Inventorying – IP-Scan

Inventory of IP Systems

TITLE	Inventorying – IP-Scan
AUTHOR	Docusnap Consulting
DATE	10/07/2019
VERSION	1.0 | valid from October 7, 2019

TABLE OF CONTENTS

1. Introduction 4

1.1 Docusnap IP Scan 4

1.2 Installing the NPCAP Driver 4

1.2.1 Risks and Difficulties 4

1.2.2 Installing NPCAP afterwards 5

2. IP Scan in Docusnap 6

2.1 IP Scan Wizard 6

2.2 Analysis and Result 9

2.3 MAC Filters for IP Systems 10

3. Optional: IP Scan Analysis Tool 11

3.1 Purpose of Use 11

3.2 Application of the Test Program 12

3.2.1 Scan 12

3.2.2 Analyze 13

3.2.3 Help 13

3.3 Transfer to Docusnap 14

3.3.1 Analysing results 14

3.3.2 Adaptation of the Docusnap IP Scan Configuration 15

4. Application Cases and Practical Examples 16

4.1 Initial Inventory 16

4.2 Increase data quality 16

4.3 Detect Security Vulnerabilities 17

1. Introduction

The IP-Scan in Docusnap gives you the possibility to search your network or that of a customer extensively for active systems. All you need for this initial overview, or to check for a complete inventory, are the relevant IP address ranges. No login information or community strings are used for the IP Scan. This way you can quickly and easily inventory a new network and get an overview.

In your own network, you can use this method to capture active components that you have not yet captured with a more detailed scan. Reasons for this could be, for example, that the system is not known or the necessary logon information is missing.

This HowTo describes the use of the IP Scan and is divided into the following chapters:

- Chapter 1 explains the necessity and installation of the NPCAP driver.
- Chapter 2 describes the actual IP Scan.
- Chapter 3 shows how to test NMAP parameters and then transfer them to Docusnap.
- In Chapter 4, use cases and practical examples are listed

1.1 Docusnap IP Scan

Docusnap distinguishes between a normal and an extended IP Scan. Both IP Scans are based on NMAP (Network Mapper). The normal IP Scan uses functions like SYN-ACK, ARP-Request, ICMP requests and name resolution. Responding systems are captured with rudimentary network information.

By using special NMAP parameters, the extended IP Scan is able to detect additional information such as the operating system.

Prerequisite for the extended IP Scan is the installation of the NPCAP driver on the inventorying system.

1.2 Installing the NPCAP Driver

Important: The installation of the NPCAP driver is not a prerequisite for the successful completion of the Docusnap installation. However, an extended IP Scan is only possible with an installed NPCAP driver.

When reinstalling Docusnap, you will be offered to install the NPCAP driver during the setup routine. This is optional and can be activated by you.

An IP Scan can be performed by the server, client or Docusnap Discovery Service. Accordingly, the setup for the Docusnap Discovery Service also includes the option to install the NPCAP driver.

If you execute your Docusnap update via the update function within the program, no NPCAP installation is offered.

1.2.1 Risks and Difficulties

Prerequisite for the installation of an additional network adapter and the NPCAP driver are local administrator rights.

When installing the NPCAP driver, please note that an additional network adapter must be added. The intervention in the system can therefore be massive. Especially with systems such as a domain controller or similar, an installation should not be carried out lightly.

It should also be noted that an installation of the NPCAP driver may compete with similar network drivers. This may also affect other versions of the NPCAP driver. For a Wireshark installation a NPCAP driver will be installed as well. Since Wireshark has different installation options, both Wireshark and Docusnap may produce incorrect results.

You can find further information on the requirements and problems with e.g. firewalls and monitoring in our White Paper Docusnap Inventory in the IP Scan chapter.

1.2.2 Installing NPCAP afterwards

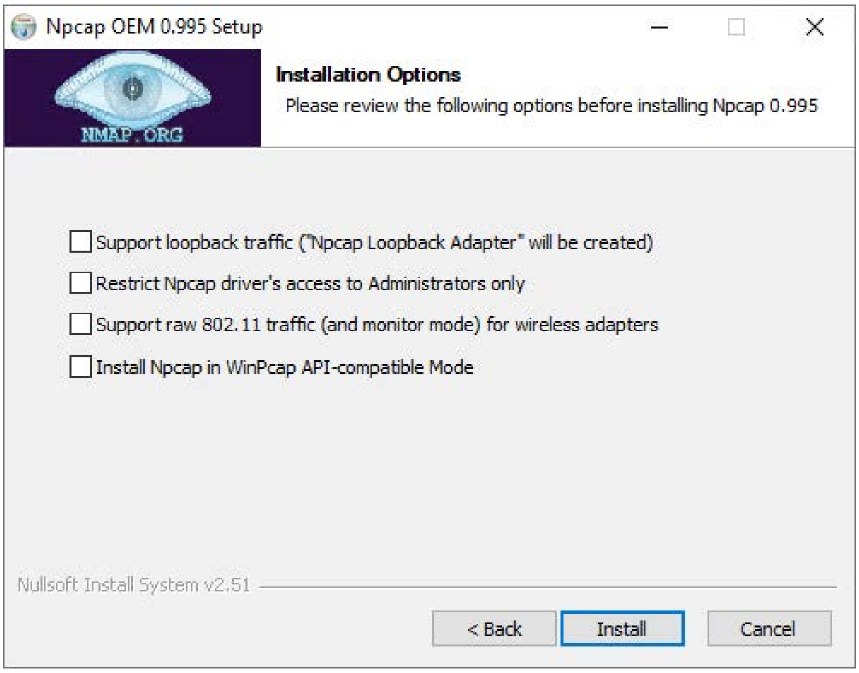
A subsequent installation of the NPCAP driver is possible. You can use the npcap-oem.exe in the Docusnap X installation folder for this. Alternatively, you can also obtain the setup from the manufacturer.

The default path of this file is:

\Program Files\Docusnap X\MSI\npcap-oem.exe

Please make sure that the corresponding options are set correctly during the subsequent installation.

With remote connections it can happen that the connection is interrupted briefly.



Npcap OEM 0.995 Setup

Installation Options

Please review the following options before installing Npcap 0.995

□ Support loopback traffic ("Npcap Loopback Adapter" will be created)
□ Restrict Npcap driver's access to Administrators only
□ Support raw 802.11 traffic (and monitor mode) for wireless adapters
□ Install Npcap in WinPcap API-compatible Mode

Fig. 1 - NPCAP Setup

2. IP Scan in Docusnap

2.1 IP Scan Wizard

The IP-Scan is a standalone inventory wizard in Docusnap. A distinction is made between the Simple IP Scan and the Advanced IP Scan. The selection can be made in the course of the wizard using a checkbox.

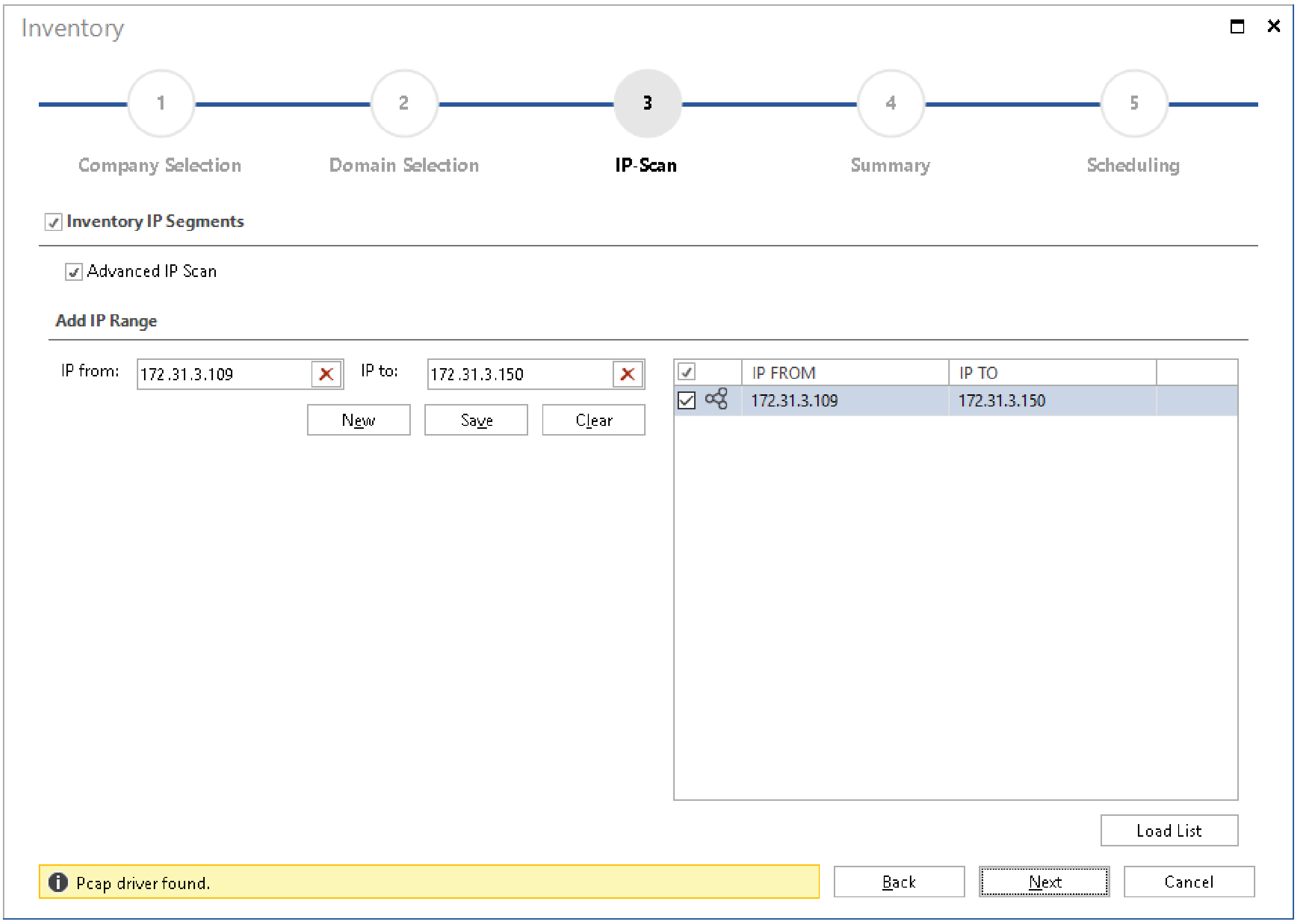
IP Scan

The IP Scan checks the addresses using ICMP requests. If the requested system responds, it is recorded as an IP system and stored in the database with additional information (scan date, IP address and subnet mask). In addition, the IP Scan attempts to resolve the associated DNS name. If this is successful, the system is registered with the DNS name.

Advanced IP Scan

With the help of the extended mode, MAC vendor, information on the operating system, operating time and the last system start are also recorded. The accuracy of the information collected is expressed as a percentage. This is because NMAP cannot always determine the operating system etc. one hundred percent. NMAP estimates this information on the basis of the response to requests sent.

If the Extended IP Scan is activated, Docusnap searches for the required NPCAP driver. If this is not available, the extended IP Scan cannot be used.



☑ Inventory IP Segments

☑ Advanced IP Scan

Add IP Range

IP from: 172.31.3.109

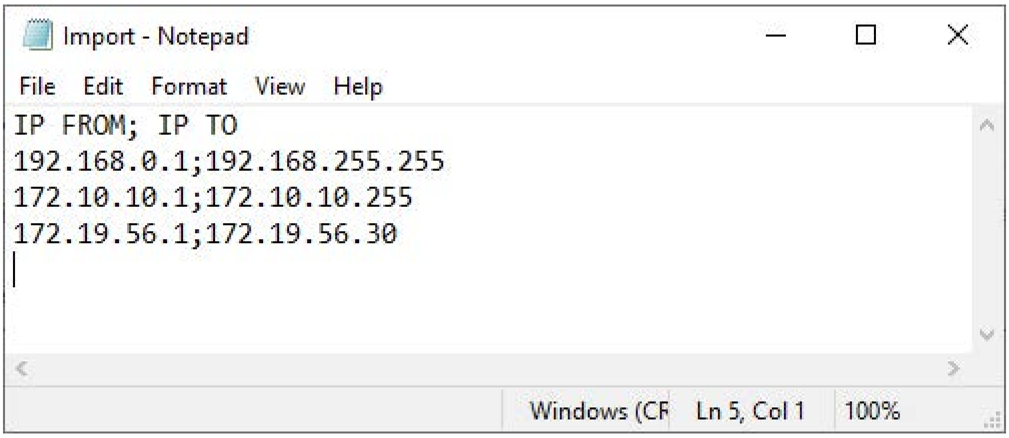
IP to: 172.31.3.150

☑	IP FROM	IP TO
☑	172.31.3.109	172.31.3.150

Pcap driver found.

Fig. 2 - IP Scan Wizard

If you want to specify several networks for inventory it is recommended to use the CSV import. You can call this up by choosing **Load list**. In the following figure the structure of the CSV file is described.



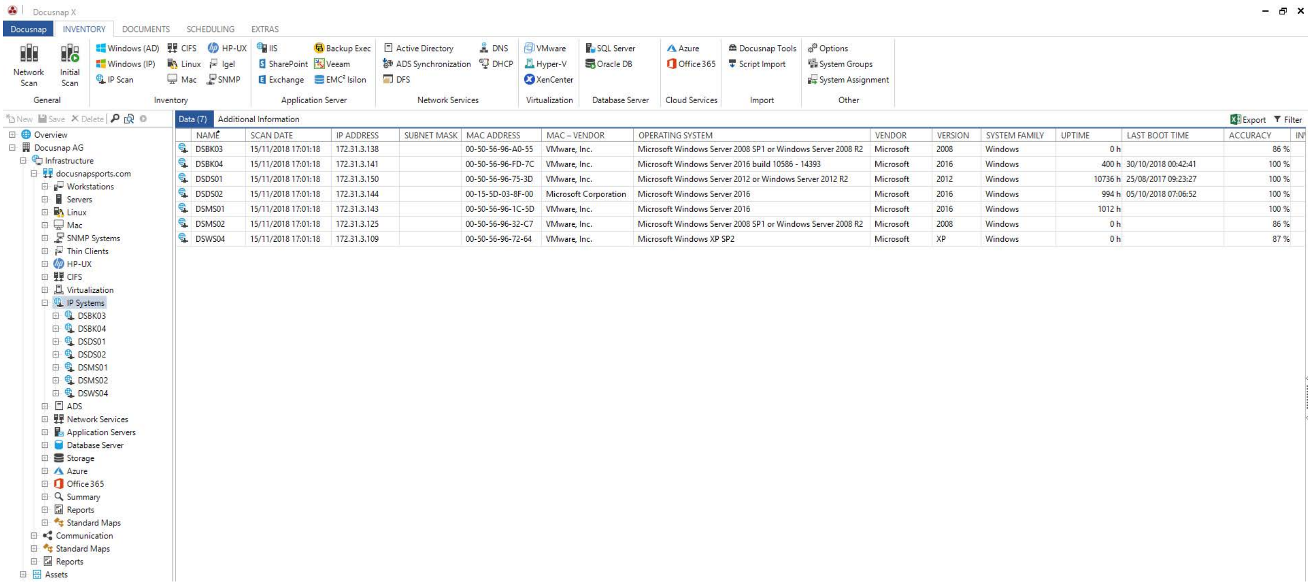
```
IP FROM; IP TO
192.168.0.1;192.168.255.255
172.10.10.1;172.10.10.255
172.19.56.1;172.19.56.30
```

Fig. 3 - IP Ranges - CSV Import

The maximum size of a network segment is limited to **Class B** (192.168.1.1 - 192.168. 255.255).

2.2 Analysis and Result

You can find the results of your IP Scan in the Docusnap data tree under Company - Infrastructure - Domain - IP Systems



NAME	SCAN DATE	IP ADDRESS	SUBNET MASK	MAC ADDRESS	MAC – VENDOR	OPERATING SYSTEM	VENDOR	VERSION	SYSTEM FAMILY	UPTIME	LAST BOOT TIME	ACCURACY	IN
DSBK03	15/11/2018 17:01:18	172.31.3.138		00-50-56-96-A0-55	VMware, Inc.	Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2	Microsoft	2008	Windows	0 h		86 %	
DSBK04	15/11/2018 17:01:18	172.31.3.141		00-50-56-96-FD-7C	VMware, Inc.	Microsoft Windows Server 2016 build 10586 - 14393	Microsoft	2016	Windows	400 h	30/10/2018 00:42:41	100 %	
DSDS01	15/11/2018 17:01:18	172.31.3.150		00-50-56-96-75-3D	VMware, Inc.	Microsoft Windows Server 2012 or Windows Server 2012 R2	Microsoft	2012	Windows	10736 h	25/08/2017 09:23:27	100 %	
DSDS02	15/11/2018 17:01:18	172.31.3.144		00-15-5D-03-8F-00	Microsoft Corporation	Microsoft Windows Server 2016	Microsoft	2016	Windows	994 h	05/10/2018 07:06:52	100 %	
DSMS01	15/11/2018 17:01:18	172.31.3.143		00-50-56-96-1C-5D	VMware, Inc.	Microsoft Windows Server 2016	Microsoft	2016	Windows	1012 h		100 %	
DSMS02	15/11/2018 17:01:18	172.31.3.125		00-50-56-96-32-C7	VMware, Inc.	Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2	Microsoft	2008	Windows	0 h		86 %	
DSWS04	15/11/2018 17:01:18	172.31.3.109		00-50-56-96-72-64	VMware, Inc.	Microsoft Windows XP SP2	Microsoft	XP	Windows	0 h		87 %	

Fig. 4 - Results of the Extended IP Scan

Overview of the information that can be captured:

- Name:	Name of the system. If a DNS entry exists, this DNS entry will be used as the name, otherwise the IP address.
- Scan Date:	Time at which the system was last captured by IP Scan
- IP Address:	IP address of the system
- Subnet Mask:	Subnet mask of the system
- MAC Address:	MAC address of the system
- MAC Vendor:	Vendor - Based on the MAC address entered
- Operating System:	Information on the operating system used
- Vendor:	Vendor of the operating system
- Version:	Version number of the operating system
- System Family:	Family, e.g. Windows or Linux
- Operating Time:	Time in hours
- Last Boot Start:	Date on which the system was last booted
- Accuracy:	Indication of the accuracy of the extended information in percent

With the help of advanced information such as the MAC vendor and information on the operating system, a general overview of the network can be obtained. The systems can then be assigned to an assistant for further inventory.

IP systems are considered in reports as well as in the network and Topology Plan.

2.3 MAC Filters for IP Systems

Some systems can only be captured via IP Scan because no other standard interface, e.g. SNMP, is supported. A MAC filter is available so that these systems can be displayed in the Topology Plan as telephones, for example. This makes it easier for you to distinguish the IP systems in the Topology Plan.

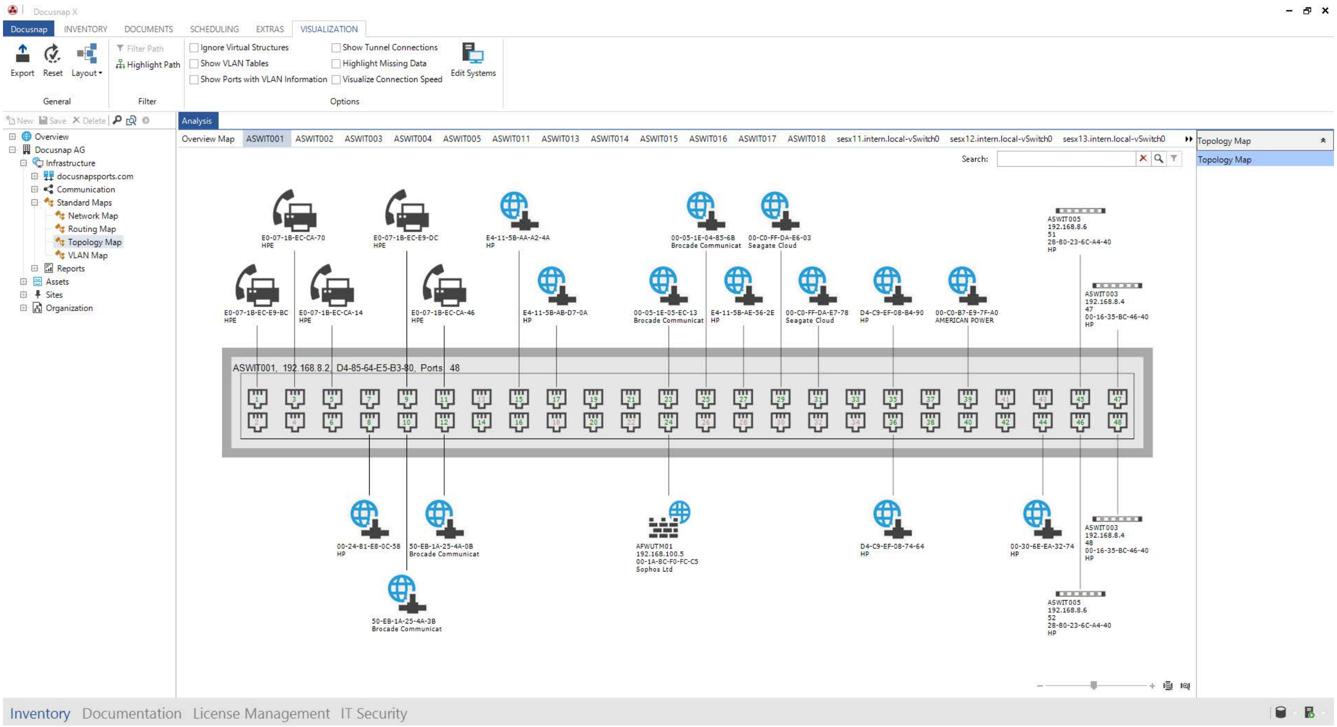


Fig. 5 - MAC Filters for IP Systems

Procedure:

- Identify the lowest common denominator at the MAC address. For two IP telephones, each with one MAC address **E0-07-1B-EC-CA-70** and **E0-07-1B-EC-E9-DC**, the lowest common denominator would be **E0-07-1B-**.
- Switch to Docusnap **Administration** - **Inventory** tab - **MAC filter**
- Put the MAC address there - **E0-07-1B-**
- Supported wildcard characters are ***** to specify multiple arbitrary characters and **?** to specify exactly one arbitrary character.

MAC addresses of the Ignore and Virtual type are no longer displayed in the Topology Plan.

Further information about the MAC Filter can be found in the Docusnap manual in the MAC Filter section. (F1 key in the corresponding area within the Docusnap Administration) or in the HowTo **Inventory and Analysis of SNMP** in the **Docusnap Knowledge Base**.

3. Optional: IP Scan Analysis Tool

The IP Scan Analysis Tool is available on request from Docusnap Support.

3.1 Purpose of Use

Every network is different. Thus, it can happen that the IP Scan does not deliver any results in rare cases. This can be caused by the virus scanner, the configuration of the firewall or a proxy. Various network components can affect the results of the IP Scan. The Docusnap IP Scan uses parameters in the standard which successfully inventory data for a large part of the networks. To get the best results with the IP Scan in your network, you can use the IP Scan Analysis Tool to find out the NMAP parameters that are right for you. You can then pass them to Docusnap.

The IP Scan Analysis Tool is a standalone application. No Docusnap installation is required. Prerequisite is the installation of the NPAC driver.

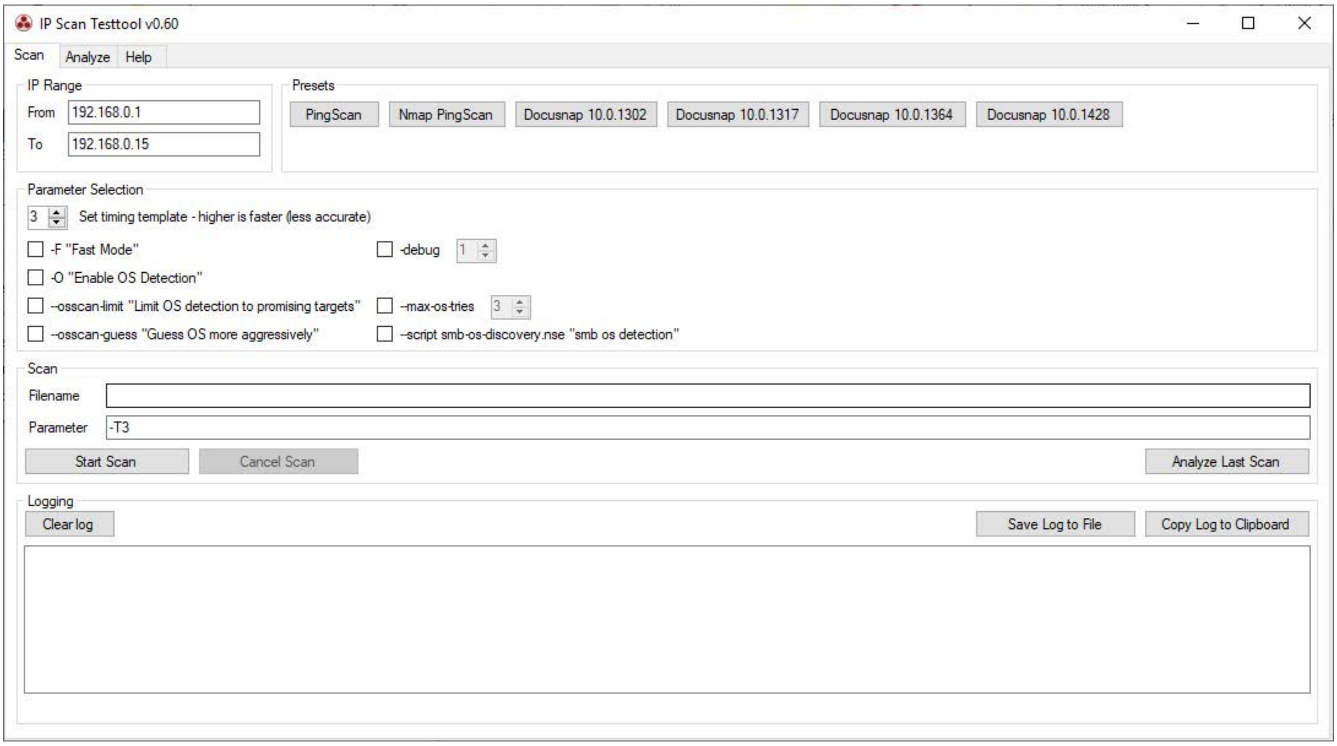
For the best possible analysis, you should run the IP Scan Analysis Tool on the same system as the Docusnap IP Scan is running on, e.g. Docusnap Server or Docusnap Discovery Service.

Standard parameters of the Docusnap IP Scan, Docusnap version 10.0.1472.2:

```
-&lt;font color="#ffff00"&gt;-==- proudly presents
```

3.2 Application of the Test Program

If you start the IP Scan Analysis Tool with a double-click, a new window opens. Within this GUI, you can perform an IP Scan, influence parameters, and then analyse the results.



IP Range
From 192.168.0.1
To 192.168.0.15

Parameter Selection
3 Set timing template - higher is faster (less accurate)
□ -F "Fast Mode" □ -debug 1
□ -O "Enable OS Detection"
□ --osscan-limit "Limit OS detection to promising targets" □ --max-os-tries 3
□ --osscan-guess "Guess OS more aggressively" □ --script smb-os-discovery.nse "smb os detection"

Scan
Filename
Parameter -T3

Fig. 6 - IP Scan Analysis Tool GUI

The Analysis Tool is divided into three areas. **Scan**, **Analyze** and **Help**.

3.2.1 Scan

Within the **Scan** area it is possible to adjust the parameters according to your network. You can also use **presets** to do this. The presets differ in the parameters used. The following presets are available:

• PingScan:	Parameter -PE - Ping. (echo reply expected)
• Nmap PingScan:	Parameter -sP - simple IP Scan in Docusnap
• Docusnap Version:	Uses NMAP parameters of the respective Docusnap version

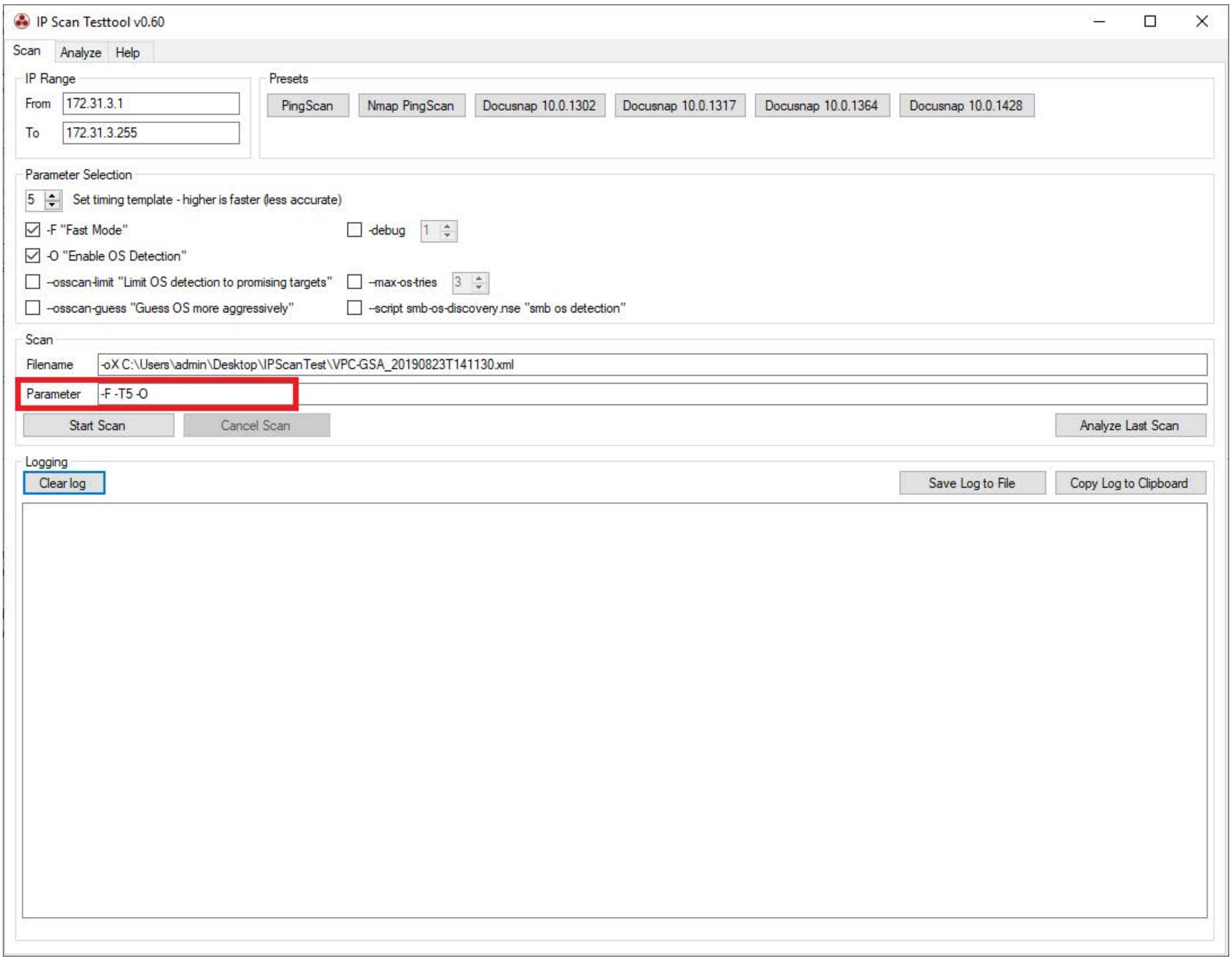
You can adjust the parameters to be used under **Parameter Section**. Parameters can be selected using the checkboxes or added by entering text into the text box **Parameter**. A detailed overview of all available NMAP parameters can be found at https://nmap.org/.

In the following example the scan is performed with the preset of the last Docusnap version. The parameters are set automatically with a click on the respective preset. The **Start Scan** button starts the scan with the specified parameters.

The parameters used and the path of the log file can be found in the respective text boxes. Logfiles are saved in an automatically created folder on your desktop. In the logging, you see information about the current status of the scan.

Example:
In order to accelerate the execution of the IP Scan, the speed is increased and the measures for operating system detection are minimized.

Note that increasing the speed can affect the quality of the results.



From 172.31.3.1
To 172.31.3.255

5 Set timing template - higher is faster (less accurate)

☑ -F "Fast Mode" □ -debug 1

☑ -O "Enable OS Detection"

□ --osscan-limit "Limit OS detection to promising targets" □ --max-os-tries 3

□ --osscan-guess "Guess OS more aggressively" □ --script smb-os-discovery.nse "smb os detection"

Filename -oX C:\Users\admin\Desktop\IPScanTest\VPC-GSA_20190823T141130.xml

Parameter -F -T5 -O

Fig. 7 - Customizing the IP Scan Analysis Tool Parameters

3.2.2 Analyze

In the **Analyze** area you can evaluate the results of your last or previous scans. More detailed information on analysis can be found in the following chapter Analysing Results

3.2.3 Help

Within the **Help** tab you will find more information about **timing settings** and **analysis**.

3.3 Transfer to Docusnap

3.3.1 Analysing results

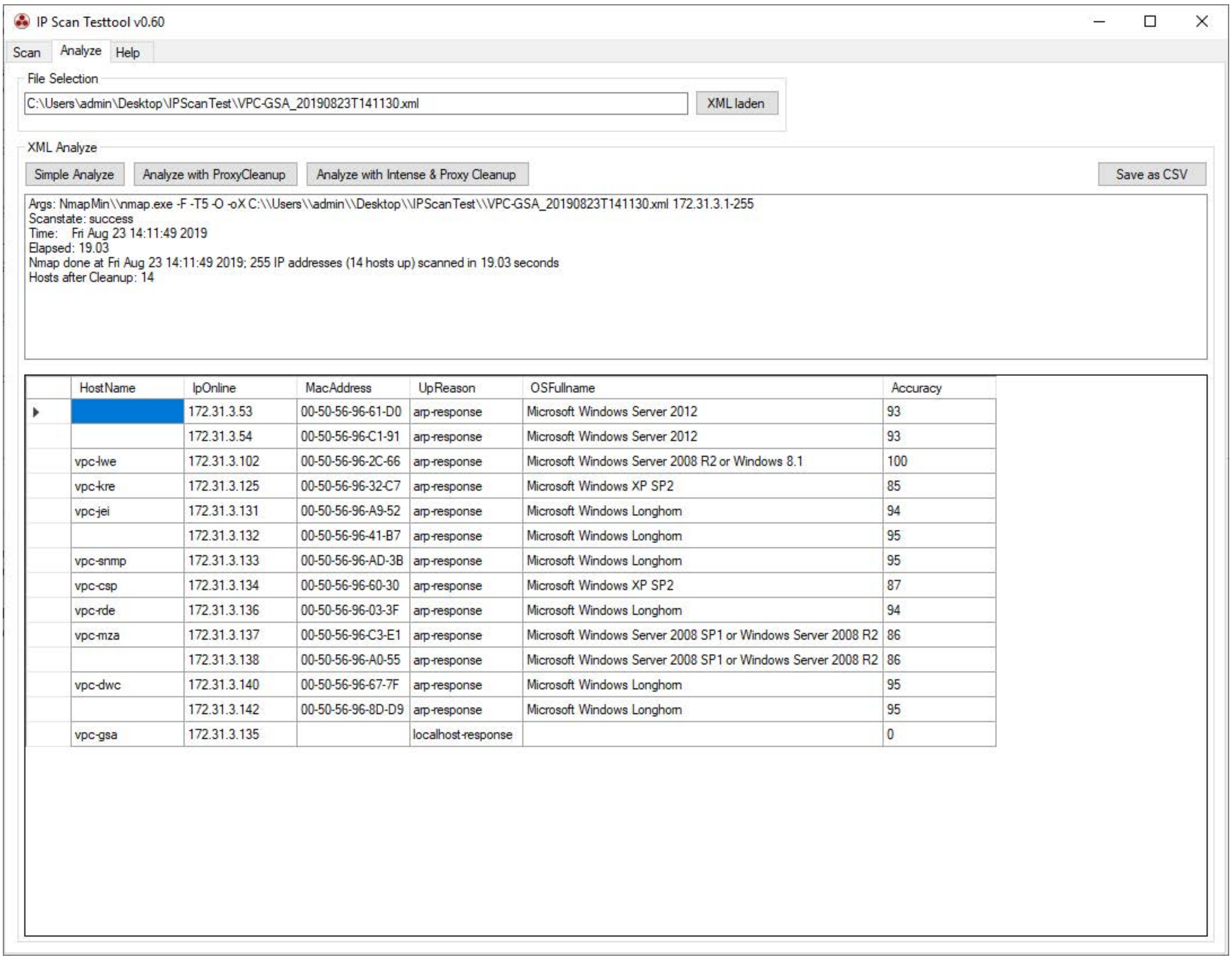
You can then evaluate the results of your scans in the Analyze area. By default, the IP Scan Analysis Tool opens the last scan performed. If you want to evaluate a certain scan, you can load the desired .xml file into the analysis window via File Selection.

A distinction is made between Simple Analyze and Analyze with ProxyCleanup.

In the Simple Analyze, only the results from the scan are evaluated. Incorrectly detected hosts, e.g. triggered by a transparent proxy, are not filtered.

In a Cleanup Analyze, the detected hosts are then filtered in the same way as in Docusnap. This tries to filter out hosts that were wrongly recognized as positive. In networks with a transparent proxy, it may happen that the proxy responds to every request of the IP Scan. Thus all addresses are recognized as positive. The Cleanup function is used to filter out incorrectly detected systems. You can then see the results of your scan in the analysis window and export them to a CSV file, for example.

If the results of the scan correspond to the systems of your network, you can then pass the parameters you set to Docusnap.



File Selection: C:\Users\admin\Desktop\IPScanTest\VPC-GSA_20190823T141130.xml

```
Args: NmapMin\\nmap.exe -F -T5 -O -oX C:\\Users\\admin\\Desktop\\IPScanTest\\VPC-GSA_20190823T141130.xml 172.31.3.1-255
Scanstate: success
Time:   Fri Aug 23 14:11:49 2019
Elapsed: 19.03
Nmap done at Fri Aug 23 14:11:49 2019; 255 IP addresses (14 hosts up) scanned in 19.03 seconds
Hosts after Cleanup: 14
```

	HostName	IpOnline	MacAddress	UpReason	OSFullname	Accuracy
▶		172.31.3.53	00-50-56-96-61-D0	arp-response	Microsoft Windows Server 2012	93
		172.31.3.54	00-50-56-96-C1-91	arp-response	Microsoft Windows Server 2012	93
	vpc-lwe	172.31.3.102	00-50-56-96-2C-66	arp-response	Microsoft Windows Server 2008 R2 or Windows 8.1	100
	vpc-kre	172.31.3.125	00-50-56-96-32-C7	arp-response	Microsoft Windows XP SP2	85
	vpc-jei	172.31.3.131	00-50-56-96-A9-52	arp-response	Microsoft Windows Longhorn	94
		172.31.3.132	00-50-56-96-41-B7	arp-response	Microsoft Windows Longhorn	95
	vpc-snmp	172.31.3.133	00-50-56-96-AD-3B	arp-response	Microsoft Windows Longhorn	95
	vpc-csp	172.31.3.134	00-50-56-96-60-30	arp-response	Microsoft Windows XP SP2	87
	vpc-rde	172.31.3.136	00-50-56-96-03-3F	arp-response	Microsoft Windows Longhorn	94
	vpc-mza	172.31.3.137	00-50-56-96-C3-E1	arp-response	Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2	86
		172.31.3.138	00-50-56-96-A0-55	arp-response	Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2	86
	vpc-dwc	172.31.3.140	00-50-56-96-67-7F	arp-response	Microsoft Windows Longhorn	95
		172.31.3.142	00-50-56-96-8D-D9	arp-response	Microsoft Windows Longhorn	95
	vpc-gsa	172.31.3.135		localhost-response		0

Fig. 8 - Results of the IP Scan Analysis Tool

3.3.2 Adaptation of the Docusnap IP Scan Configuration

The NMAP parameters for the IP Scan are performed in **DocusnapSettings.xml**. Please note that this adjustment must be carried out on every system. If, for example, you have several Docusnap Discovery Services in use, the DocusnapSettings.xml must be adapted on the respective system.

If no parameters are set, the Docusnap IP Scan automatically uses the parameters of the respective Docusnap version.

By default, DocusnapSettings.xml is located on the Docusnap or Docusnap Discovery Service host system in the following directory:

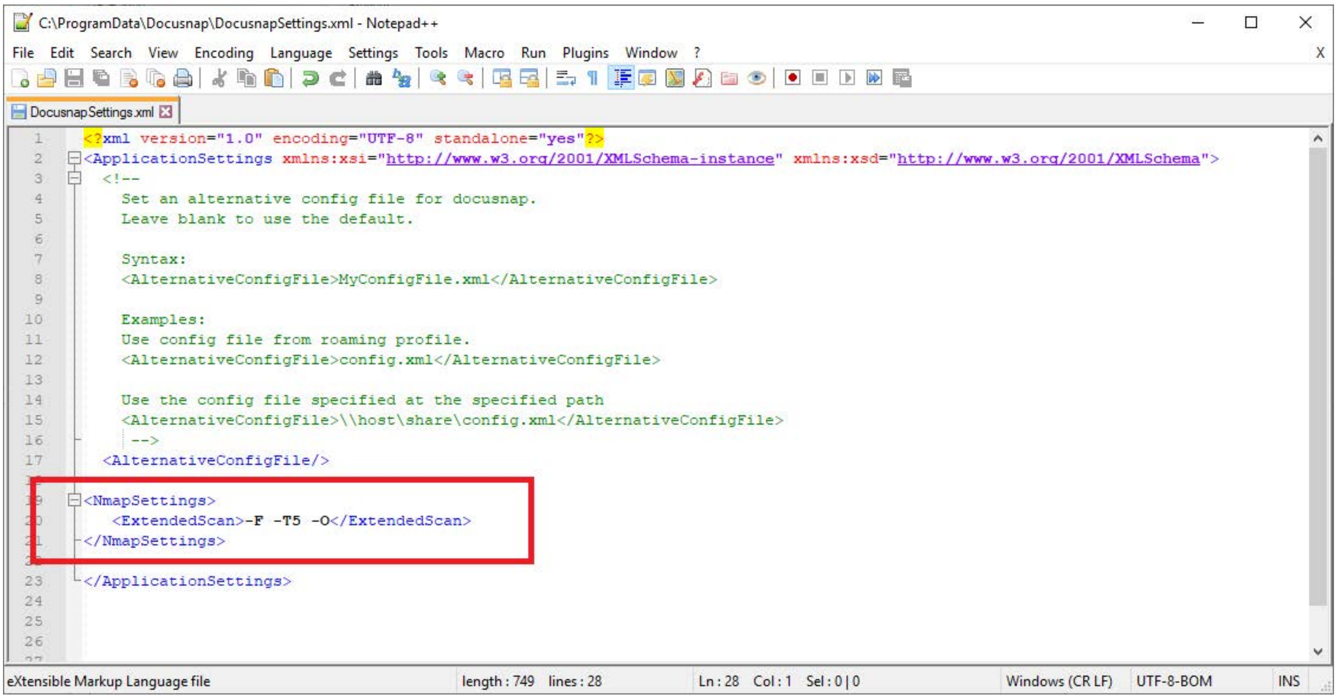
C:\ProgramData\Docusnap\DocusnapSettings.xml

You can edit DocusnapSettings.xml with a text editor, such as Notepad.

Within the <ApplicationSettings> tags the new tags are inserted. Between the <ExtendedScan> tags you can then store your parameters.

NMAP parameter tags for DocusanpSettings.xml:

```
<NmapSettings>
    <ExtendedScan></ExtendedScan>
</NmapSettings>
```



C:\ProgramData\Docusnap\DocusnapSettings.xml - Notepad++
File
Edit
Search
View
Encoding
Language
Settings
Tools
Macro
Run
Plugins
Window
?
DocusnapSettings.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ApplicationSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <!--
    Set an alternative config file for docusnap.
    Leave blank to use the default.

    Syntax:
    <AlternativeConfigFile>MyConfigFile.xml</AlternativeConfigFile>

    Examples:
    Use config file from roaming profile.
    <AlternativeConfigFile>config.xml</AlternativeConfigFile>

    Use the config file specified at the specified path
    <AlternativeConfigFile>\\host\share\config.xml</AlternativeConfigFile>
     -->
  <AlternativeConfigFile/>

<NmapSettings>
   <ExtendedScan>-F -T5 -O</ExtendedScan>
</NmapSettings>

</ApplicationSettings>
```

eXtensible Markup Language file
length : 749   lines : 28
Ln : 28   Col : 1   Sel : 0 | 0
Windows (CR LF)
UTF-8-BOM
INS

Fig. 9 - NMAP Parameters in Docusnap - DocusanpSettings.xml

4. Application Cases and Practical Examples

4.1 Initial Inventory

A complete and detailed inventory of a network environment is only possible with sufficiently privileged users. Often the person taking the inventory has neither root access to Linux systems nor administrative access to Windows systems for a new customer. Nevertheless, the network needs a first overview.

The advanced IP Scan allows you to analyse the desired networks without the need for administrative rights. You can find out how many systems are available. With the help of the operating system information it is then possible to subdivide the data into corresponding categories.

- ➔ Number of Windows systems
- ➔ Number of Linux systems
- ➔ Number of possible SNMP systems
- ➔ Etc.

4.2 Increase data quality

A prerequisite for high-quality documentation is good data quality in Docusnap. Since there is often no overview of the existing systems, it is not possible to check the inventoried systems against each other. With the help of the IP Scan it is possible for you to create an overview with unknown systems and to capture them specifically.

Initial situation:
All the company's printers are in the XYZ network. This network is already regularly inventoried via SNMP. In order to make sure that all systems within the network are really captured, the IP Scan is also used regularly.

In this case, if devices are not yet included in Docusnap, they will now be added to the IP systems.

You should then check the IP systems that have been captured with regard to the SNMP interface.

If these systems are recorded as SNMP systems in the future, the entry below the IP systems will be moved. However, a downgrade is not possible - e.g. SNMP to IP system.

4.3 Detect Security Vulnerabilities

Bring your own device, old network components and Internet of Things. These systems are often associated with security vulnerabilities. The following describes how you can detect, document and react to security vulnerabilities using the Docusnap IP Scan.

Detect old network components:

In a growing network, more and more old systems may become available over time. Depending on the function, this can result in a security gap. If these systems do not support at least the SNMP protocol as an interface, it will be difficult to record, document and react accordingly.

The IP Scan allows you to perform a regular scan of your network. If, for example, an old switch is still in use, it is detected by the IP Scan. This will prevent your network from failing due to outdated hardware, for example.

Bring your own Device / Internet of Thins

The statement "Every new refrigerator has an IP address" does not quite correspond to reality, but hits the nail on the head. Various systems are connected to the networks of a company. From workstations, servers, private mobile phones to everyday systems, everything is included. Due to the security of the network, these are often divided into different areas. Security gaps can occur if the coffee machine is suddenly available in the same VLAN as the switches.

To detect such a misconfiguration, the IP Scan is a good choice. Since all active systems are captured on the network, you can also find the everyday systems and other devices and check their network configuration.

LIST OF FIGURES

FIG. 1 - NPCAP SETUP 5
FIG. 2 - IP SCAN WIZARD 7
FIG. 3 - IP RANGES - CSV IMPORT 8
FIG. 4 - RESULTS OF THE EXTENDED IP SCAN 9
FIG. 5 - MAC FILTERS FOR IP SYSTEMS 10
FIG. 6 - IP SCAN ANALYSIS TOOL GUI 12
FIG. 7 - CUSTOMIZING THE IP SCAN ANALYSIS TOOL PARAMETERS 13
FIG. 8 - RESULTS OF THE IP SCAN ANALYSIS TOOL 14
FIG. 9 - NMAP PARAMETERS IN DOCUSNAP - DOCUSANPSETTINGS.XML 15

VERSION HISTORY

date	Description of the
October 7, 2019	Version 1.0 - Description of the IP Scan

Docusnap®