

Network Performance

DOMAIN 3.0

MODULE 11



Networking Performance Topics

Monitoring Performance

Common Metrics

SNMP

NetFlow

Network Security Monitoring



Monitoring Performance



What are Metrics?

Performance values that you monitor

You watch trends to:

- Identify incidents and problems
- Plan for upgrades
- Redistribute load if necessary



Out-of-Band Management

Out of band management refers to using a different communication path, outside the normal network, to remotely access and administer a device

The idea is that if the network is down, you can't use it to connect to fix the problem

Modems and console cables are the most common forms of oob management

You can connect a modem directly to a device

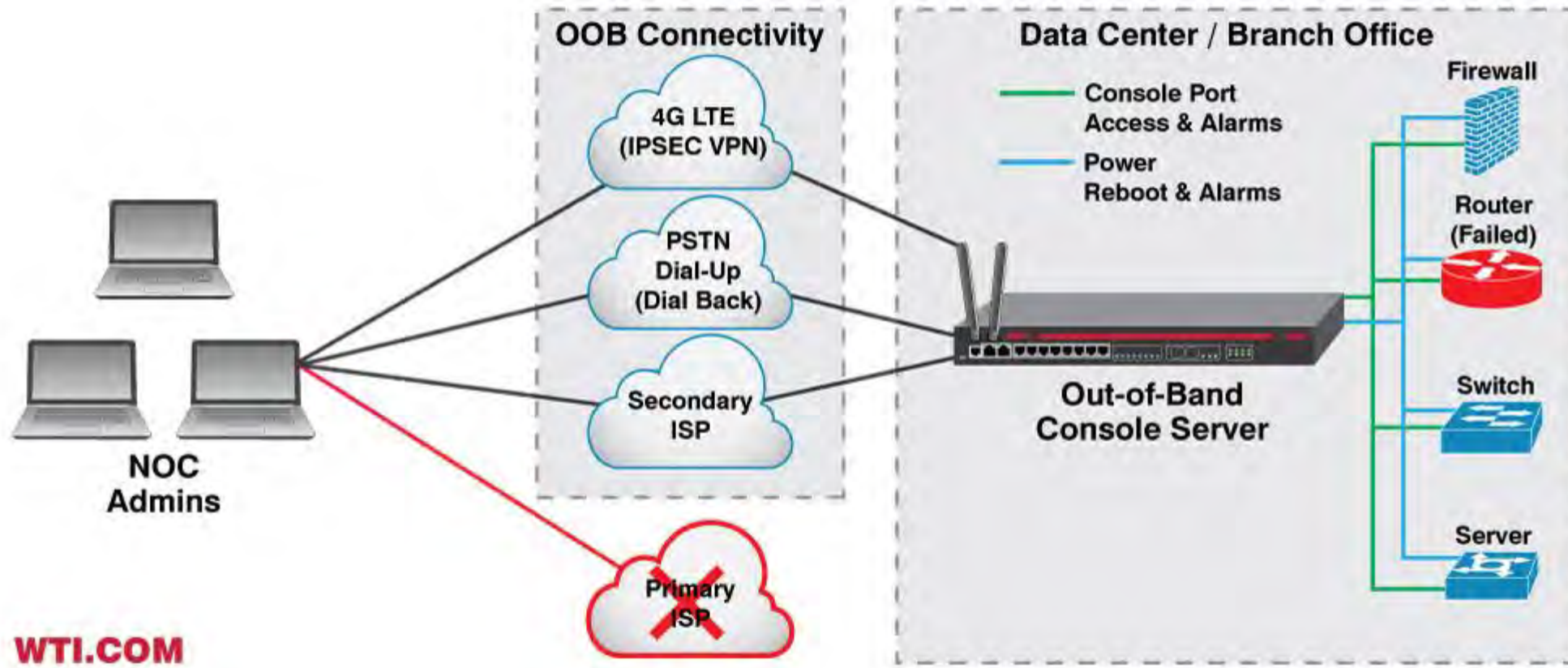
You can also connect to a dedicated server that has console connections to several devices

- A dedicated server should be able to function independently, and not rely on the devices you are attempting to repair

In some cases, you will not be able to resolve an issue remotely

- You'll have to travel to the datacenter, or have a technician present there, to reboot systems, start generators, troubleshoot physical or environmental issues, etc.

Out-of-Band Management Example



What is a Baseline?

In a general sense, the term *baseline* refers to a minimum requirement

It can also refer to a starting point, for the administrator to improve upon, until the desired baseline is achieved

In security, the word *baseline* refers to configurations and settings necessary for a system to meet a minimum level of security

In terms of performance, *baseline* refers to the acceptable minimum level of performance

In networking, the term *baseline* can refer to a snapshot of “normal” traffic patterns

- Network traffic is recorded for a few weeks, and then analyzed to create a profile of existing patterns
- The profile is then used to identify and track new trends and patterns, including undesirable and abnormal traffic

In all cases, the initial baseline might not be the desired target

- After the first baseline is recorded, security issues and performance bottlenecks should be remediated
- Then another (hopefully desired) baseline can be captured and used as a reference

What to Baseline

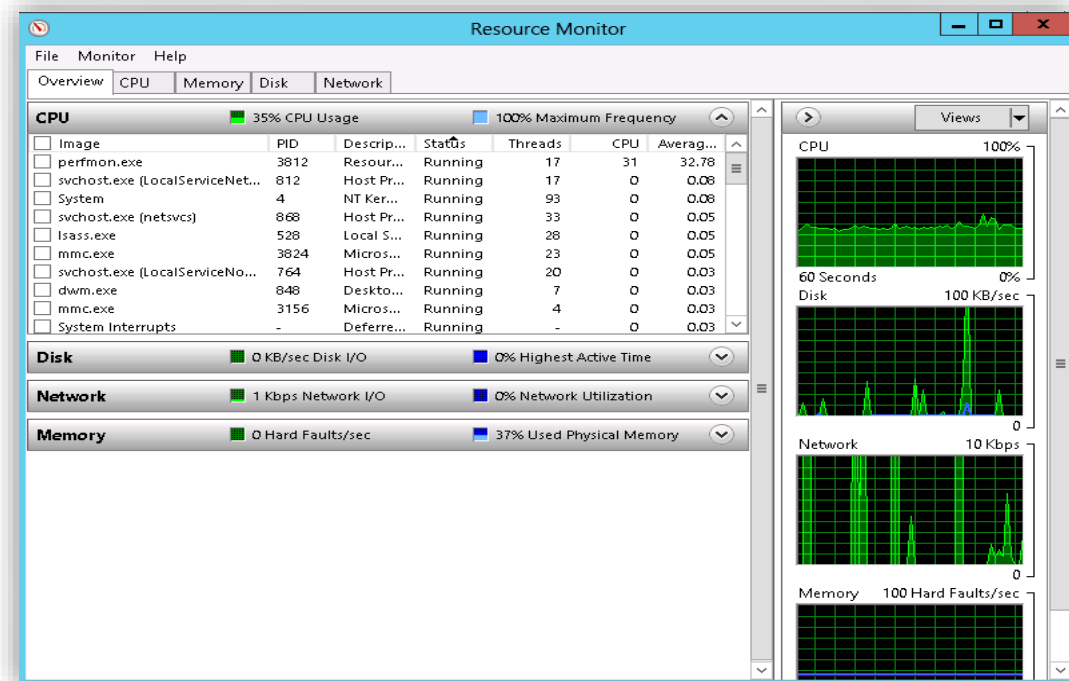
Performance of critical systems

- CPU, RAM, Disk, Network Interface

Database performance

Performance of critical processes

- Operational/human as well as technical



What is a Network Traffic Baseline?

In terms of network traffic, a baseline is a profile of what traffic on your network “normally” looks like

You record and analyze network traffic and performance for a week or two

The analysis gives you a benchmark to identify new traffic patterns and trends

You can compare and chart normal to abnormal traffic

You should baseline and review:

- all traffic to the Internet
- all traffic for business critical applications
- all traffic to/from critical systems
- and all systems backup traffic

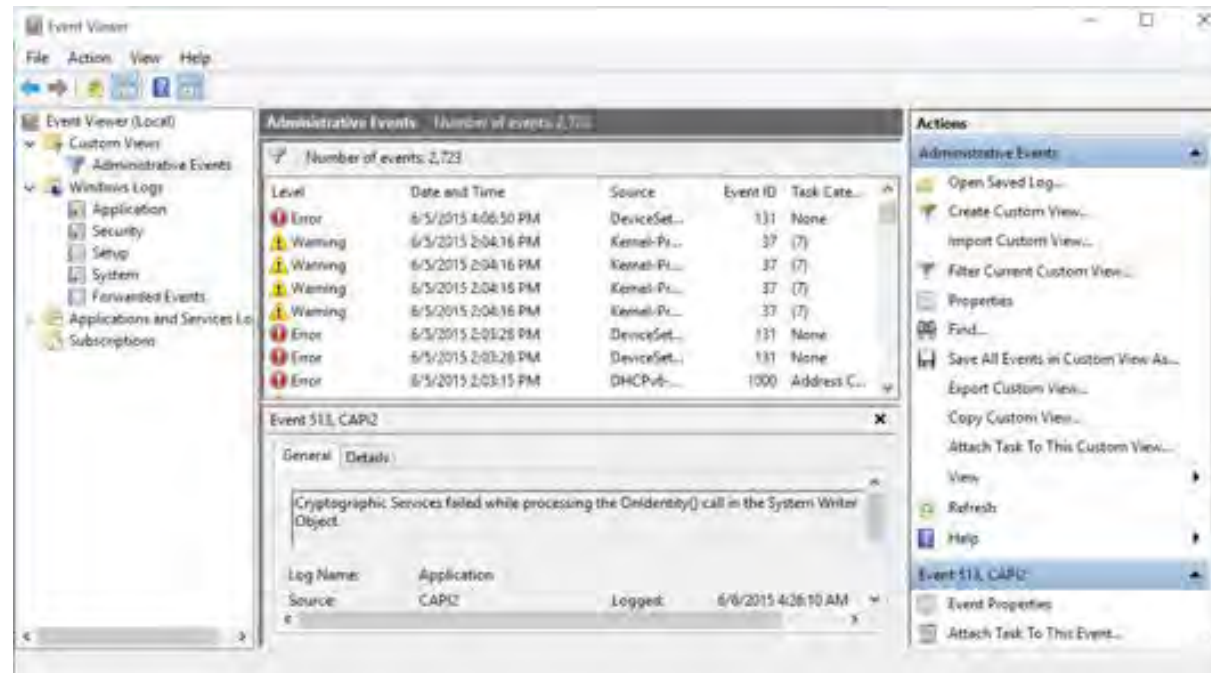
After conducting an initial baseline scan, you should mitigate vulnerabilities and performance bottlenecks, then create a new baseline

Log Reviewing

Review logs as a proactive measure for planning, performance, troubleshooting, and security

Compare logs to baseline

Collect evidence of security events



Network Device Logs

You can review device logs to see events that have happened on the network

You can correlate entries from various logs to get a larger picture of an incident

You can search device logs when auditing for security violations or attacks

To ensure that log data remains safe, you can forward logs to a Syslog server

You can filter logs to focus on:

- Specific types of entries
- Specific severity levels

When remotely accessing the console of a Cisco device, you will have to specify the logging level

To see all logging, you might have to physically be present at the device and connect to the console



Common Metrics



Uptime / Downtime

The most basic metric you can track on a device, link or system

How long something has been down or up is a very common starting point for other investigations

You can use outside systems to regularly ping a device or service and log any failures to respond

You can also check timestamps in a system log to see time gaps, as well as when a system or service restarted

Interface Statistics / Status

Depending on the device type, an interface can give you various statistics:

Link State (Up / Down)

Speed / Duplex

Encapsulation type

Reliability, Tx and Rx load

Cyclical Redundancy Checks (CRCs)

Input and output packet and byte counts

Error counts by type

```
Switch#show int fa0/3
FastEthernet0/3 is up, line protocol is up (connected)
  Hardware is Lance, address is 0003.e434.0503 (bia 0003.e434.0503)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

Interface Errors

CRC Errors

Giants

Runts

Collisions

Encapsulation Errors

```
5 minute output rate 0 bits/sec, 0 packets/sec
 956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
2357 packets output, 263570 bytes, 0 underruns
0 output errors, 0 collisions, 10 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Device/Chassis Counters

Here are basic counters you can monitor on most network devices and servers:

Temperature

- CPU, fan, GPU, Voltage Regulator Module (VRM), chipset

CPU Usage

- Total, per core, per process

Memory

- Physical memory use
- available memory
- virtual memory
- used/committed memory
- page faults/sec

Disk

- Storage used / remaining
- Disk busytime

Bandwidth utilization

- Total, per interface



Network Metrics

Bandwidth

- Total available bandwidth

Bandwidth utilization

- The percentage of bandwidth being utilized

Packet drops

- The number of packets on a network that do not reach their intended destination

Packet error rate

- The frequency of errors

Realtime Traffic Metrics

Monitoring loss, latency, and jitter informs the administrator that more needs to be done to provide QoS for realtime traffic such as VoIP, collaborative video, online gaming

Packet loss

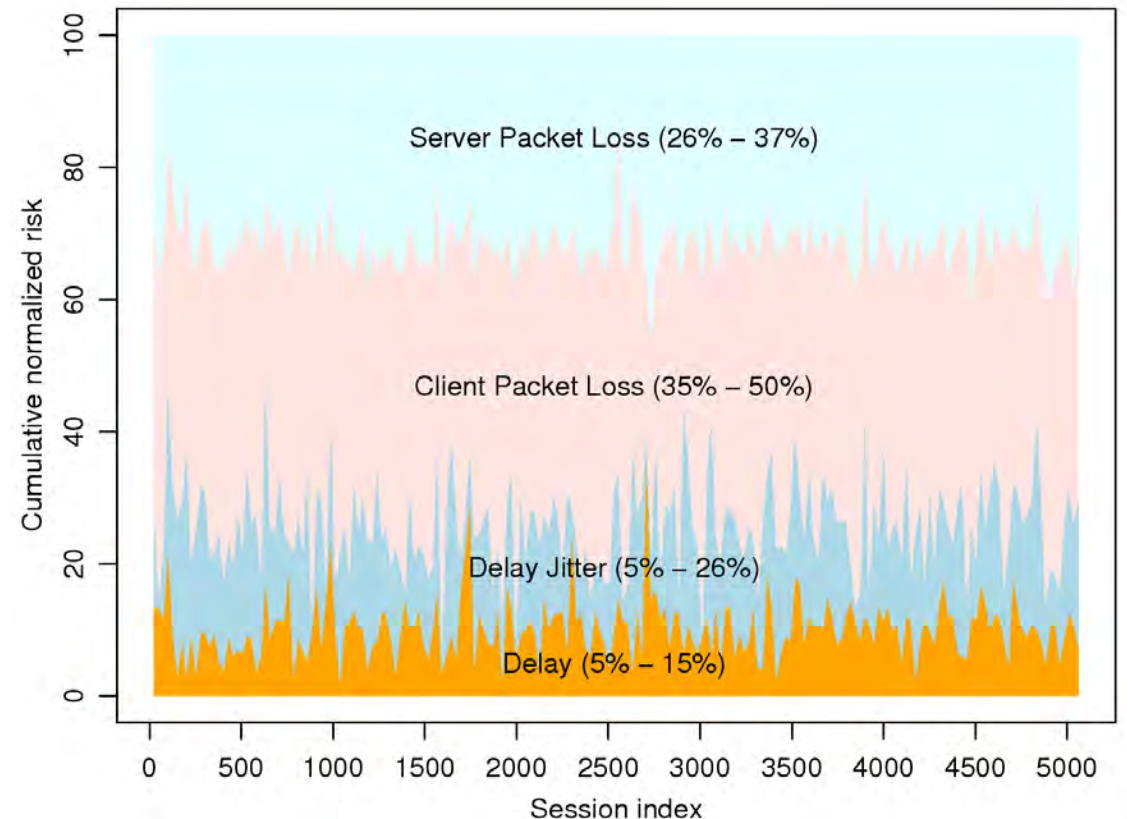
- Packets that never arrive

Latency

- Delay between transmission and reception

Jitter

- Variable delay
- Worst impact on audio
- Hardest to compensate for



UPS Metrics

Input and output voltage

Battery charge (percentage)

Load

Battery status

Battery current

- positive when discharging
- negative when charging

Time remaining before shutoff due to low battery

Temperature



Environmental Factors and Sensors

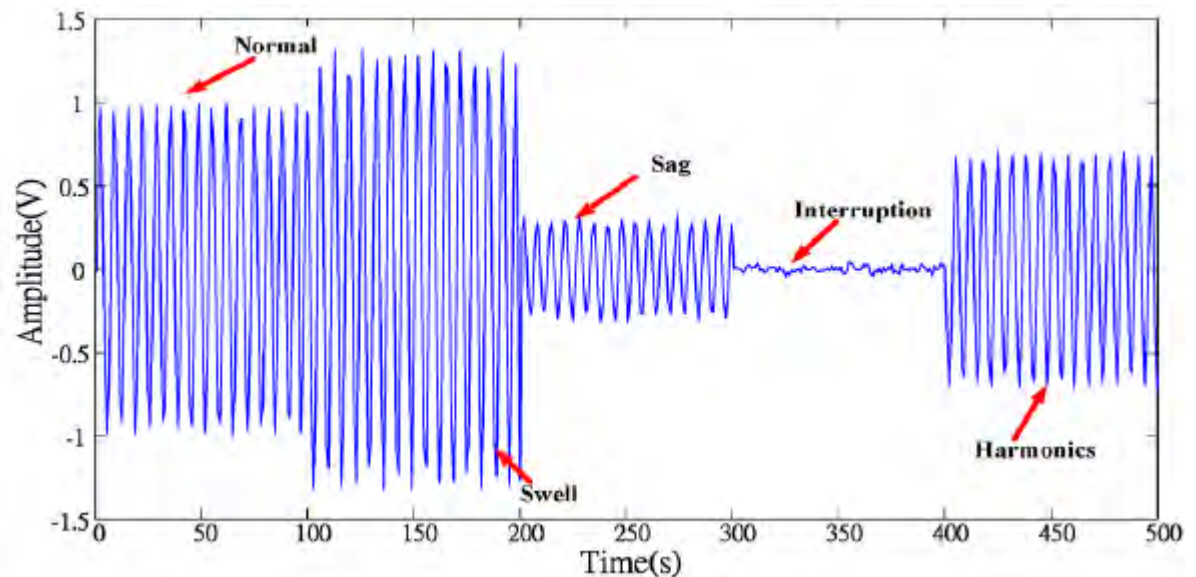
Temperature

Humidity

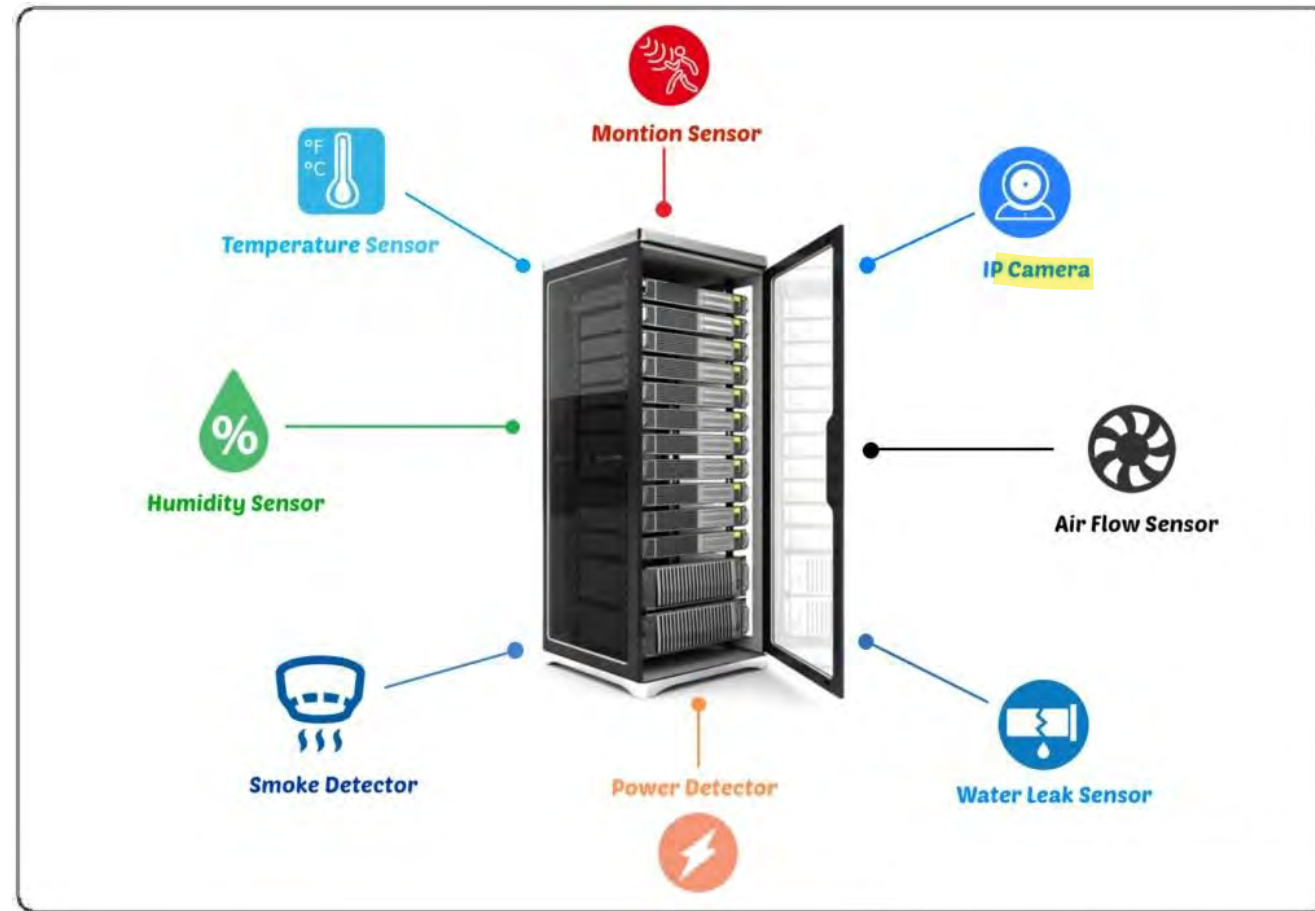
Electrical

- Line voltage
- Spikes, sags, surges
- Blackouts, brownouts
- Frequency and harmonics

Power Quality Over Time Example



Server Room Environmental Remote Monitoring





SNMP



Simple Network Management Protocol (SNMP)

Used to centrally monitor devices on a network

An SNMP manager polls agents for information

- Polling is done round-robin style, on a regular interval (every few minutes)
- Manager is software on a server or workstation
- Agent is small software installed or built into a device OS

The manager uses a Management Information Base (MIB) to know what types of information an agent can provide

- A MIB is a set of counters (Object IDs) relevant to the device

SNMP Security

SNMP has several versions that are still in use

- v1, v2, v2c all communicate in clear text
- v3 is encrypted
- Not all devices support v3

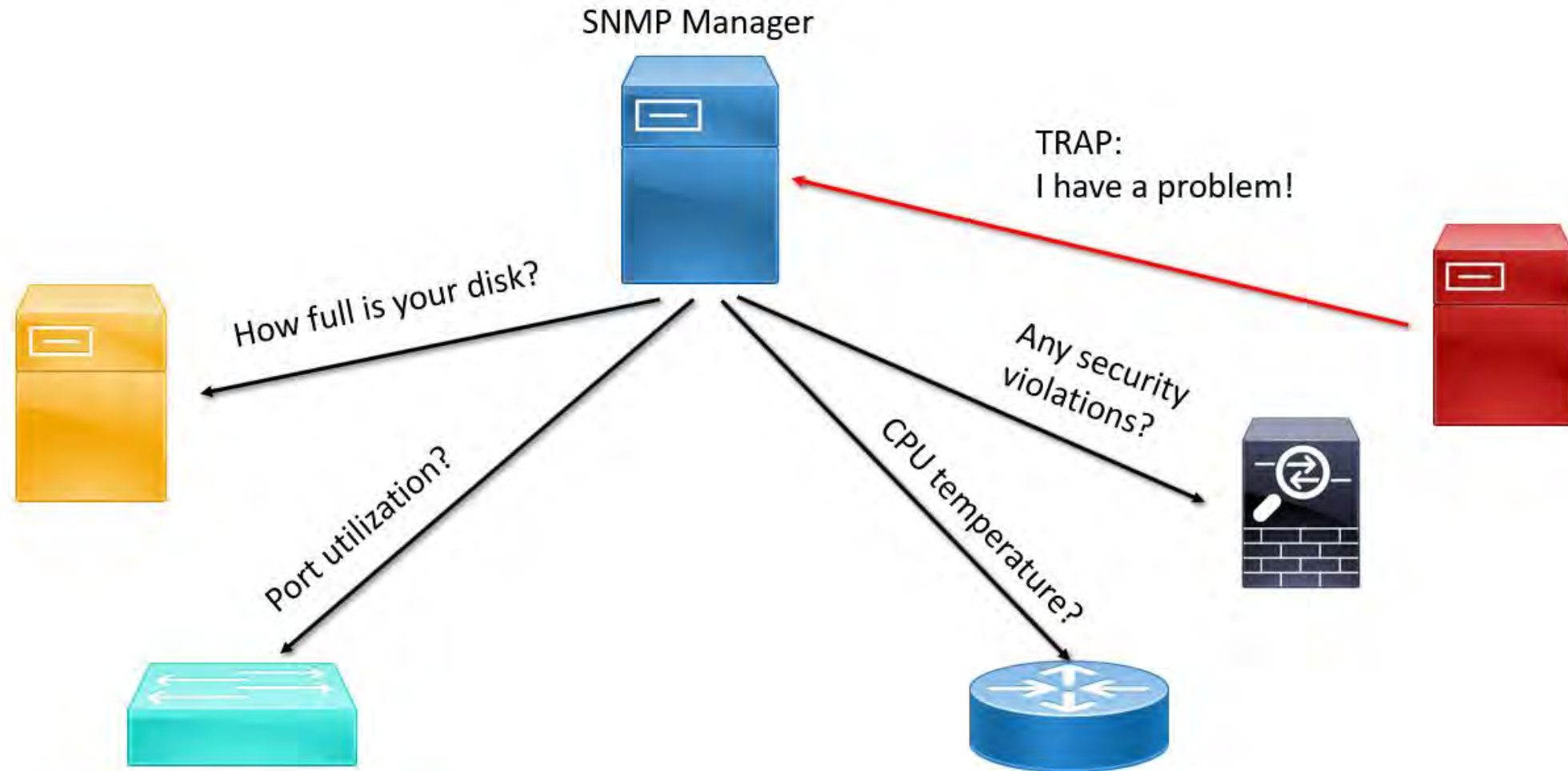
Both the manager and agent are configured with a simple authentication mechanism called the “community string”

- Simple text string
- An agent will only respond to a manager that has the same community string
- There are two default community strings:
 - “Public” – for read-only queries
 - “Private” – for read/write communications
 - You should change your community strings for security

SNMP Ports:

- UDP 161 - Manager queries and agent replies
- UDP 162 – Agents “raise traps” (send pre-configured alerts) to the manager

SNMP Process Example



SNMP Components

Managed Devices

- Router, switch, hub, firewall, computer, server service (DHCP, DNS, etc.) printer, IoT device

Agents

- Software installed on managed device
- Responds to the NMS

Network Management System (NMS)

- Typically software installed on a dedicated computer

SNMP Network Management System

Aka SNMP Manager

Uses SNMP to query devices about their current status

Uses a Management Information Base (MIB) to know what questions to ask the various devices

Different devices have their own MIBs

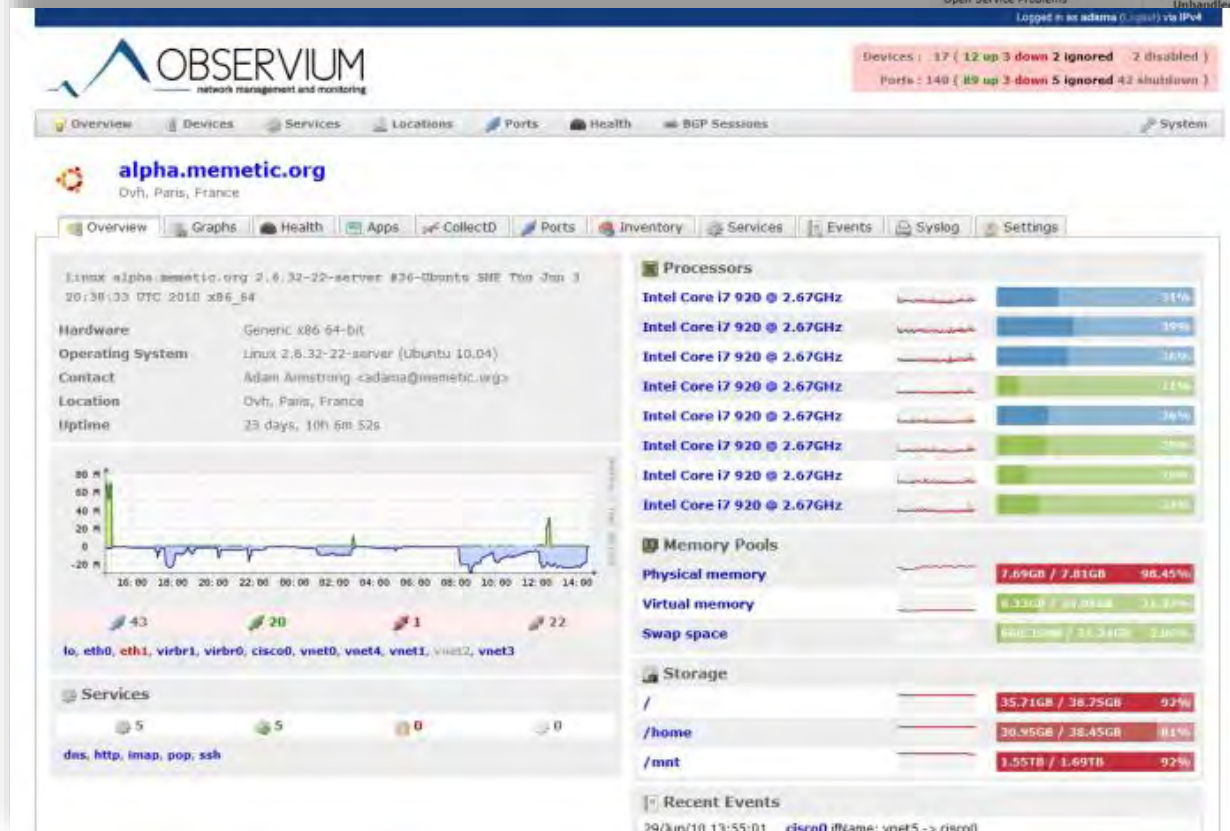
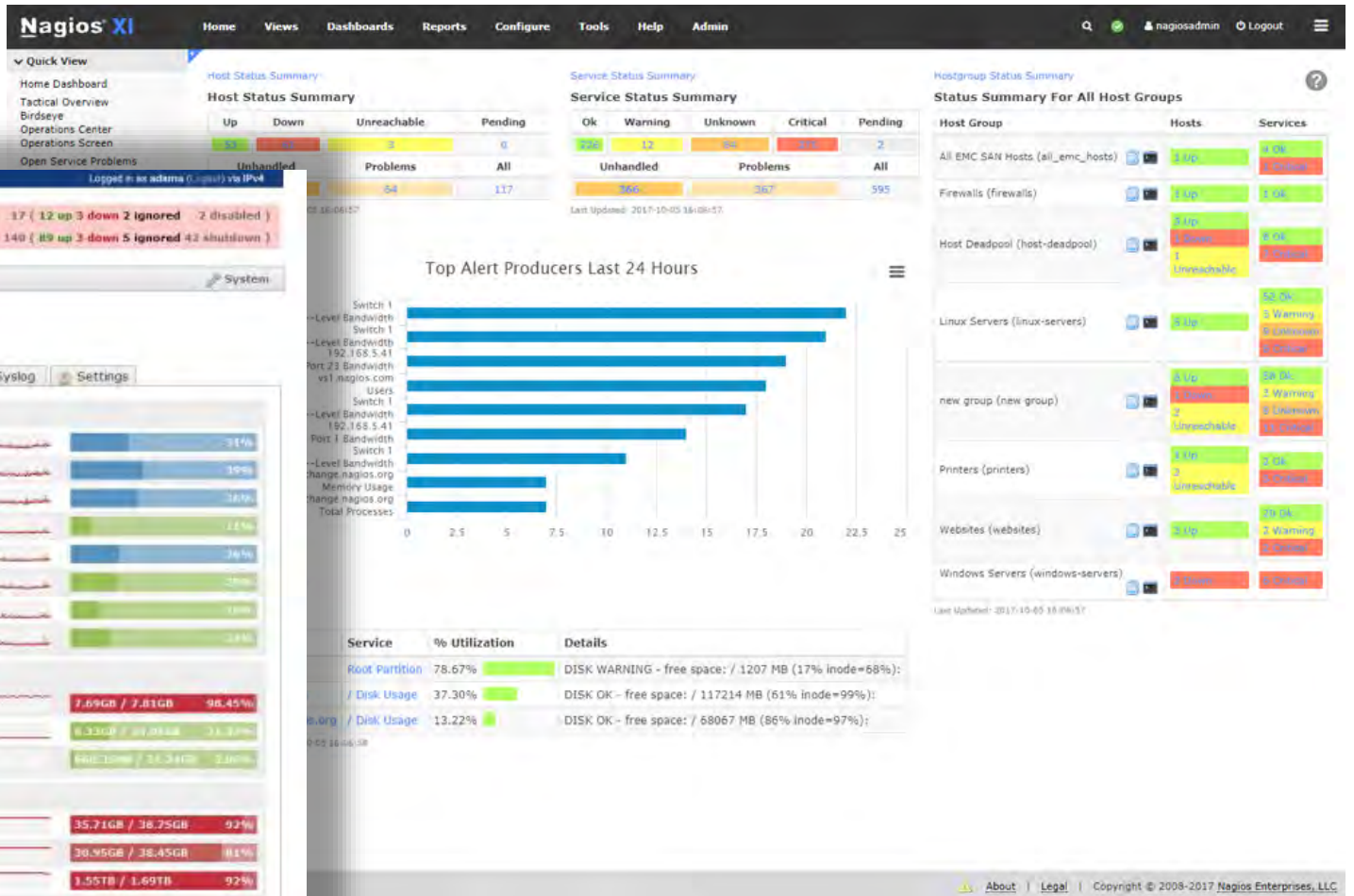
The manager “walks” through the MIB

SNMP message types:

- Get
- GetNext
- Set
- Trap



SNMP Management Console Examples



Object Identifier (OID)

Represents a single “question” an SNMP manager can ask an agent

Identifies a very specific, unique counter on a device

Has a corresponding name and data type

When queried by manager, agent will return a value

Name/OID	Value	Type
.1.3.6.1.2.1.1.1.0 (.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0)	Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE ...	OctetString

Management Information Base (MIB)

A collection of OIDs stored in a text file

A set of questions that an SNMP manager can ask a device regarding its status

Standardized vendor-neutral MIBs define functionality common to all devices of the same type

The manufacturer creates additional MIBs specific to their products

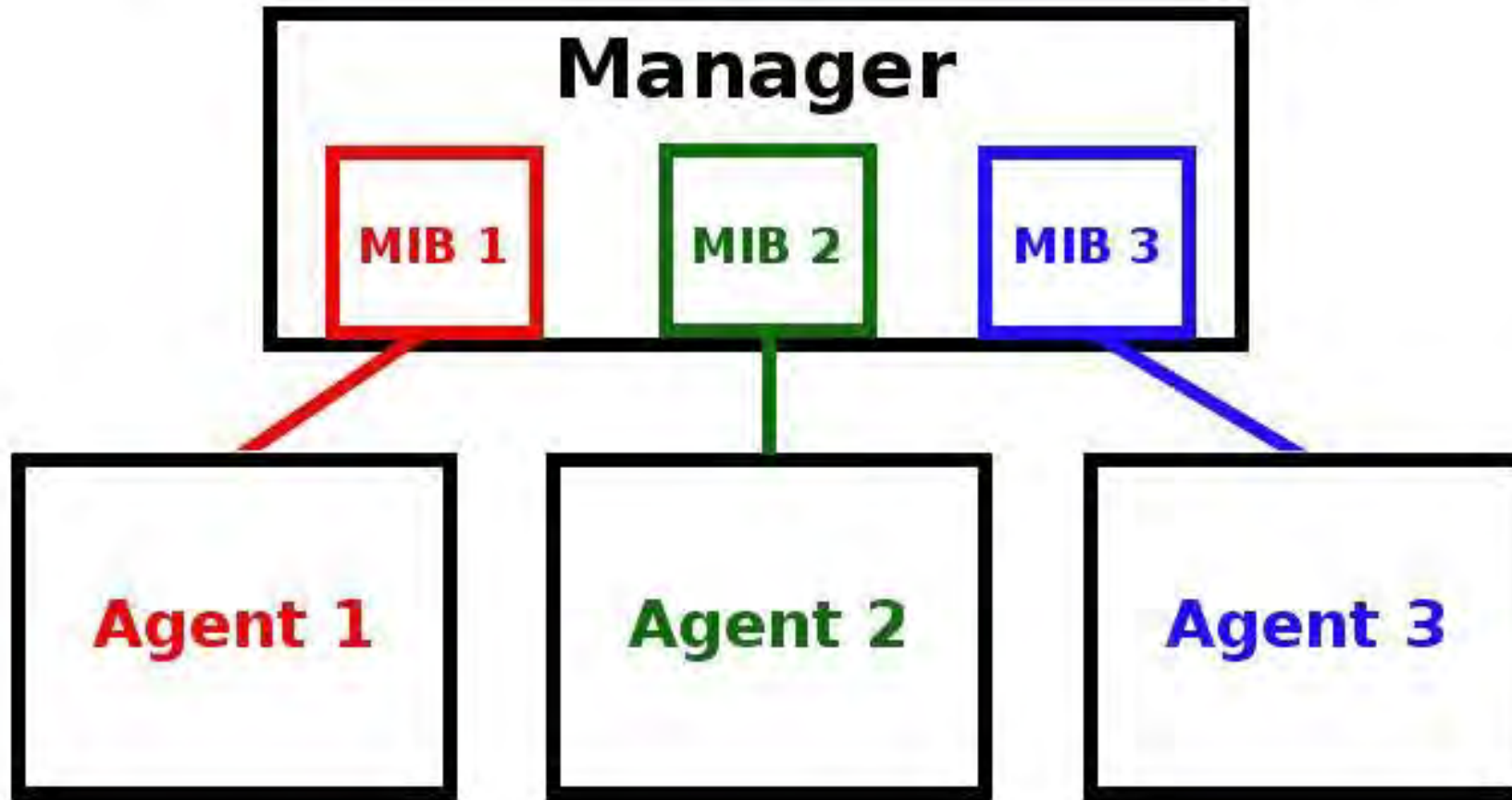
An agent might use multiple MIBs to monitor one device

Most SNMP managers have MIBs already installed

- Vendor-neutral MIBs
- Vendor-specific MIBs for popular products

You might have to install additional MIBs into the manager to query all functions

SNMP MIBs and Agents



MIB Hierarchy

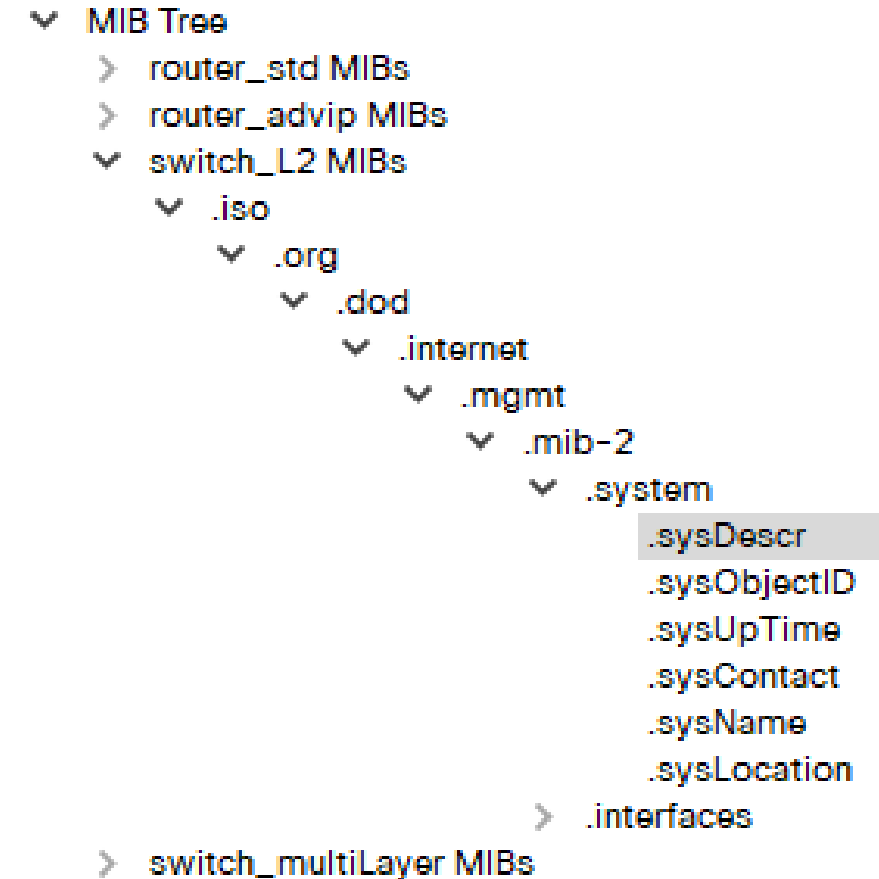
All OIDs, regardless of manufacturer, are part of a global hierarchy

Each OID is unique

The SNMP manager must know what MIBs the agent is using

- At least know a starting OID to query
- The manager can then repeatedly issue a “get-next” command
- The agent will provide information about successive OIDs
- The manager does not need to OIDs for every single counter on the device

SNMP MIBs



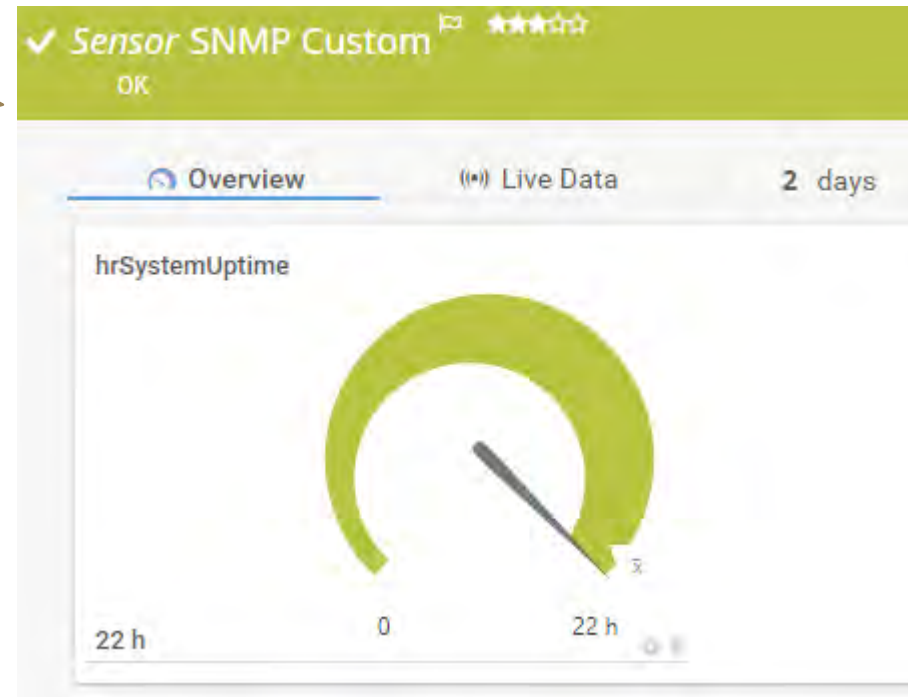
SNMP Get Example

Example: Ask the system for its uptime status

NMS: "Get 1.3.6.1.2.1.25.1.1.0"

Agent: "22 hours"

Agent response
might look
something like
this in NMS
console



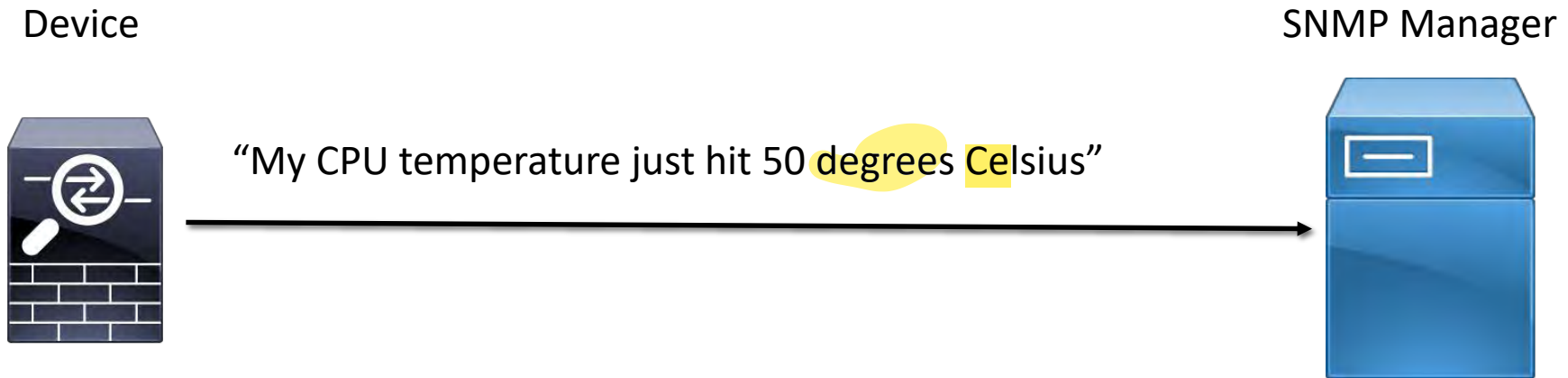
SNMP Trap

An alert sent from the agent to the manager when an event happens

Sent immediately

- The device does not wait for the manager to poll for the information

Admin must enable and configure



Command Line SNMP Monitoring

snmpget

- Query a single OID

snmpwalk

- Query an entire MIB starting from a particular OID

Same syntax for both



snmpget [options] [community string] [host name/address] [OID]

```
$ snmpget -v 2c 127.0.0.1 -c public .1.3.6.1.2.1.1.5.0
SNMPv2-MIB::sysName.0 = STRING: centos7

$ snmpget -v 2c 127.0.0.1 -c public sysName.0
SNMPv2-MIB::sysName.0 = STRING: centos7
```



NetFlow



What is NetFlow?

A network device feature first introduced by Cisco

Provides the ability to collect IP network traffic as it enters or exits an interface

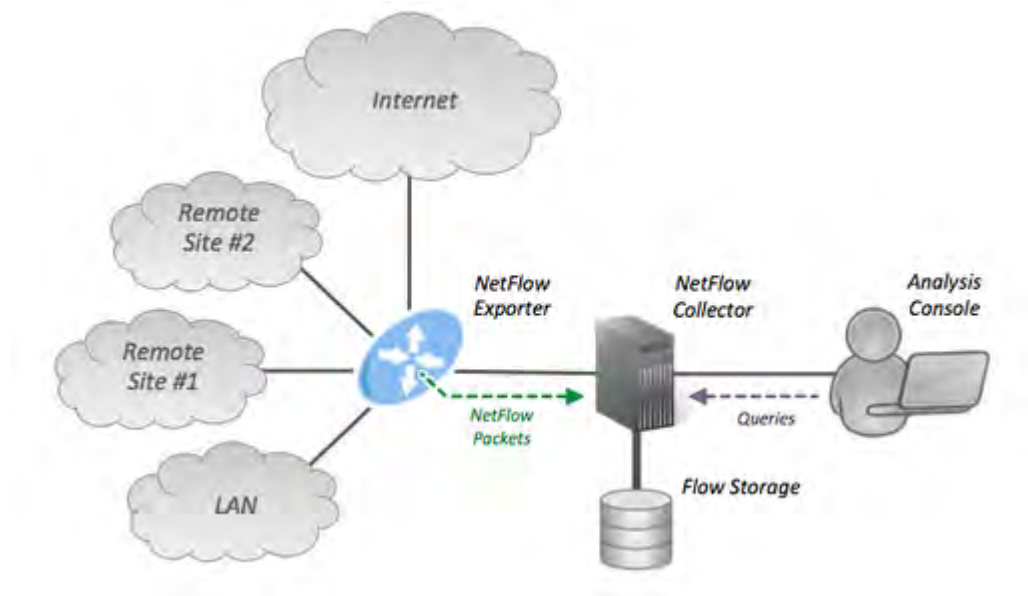
Provides insight into bandwidth usage

Three main components:

- Flow exporter
- Flow collector
- Analysis application

NetFlow v9 is the basis of an IETF standard

Other vendors have similar offerings



Flow According to Cisco

Cisco defines a *flow* as a unidirectional sequence of packets that share the same seven values:

1. Ingress interface (SNMP ifIndex)
2. Source IP address
3. Destination IP address
4. IP protocol
5. Source port for UDP or TCP, 0 for other protocols
6. Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols
7. IP Type of Service

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	
Flows								
2010-09-01 00:00:00.459	0.000	UDP	127.0.0.1:24920	->	192.168.0.1:22126	1	46	1
2010-09-01 00:00:00.363	0.000	UDP	192.168.0.1:22126	->	127.0.0.1:24920	1	80	1

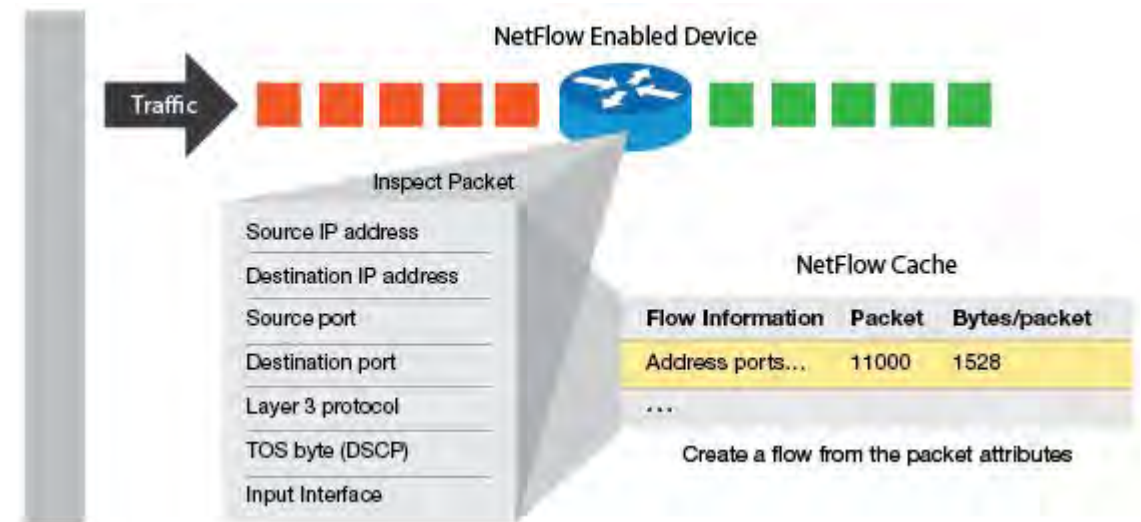
Uses for NetFlow Data

Provides an understanding of:

- Where network traffic data is coming from and going to
- How much traffic is being generated
- Who is consuming most bandwidth

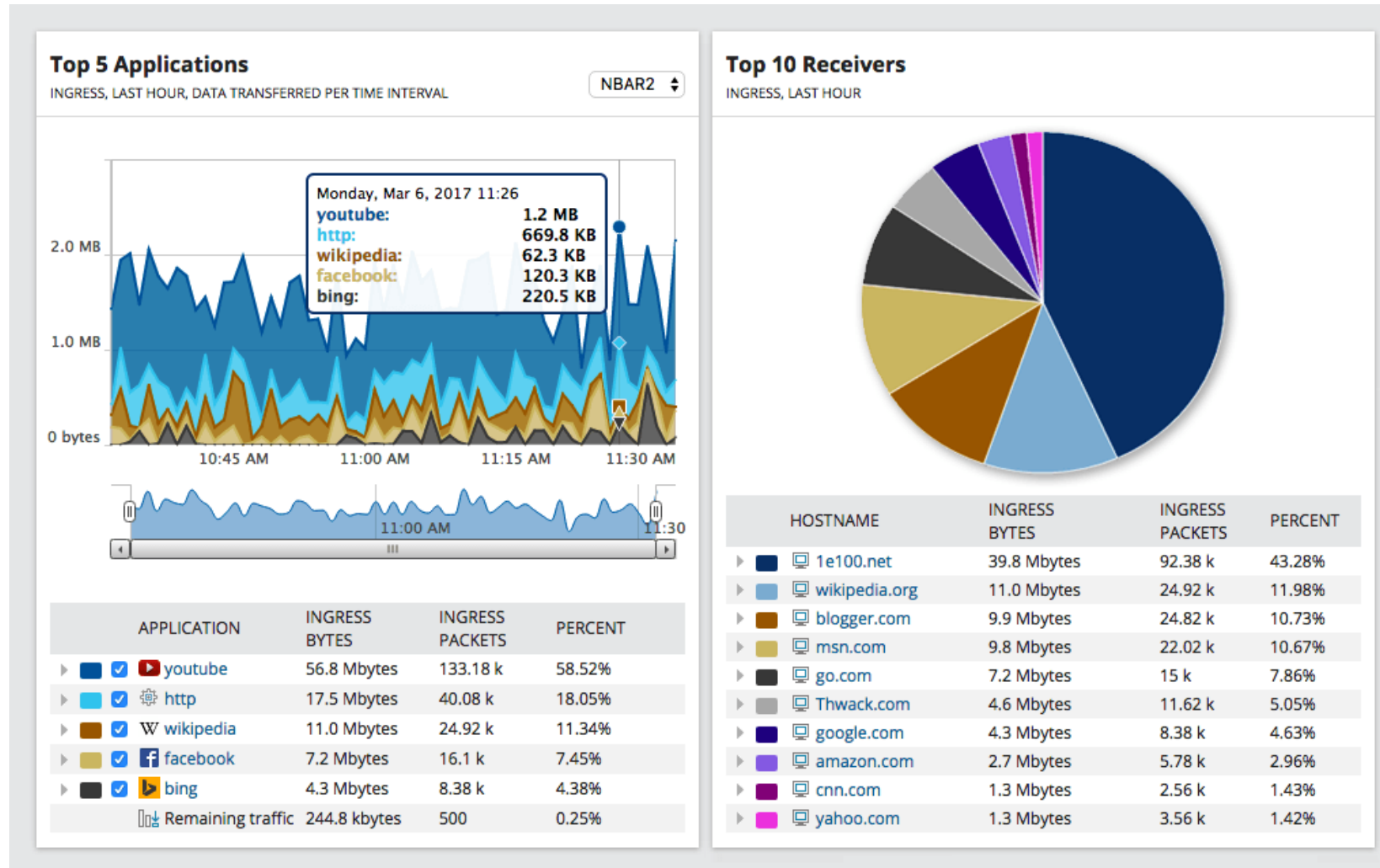
Can be used for:

- Anomaly detection
- Monitoring bandwidth usage
- Capacity planning
- Validating effectiveness of QoS policy



NetFlow Traffic Analysis Example

Jason





Network Security Monitoring



Port Scanning

Probe a server/device for open ports

An open port implies a listening (and possibly vulnerable) service behind it

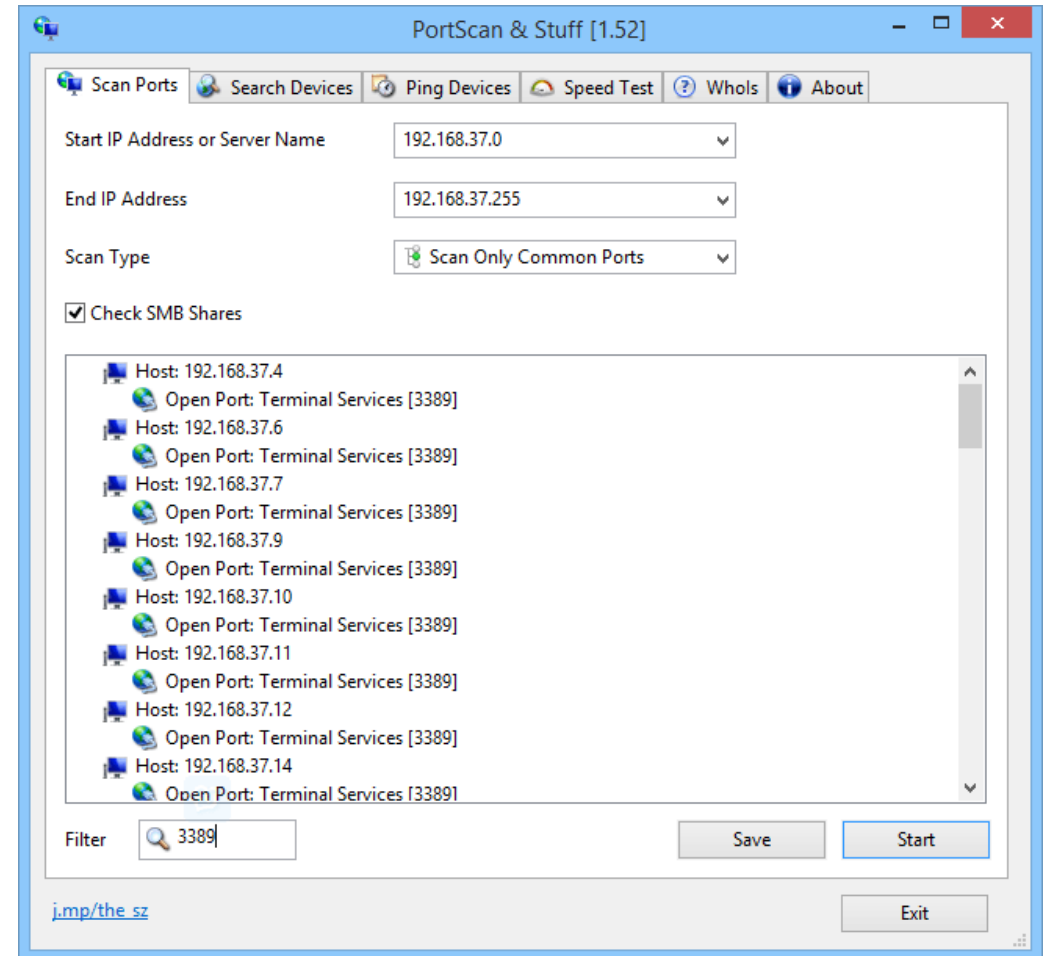
- It can also reveal a maliciously placed back door

Port scanning will help you identify and stop unauthorized or vulnerable processes that use the network

A port scan will report a port as:

- Open
- Closed
- Filtered (status unknown due to firewall)

You can correlate findings on a computer by using the `netstat` command-line utility



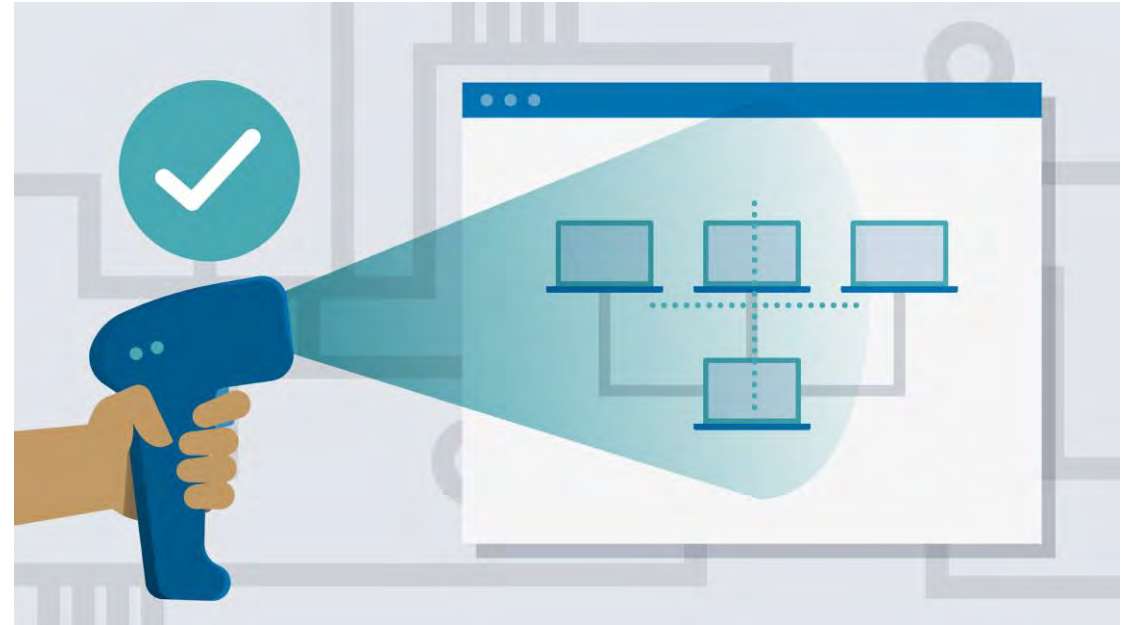
Vulnerability Scanning

Detect weaknesses on devices attached to the network

Scan computers, storage, network devices and communication devices

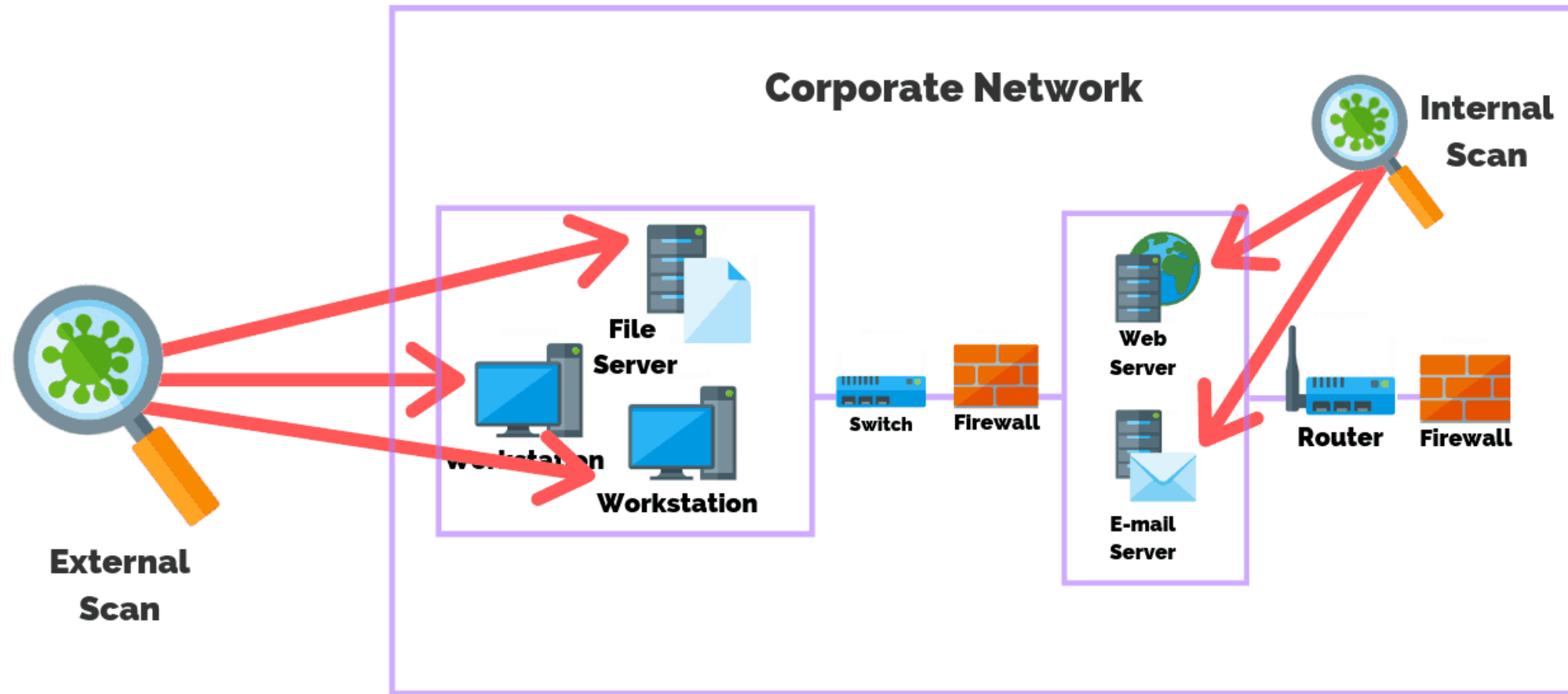
Can measure the effectiveness of countermeasures that are implemented

Can be performed regularly by the IT team as part of routine security monitoring

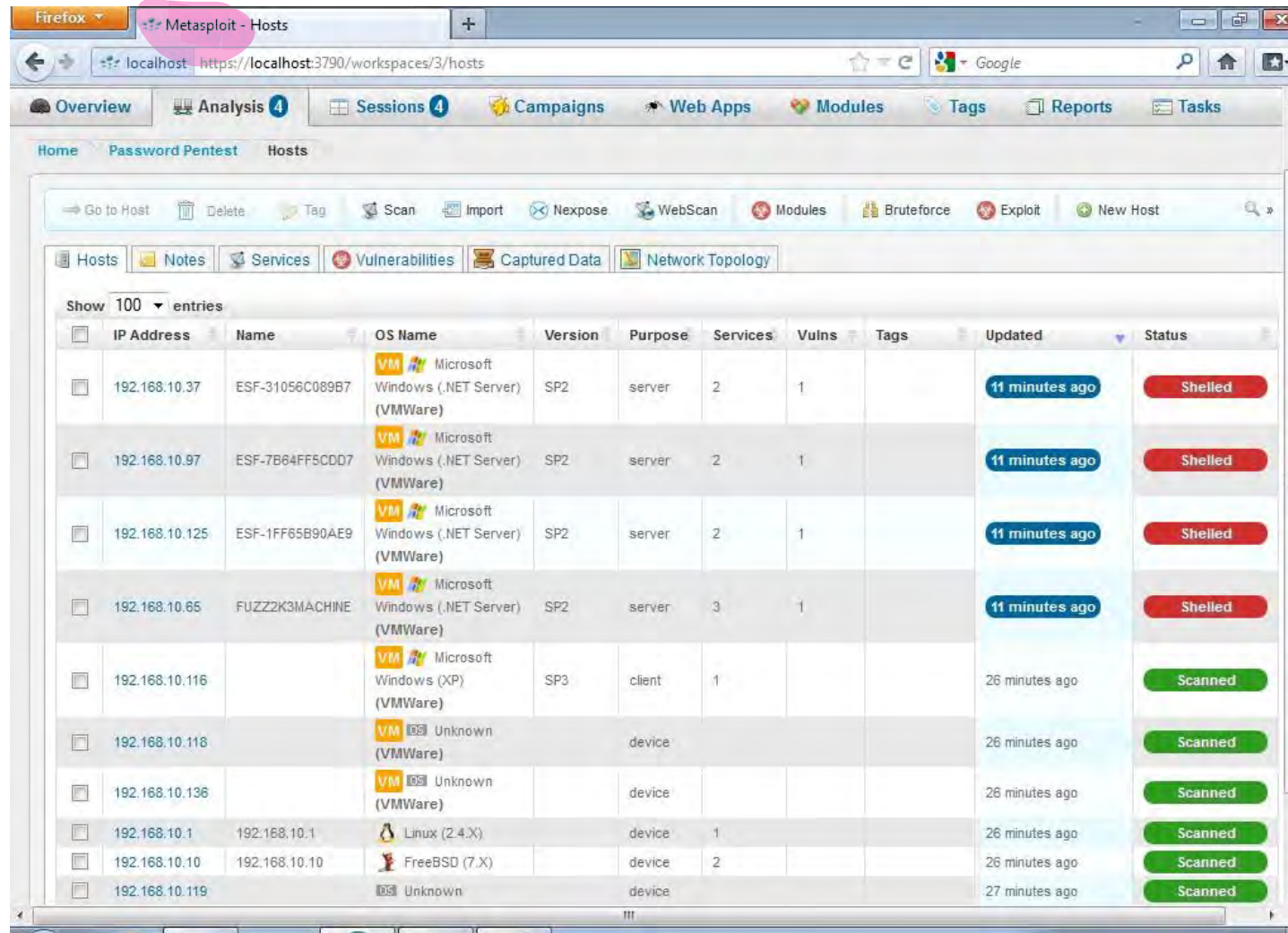


Note: Do not confuse a vulnerability scan with a penetration test. A vulnerability scan searches for weaknesses that may or may not be exploitable. A penetration test involves actively breaking into a network.

Vulnerability Scanning Example



Vulnerability Scan Output Example



The screenshot shows the Metasploit web interface in a Firefox browser. The address bar displays `https://localhost:3790/workspaces/3/hosts`. The interface includes a top navigation bar with tabs for Overview, Analysis (4), Sessions (4), Campaigns, Web Apps, Modules, Tags, Reports, and Tasks. Below this is a sub-navigation bar with Home, Password Pentest, and Hosts. A toolbar contains icons for Go to Host, Delete, Tag, Scan, Import, Nexpose, WebScan, Modules, Bruteforce, Exploit, and New Host. The main content area shows a list of hosts with columns for IP Address, Name, OS Name, Version, Purpose, Services, Vulns, Tags, Updated, and Status. The 'Hosts' tab is selected, and the table displays 100 entries. The first four hosts are marked as 'Shelled' and were updated 11 minutes ago. The remaining six hosts are marked as 'Scanned' and were updated 26 or 27 minutes ago.

IP Address	Name	OS Name	Version	Purpose	Services	Vulns	Tags	Updated	Status
192.168.10.37	ESF-31056C089B7	Microsoft Windows (.NET Server) (VMWare)	SP2	server	2	1		11 minutes ago	Shelled
192.168.10.97	ESF-7B64FF5CDD7	Microsoft Windows (.NET Server) (VMWare)	SP2	server	2	1		11 minutes ago	Shelled
192.168.10.125	ESF-1FF65B90AE9	Microsoft Windows (.NET Server) (VMWare)	SP2	server	2	1		11 minutes ago	Shelled
192.168.10.65	FUZZ2K3MACHINE	Microsoft Windows (.NET Server) (VMWare)	SP2	server	3	1		11 minutes ago	Shelled
192.168.10.116		Microsoft Windows (XP) (VMWare)	SP3	client	1			26 minutes ago	Scanned
192.168.10.118		Unknown (VMWare)		device				26 minutes ago	Scanned
192.168.10.136		Unknown (VMWare)		device				26 minutes ago	Scanned
192.168.10.1	192.168.10.1	Linux (2.4.X)		device	1			26 minutes ago	Scanned
192.168.10.10	192.168.10.10	FreeBSD (7.X)		device	2			26 minutes ago	Scanned
192.168.10.119		Unknown		device				27 minutes ago	Scanned

Patch Management Monitoring

A patch is a software update provided by the manufacturer

Patches can be used to improve performance, add functionality, or remediate security vulnerabilities

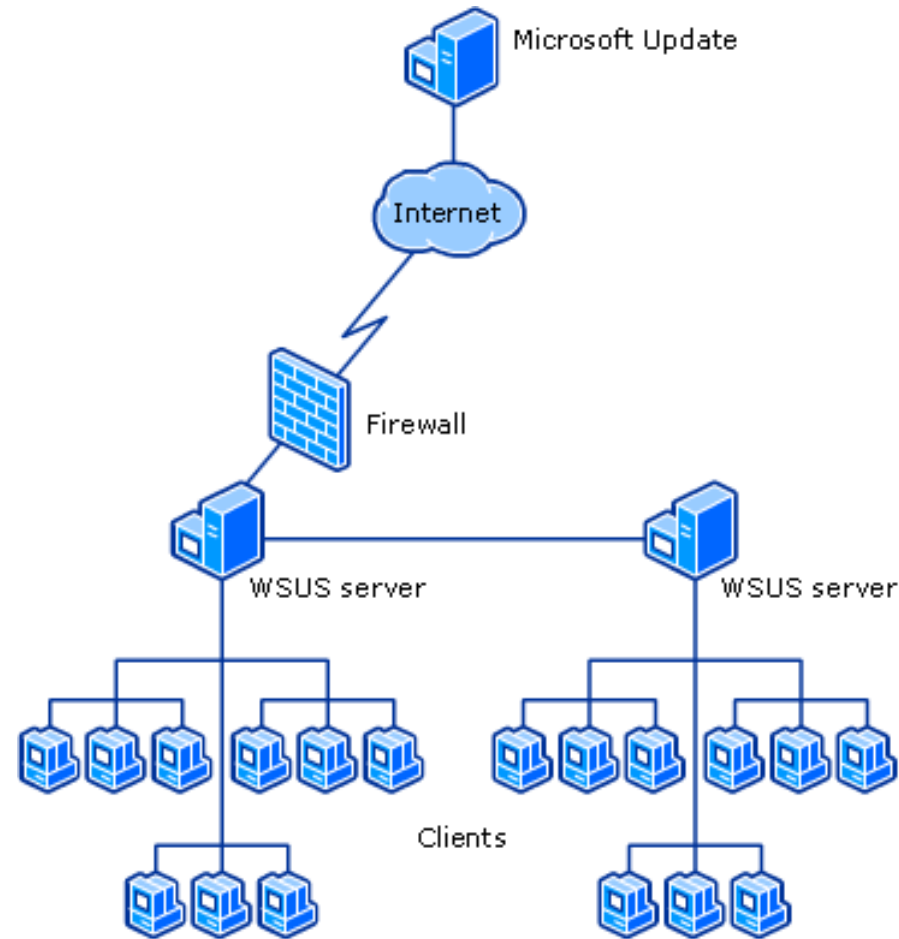
Patch management refers to a complete system for downloading, testing, and deploying patches to devices on the network

Patch management includes:

- Maintaining current knowledge of available patches
- Deciding what patches are needed for which systems
- Testing, approving and automatically deploying patches in a controlled manner
- Testing systems after installation
- Documenting procedures and configurations



Typical Patch Management Architecture



Patch Management Example

The screenshot displays the Patch Manager console interface. On the left is a navigation tree with the following structure:

- Patch Manager (pm-aus-wspm-01)
 - Enterprise
 - Update Services
 - PM-AUS-WSUS-01
 - Updates
 - All Updates (selected)
 - Critical Updates
 - Security Updates
 - Definition Updates
 - Last Month
 - Microsoft Updates - This Week
 - Service Packs
 - Third Party Updates
 - Update Rollups
 - Computers and Groups
 - Configuration Manager Site Servers
 - Microsoft Windows Network
 - Managed Computers
 - Agents
 - Administration and Reporting
 - Software Publishing
 - All Packages
 - Adobe Packages
 - Adobe Systems, Inc. Packages
 - Apple Packages
 - Citrix Packages
 - Dell Packages
 - Foxit Corporation Packages
 - Google Packages
 - Malwarebytes Packages

The main pane shows the 'All Updates' view. At the top, it indicates 'Approval State: (Any Approval State) Update State: (Failed or Needed) Last Refresh: 5/8/2015 8:48:03 AM'. Below this, filters are set to 'Approval: All', 'Status: Failed or Needed', and 'Classifications: All Classifications'. A summary line shows '(215) of 12180 total updates shown (55) Approved (45) Security Updates (6) Critical Updates Last Refresh: 5/8/2015 8:48:03 AM (1) selected'. A message says 'Drag a column header here to group by that column.'.

The update list table has the following columns: Title, Classification, Arrival Date, Approval, Declined, and Status. The selected update is:

Title	Classification	Arrival Date	Approval	Declined	Status
Windows Server Update Services 3.0 SP2 Dyn...	Updates	10/6/2014 3:30:25...	Approved	No	Ready
Update for Windows Server 2008 R2 x64 Editio...	Updates	10/6/2014 4:44:56...	Approved	No	Ready
Update for Windows Server 2008 R2 x64 Editio...	Updates	10/6/2014 4:55:23...	Not approved	No	Files
Update for Windows Server 2008 R2 x64 Editio...	Updates	10/6/2014 5:01:22...	Not approved	No	Files
Security Update for Windows Server 2008 R2 x...	Security Updates	10/6/2014 5:05:19...	Approved	No	Ready
Security Update for Microsoft .NET Framework...	Security Updates	10/6/2014			
Security Update for Microsoft .NET Framework...	Security Updates	10/6/2014			
Update for Windows Server 2008 R2 x64 Editio...	Updates	10/6/2014			

A context menu is open over the selected update, showing options: Filter, Choose Columns, Save View Layout, Export, Update Management, **Update Management Wizard** (highlighted), New Update List Template, Update List Management, Approve, Decline, Decline (scheduled with rules), Delete, Delete (scheduled with rules), and Expire.

Below the table, the 'Update Details' tab is active. It features a 'Computers Summary' section with a pie chart and the following data:

- Computers installed: 0
- Computers pending reboot: 0
- Computers with errors: 0
- Computers downloaded: 1
- Computers needing: 0
- Computers not applicable: 7
- Computers with no status: 0

The 'Description' section reads: **Security Update for Windows Server 2008 R2 x64 Edition (KB2912390)**. Below this, a paragraph states: 'A security issue has been identified in a Microsoft software product that could affect your system. You should install this update as soon as possible. For a complete listing of the issues that are included in this update, see the associated update, you may have to restart your system.'

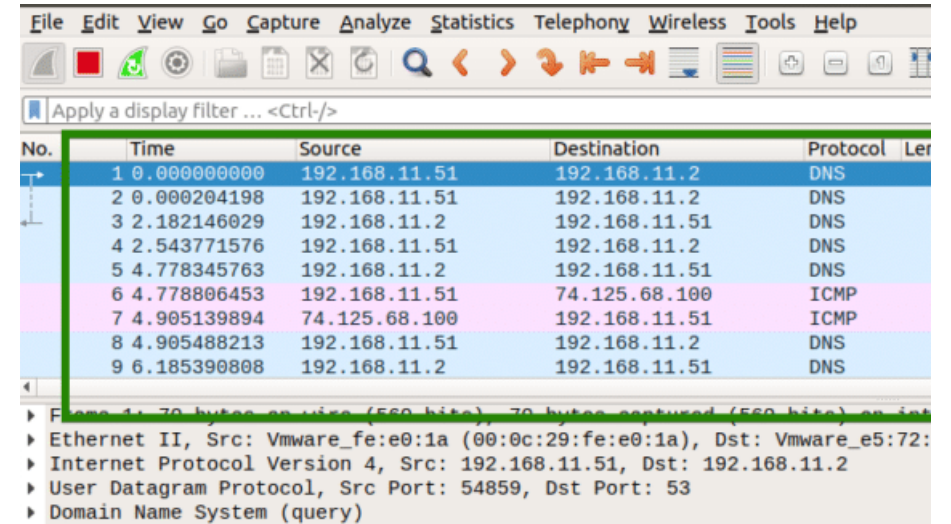
The 'More Information' section provides a link: <http://support.microsoft.com/kb/2912390>.

Packet/Traffic Analysis

Intercept and examine messages in transit

- Uses a protocol analyzer/sniffer
- Recreate entire conversations / transferred files
- Get statistics on IP, protocol and port usage
- See details of suspicious communications
- Can be performed (in a limited way) on encrypted traffic

A basic component of IDS/IPS



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table is highlighted with a green border and contains the following data:

No.	Time	Source	Destination	Protocol	Length
1	0.000000000	192.168.11.51	192.168.11.2	DNS	
2	0.000204198	192.168.11.51	192.168.11.2	DNS	
3	2.182146029	192.168.11.2	192.168.11.51	DNS	
4	2.543771576	192.168.11.51	192.168.11.2	DNS	
5	4.778345763	192.168.11.2	192.168.11.51	DNS	
6	4.778806453	192.168.11.51	74.125.68.100	ICMP	
7	4.905139894	74.125.68.100	192.168.11.51	ICMP	
8	4.905488213	192.168.11.51	192.168.11.2	DNS	
9	6.185390808	192.168.11.2	192.168.11.51	DNS	

Below the table, the packet details pane shows the expanded view of packet 1 (DNS query):

- Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
- Ethernet II, Src: Vmware_fe:e0:1a (00:0c:29:fe:e0:1a), Dst: Vmware_e5:72:1a (00:0c:29:e5:72:1a)
- Internet Protocol Version 4, Src: 192.168.11.51, Dst: 192.168.11.2
- User Datagram Protocol, Src Port: 54859, Dst Port: 53
- Domain Name System (query)

```
0000  00 50 56 e5 72 96 00 0c 29 fe e0 1a 08 00 45 00  .PV.r... )....E.
0010  00 38 c7 6c 40 00 40 11 db c2 c0 a8 0b 33 c0 a8  .8.l@.@. ....3..
0020  0b 02 d6 4b 00 35 00 24 97 bb ba d8 01 00 00 01  ...K.5.$ .....
0030  00 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f  ....g oogle.co
0040  6d 00 00 01 00 01                                     m.....
```

NIDS / NIPS

Network-based Intrusion Detection System (NIDS)

- Device or software that monitors the network for malicious activity or policy violations
- Uses strategically-placed sensors to monitor network traffic in key locations
- Compares traffic to a database of known malicious signatures
- Logs detected malicious patterns
- Can be configured to alert the administrator

Network-based Intrusion Prevention System (NIPS)

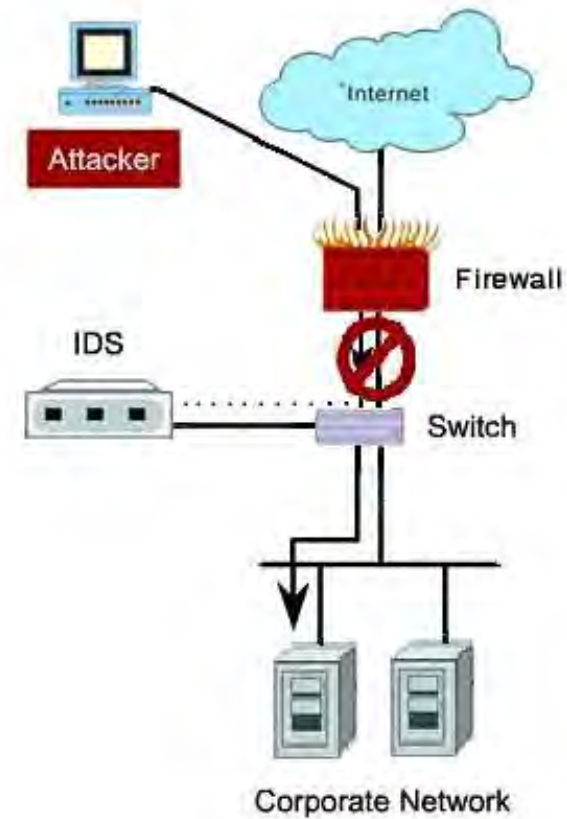
- A NIDS that uses a baseline of “good” traffic to detect anomalies
- Tells the firewall to block suspicious traffic in realtime

IDS vs IPS

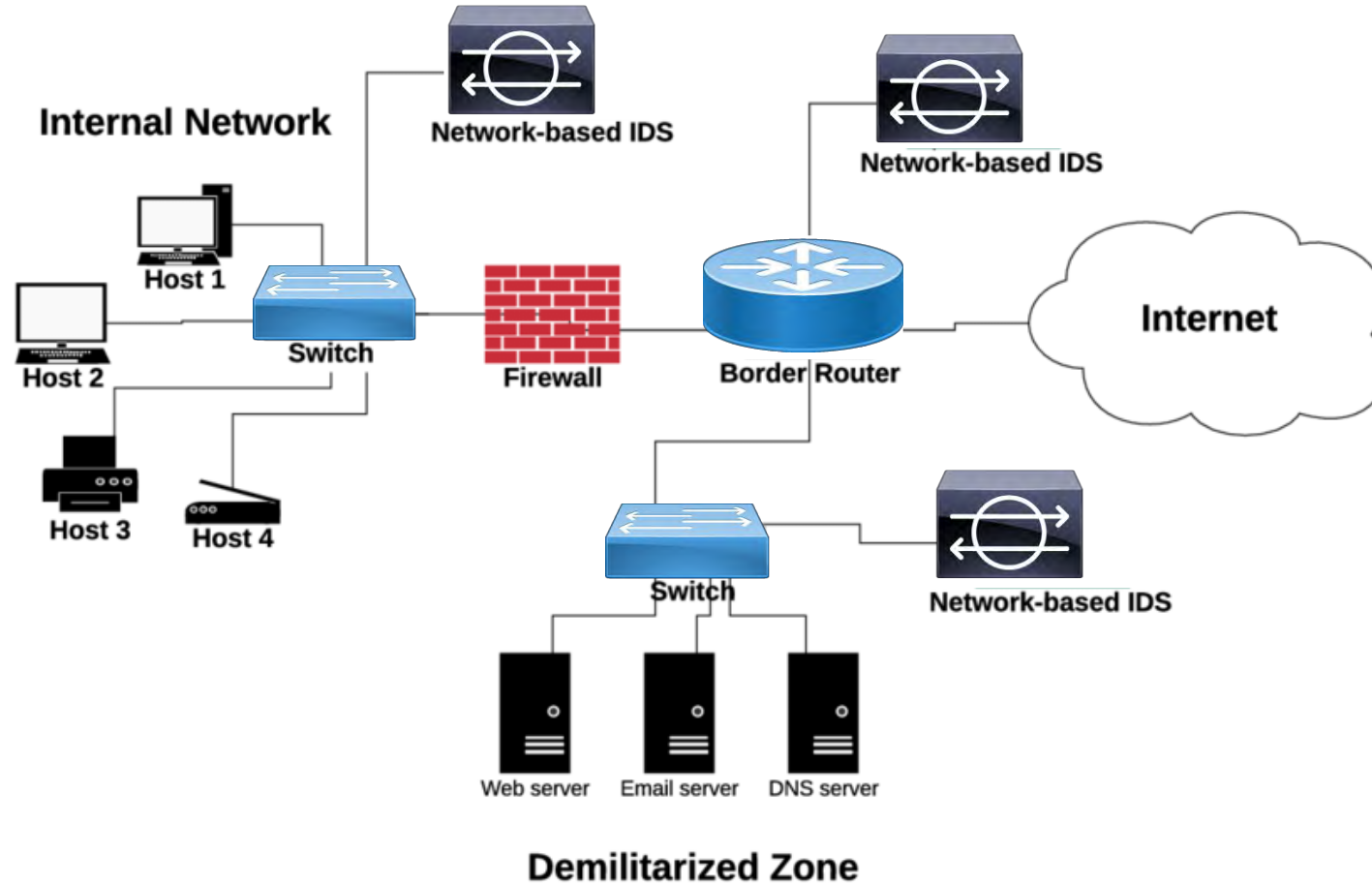
Intrusion Detection System



Intrusion Prevention System



NIDS Placement Example



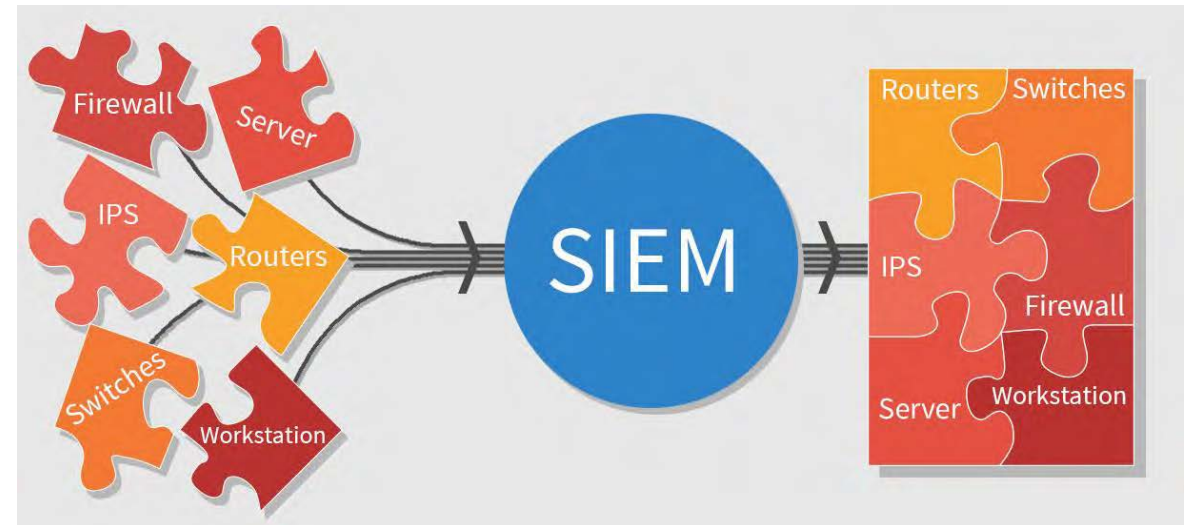
Security Information and Event Management (SIEM)

Provides the enterprise with:

- Threat monitoring
- Event correlation
- Incident response
- Reporting

Collects, centralizes, and analyzes log data from applications, servers, and network devices

- Correlates events over hours or days
- Compares events to a baseline
- Can alert you if specific events occur or a threshold is exceeded



Artificial Intelligence for IT Operations (AIOps)

AI and machine learning-based algorithms couple with predictive analytics

- A core component of SIEM platforms
- Provides SIEM with long-term, deep learning capabilities

Can adjust the infrastructure baseline and alerting thresholds over time

- Incorporates threat intelligence feeds from other sources
- Uses Big Data to detect very slow or stealth activities that traditional SIEM would miss
- Can replace repetitive, redundant tasks with automated workflows
- Typically a cloud-based service

