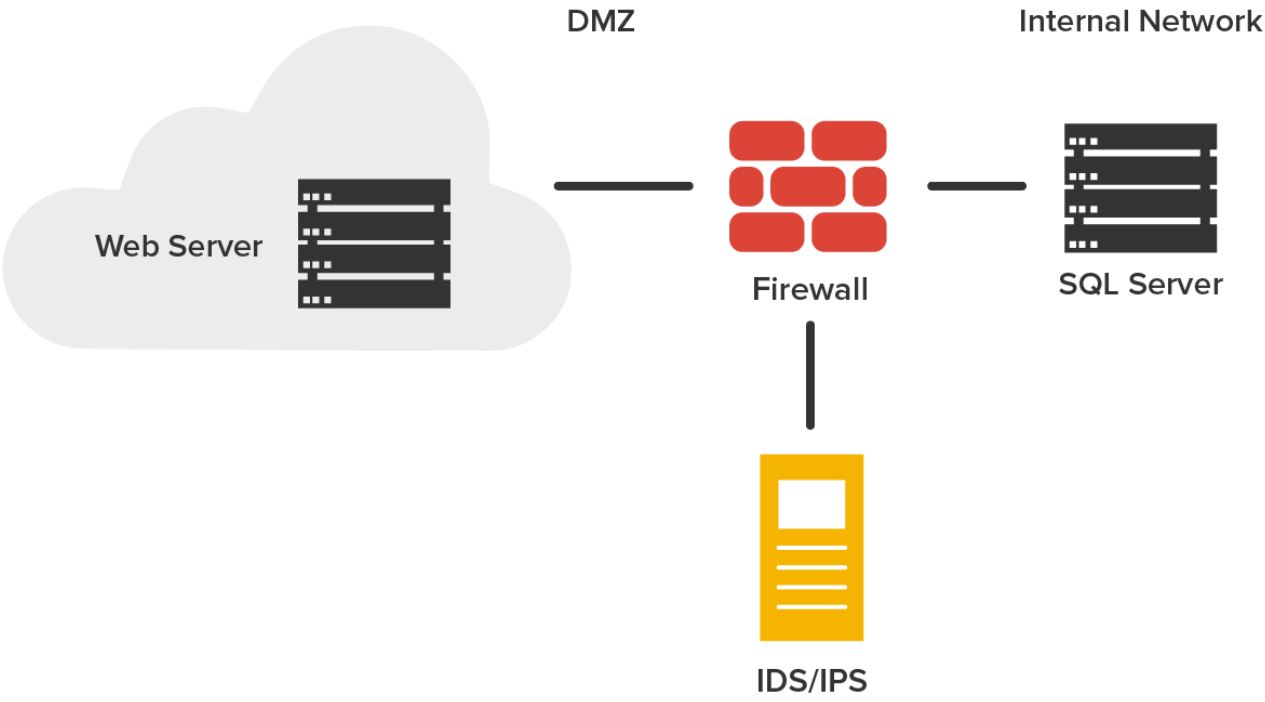
Snort is one of the most popular IDS/IPS software products around. It runs on both Linux and Windows. It's a free, open-source platform, which happens to be a big reason for its popularity. It also has some pretty cool features.

On the other hand, if you're dealing with a large corporate environment, you need some serious weaponry, and Cisco offers Adaptive Security Appliance (ASA) (shown below). It is a powerful enterprise solution that is far from free but worth it.



The following diagram shows where a typical IDS/IPS would typically be placed. You would typically find the IDS/IPS positioned between your internal router and the firewall to the outside network (internet). If using Snort, you would add the software to a Linux box and connect this box between the firewall and the router. This area

would typically be your demilitarized zone (DMZ). The Basic Analysis and Security Engine (BASE) displays and reports intrusions and attacks logged in the Snort database in a web browser for convenient analysis.



TERMS TO KNOW

Intrusion Detection System (IDS)

A network scanner that detects unwanted attempts to manipulate network systems and/or environments.

Intrusion Prevention System (IPS)

A system that monitors network and/or system activities for any strange or malicious behavior and stops the attack by shutting down ports or dropping certain types of packets.

2c. Port Scanners

A **port scanner** is a software tool designed to search a host for open ports. Network admins use port scanners to ensure the network's security, but bad guys also use them—to find a network's vulnerabilities and compromise them. To "port scan" means to scan for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) open ports on a single target host, either to legitimately connect to and use its services for business and/or personal reasons or to find and connect to those ports and subsequently attack the host and steal or manipulate it for nefarious reasons.

In contrast, **port sweeping** means scanning multiple hosts on a network for a specific listening TCP or UDP port, such as SQL (SQL injection attacks are super common today.) This is a favorite approach hackers use when trying to invade your network. They port sweep in a broad manner, and then, if they find something—in this case, SQL—they can port scan the particular host they've discovered with the desired service available to exploit and get what they're after. This is why it's a really good idea to turn off any unused services on your

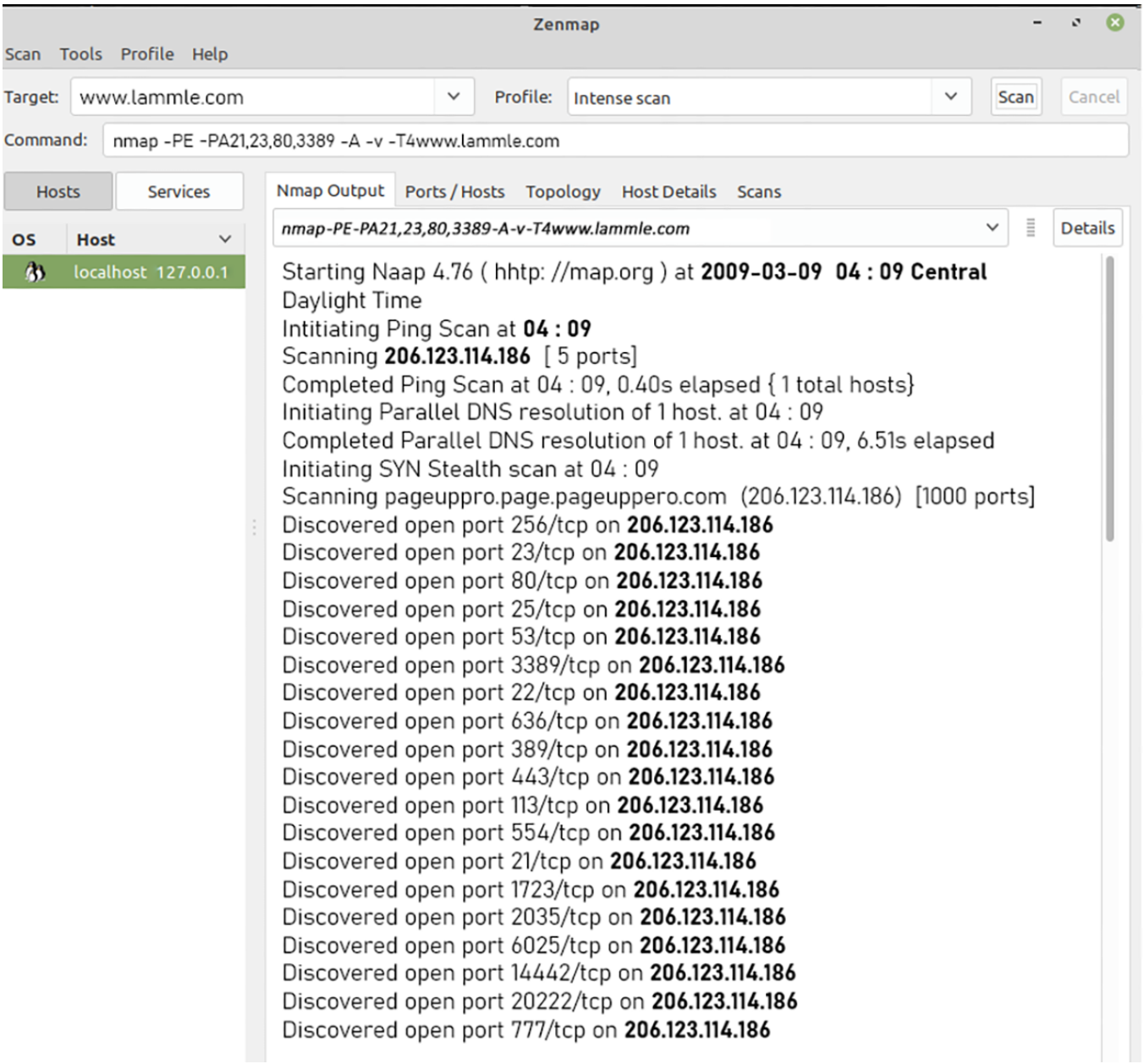
servers and routers and run only the minimum number of services required on every host machine in your network. Do yourself a big favor and make sure this is in your security policy.

A synchronized scan, or a**SYN scan**, is the most popular form of TCP scanning. Rather than use the operating system's network functions, the port scanner actually generates raw IP packets itself and monitors for responses. This scan type is also known as half-open scanning because it never really opens a full TCP connection. The port scanner generates a SYN packet, and if the targeted port is open, it will respond with a SYN-ACK (acknowledge) packet. The scanner host responds with an RST (reset) packet, closing the connection before the handshake is completed.

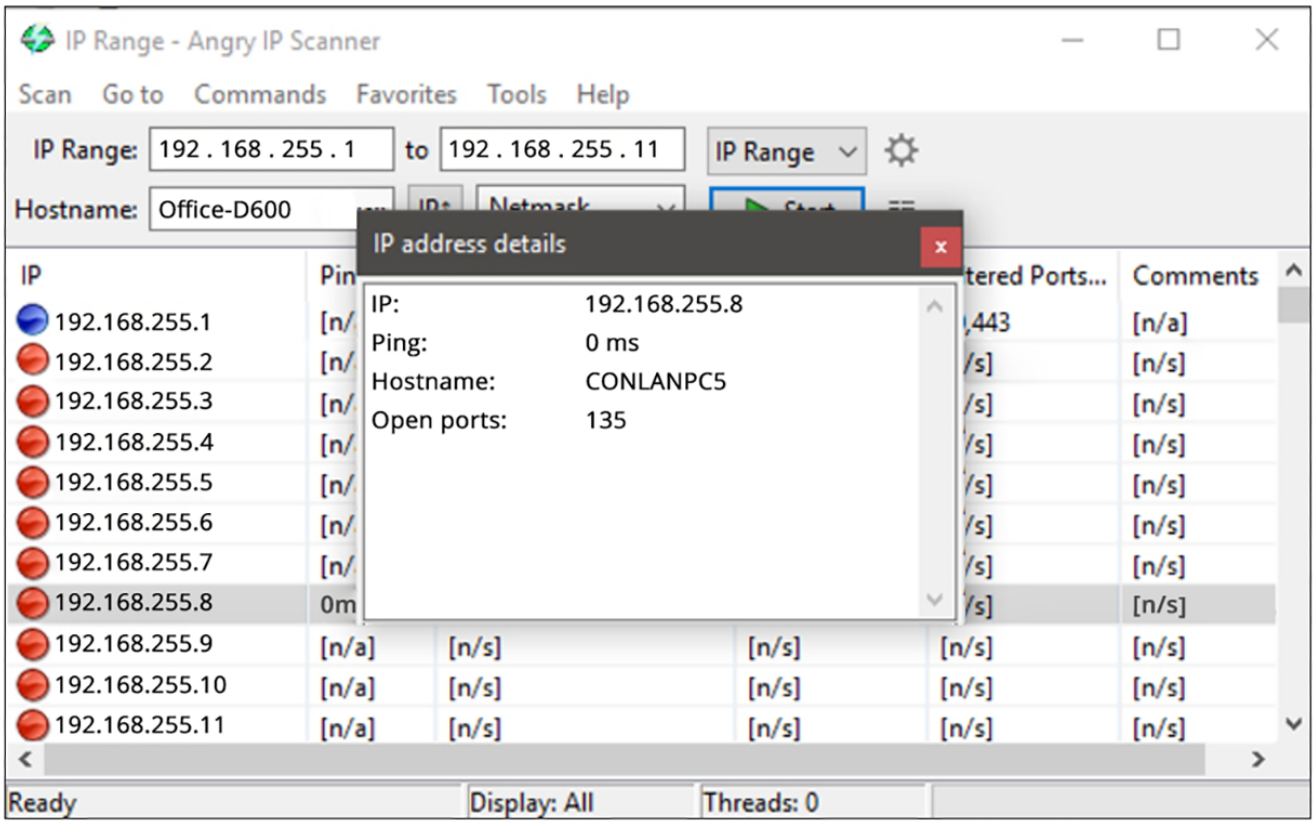
DID YOU KNOW

A free, open-source program named Network Mapper (Nmap) can be used as a port scanner, but it also does a lot more. You may want to download (nmap.org) and play with this cool program. Nmap runs on all platforms and can scan ports, check all the open services running on each host, find firewalls, and even help tremendously with network management. Nmap also comes with a complete set of instructions and equips you with documentation to help you troubleshoot and map your network.

The following screenshot shows Nmap running in Windows, performing a DNS resolution, and then a port scan to the host being monitored. Zenmap is the name of the GUI interface it uses.



Even though Nmap is pretty simple, there are even simpler tools out there—a whole lot of them. Angry IP (angryip.org), for example, provides both IP-scanning and port-scanning abilities. It is not as complex as Nmap, but it is extremely easy to use.



TERMS TO KNOW

Port Scanner

A software tool designed to search a host for open ports.

Port Sweeping

Scanning multiple hosts on a network for a specific TCP or UDP port that is listening, such as SQL.

SYN Scan

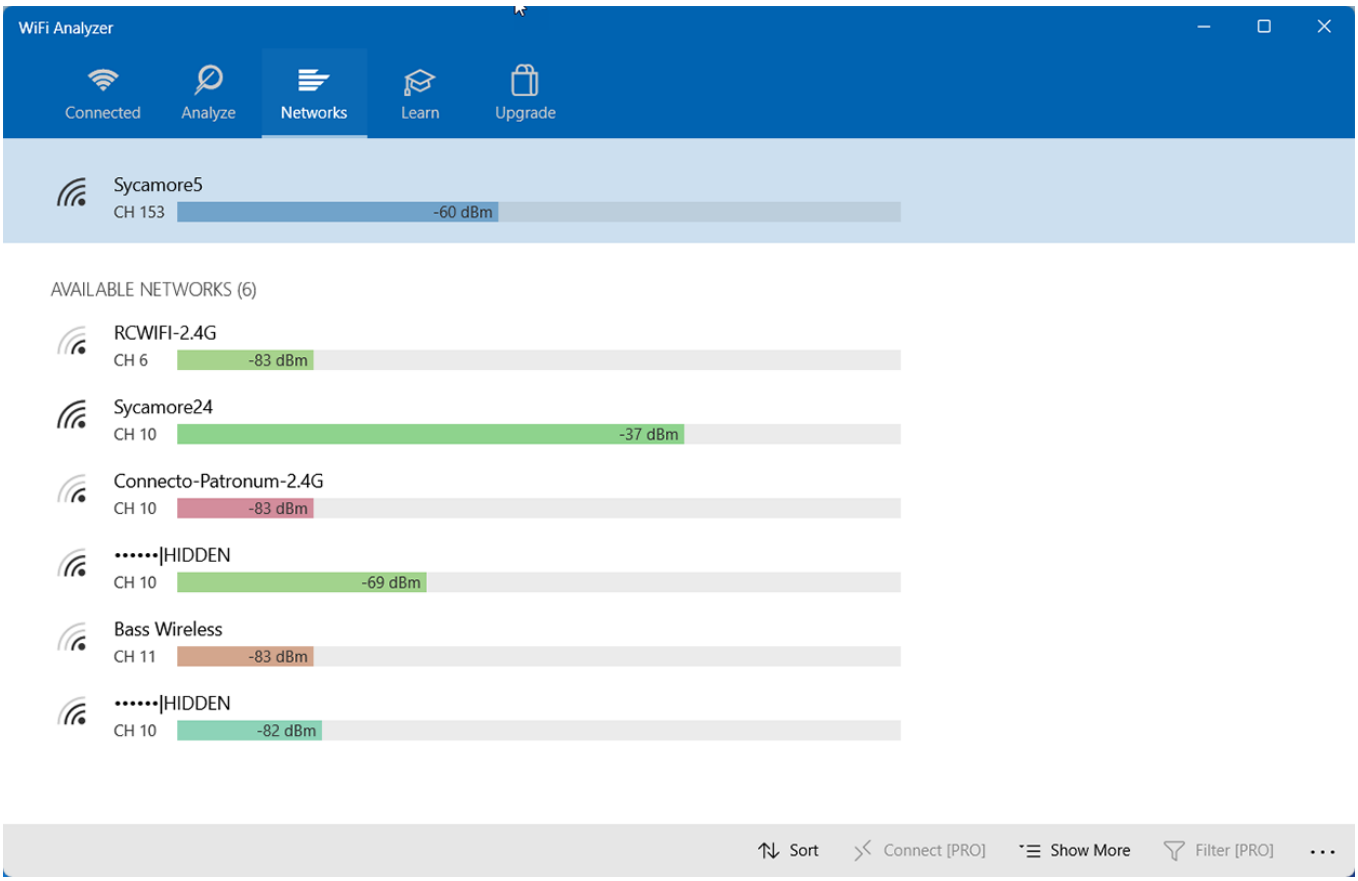
A popular form of TCP scanning that generates raw IP packets and monitors for responses.

2d. Wi-Fi Analyzers

A **Wi-Fi analyzer**, or wireless analyzer, is similar to the network analyzers already discussed but is used for sniffing wireless networks. Wi-Fi analyzers can find the channels in use, the number of clients, the amount of bandwidth used, top talkers, and more. On wireless LANs, one can capture traffic on a particular channel or on several channels when using multiple adapters.

Wi-Fi analyzers identify networks by passively collecting packets and detecting standard named networks, detecting (given time) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

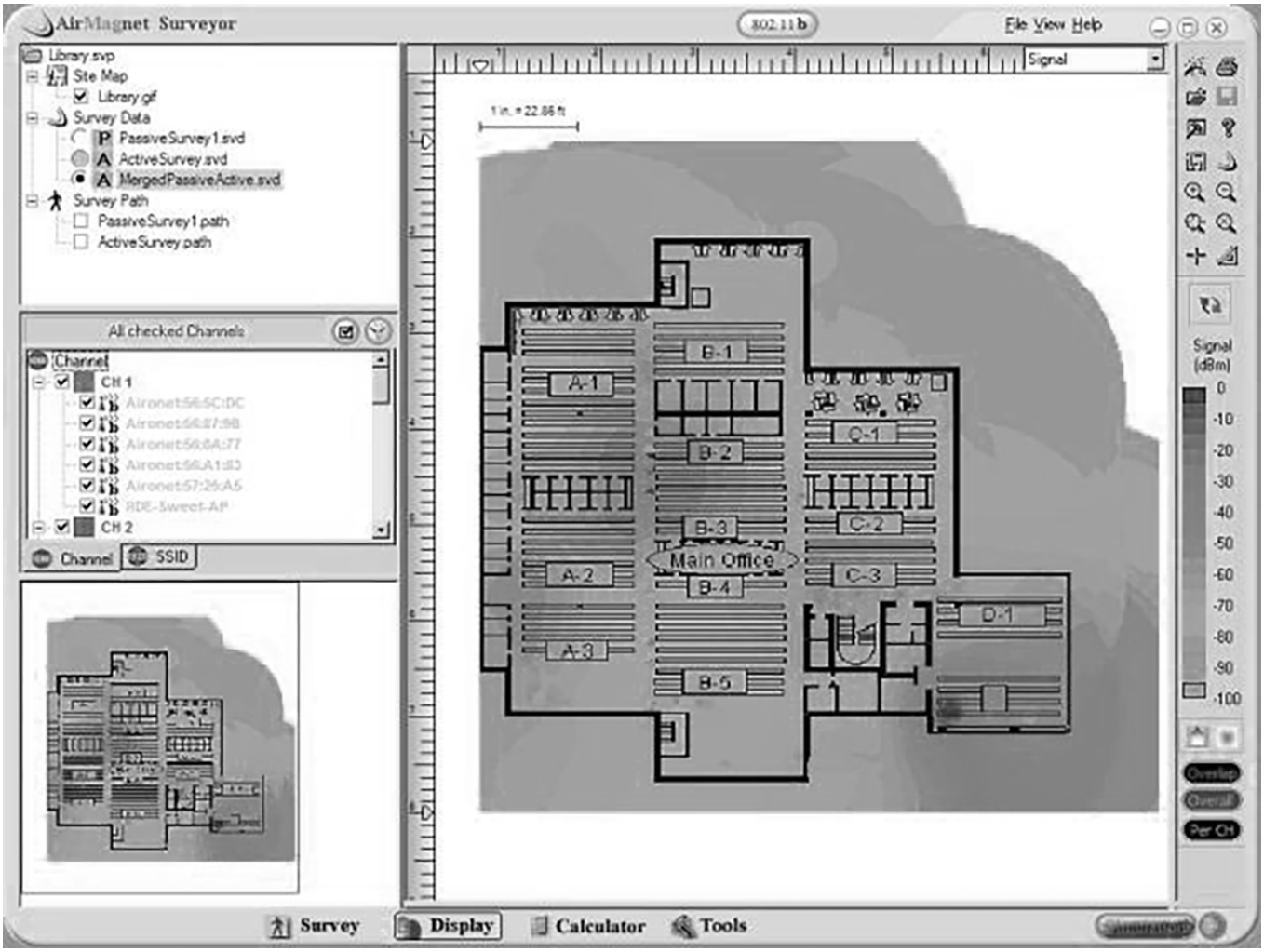
The following screenshot shows the output of a wireless analyzer.



In addition to using a wireless analyzer, to create a good wireless network, you need to do a wireless survey of the floor or building where you are installing your network. To do this, you need a **wireless survey tool**. Wireless survey tools help you design and deploy the most accurate indoor and outdoor wireless LAN networks (802.11n/a/b/g/ac) correctly the first time and prevent costly rework and IT complaints.

You can collect real-world data by performing unique true end-user experience measurements (wireless LAN throughput, data rates, retries, losses). You can also minimize the (expensive) impact of radio frequency (RF) interference sources on wireless 802.11n/a/b/g/ac LAN performance by performing simultaneous wireless spectrum analysis in a single walk-through.

In addition, you can certify the wireless network for any design/application requirements using customer-ready pass/fail assessment reports. The following screenshot shows the output of a wireless survey tool.



TERMS TO KNOW

Wi-Fi Analyzer

A network analyzer that is used for sniffing wireless networks.

Wireless Survey Tool

Software that helps design and deploy wireless LAN networks accurately.

2e. Bandwidth Speed Testers

A **bandwidth speed tester** is exactly what it sounds like. It is software that tests the speed of data transfer in the network. While there are many internet-based tools for testing the internet connection to test the performance of the LAN, you will need a tool that operates within the network.

LAN Speed Test from Totusoft is one example. It is designed to measure file transfer and network speeds (wired and wireless). It does this by building a file in memory and then transferring it both ways (removing the effects of Windows file caching) while keeping track of the time. It then does the calculations for you.

TERM TO KNOW

Bandwidth Speed Tester

Software that tests the data transfer speed in a network.

SUMMARY

In this lesson, you learned about software tools you can use for **network scanning**. These tools included **packet sniffers**, **intrusion detection and prevention systems**, **port scanners**, **Wi-Fi analyzers**, and **bandwidth speed testers**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Bandwidth Speed Tester
Software that tests the data transfer speed in a network.

Baseline
A standard level of performance against which future performance can be compared.

Intrusion Detection System (IDS)
A network scanner that detects unwanted attempts to manipulate network systems and/or environments.

Intrusion Prevention System (IPS)
A system that monitors network and/or system activities for any strange or malicious behavior and stops the attack by shutting down ports or dropping certain types of packets.

Network Scanner
A family of tools used to analyze networks.

Packet Sniffer
A network scanner that looks inside every packet on a network segment to look for evidence of bottlenecks, retransmissions, and security breaches.

Port Scanner
A software tool designed to search a host for open ports.

Port Sweeping
Scanning multiple hosts on a network for a specific TCP or UDP port that is listening, such as SQL.

SYN Scan
A popular form of TCP scanning that generates raw IP packets and monitors for responses.

Wi-Fi Analyzer
A network analyzer that is used for sniffing wireless networks.

Wireless Survey Tool

Software that helps design and deploy wireless LAN networks accurately.