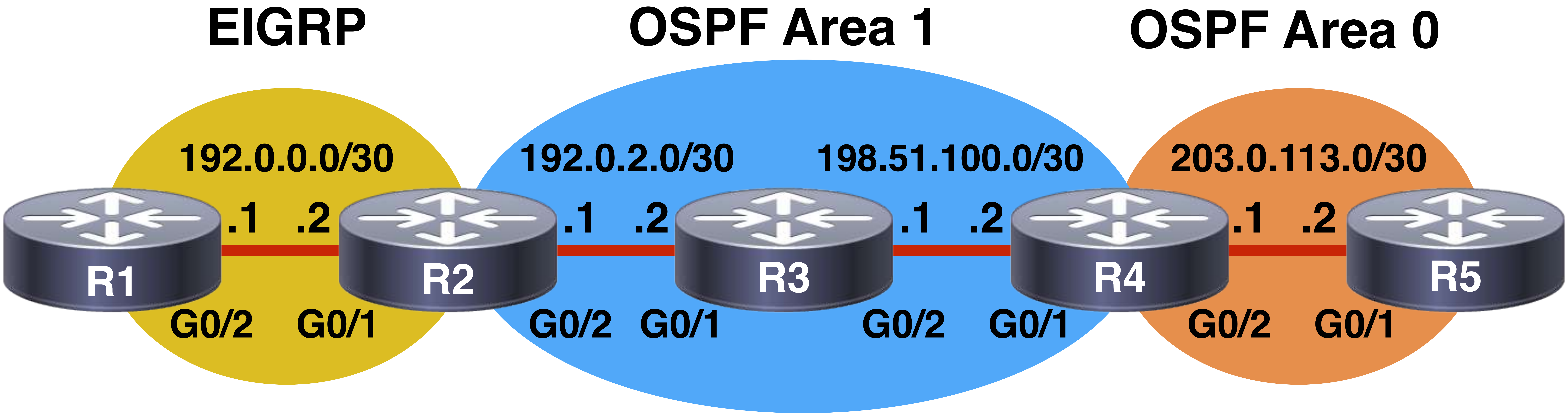
Module 4
Network Management

Command Line Utilities

The debug, traceroute, and ping Commands



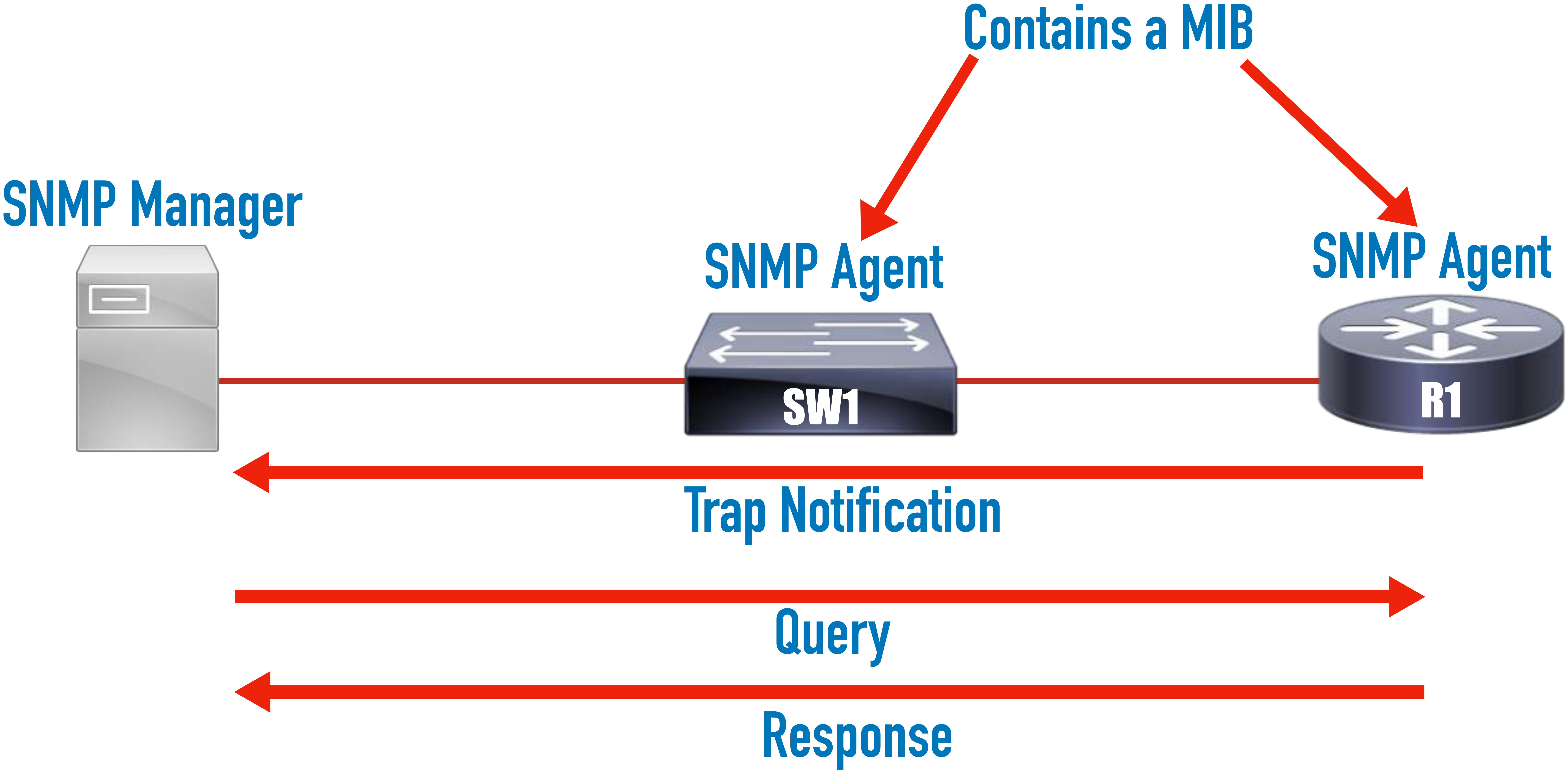
traceroute Codes

CODE	DESCRIPTION
*	Timed out
A	Administratively Prohibited (e.g. ACL)
Q	Source Quench (Destination Too Busy)
I	User Interrupted Test
U	Port Unreachable
H	Host Unreachable
N	Network Unreachable
P	Protocol Unreachable
T	Timeout
?	Unknown Packet Type

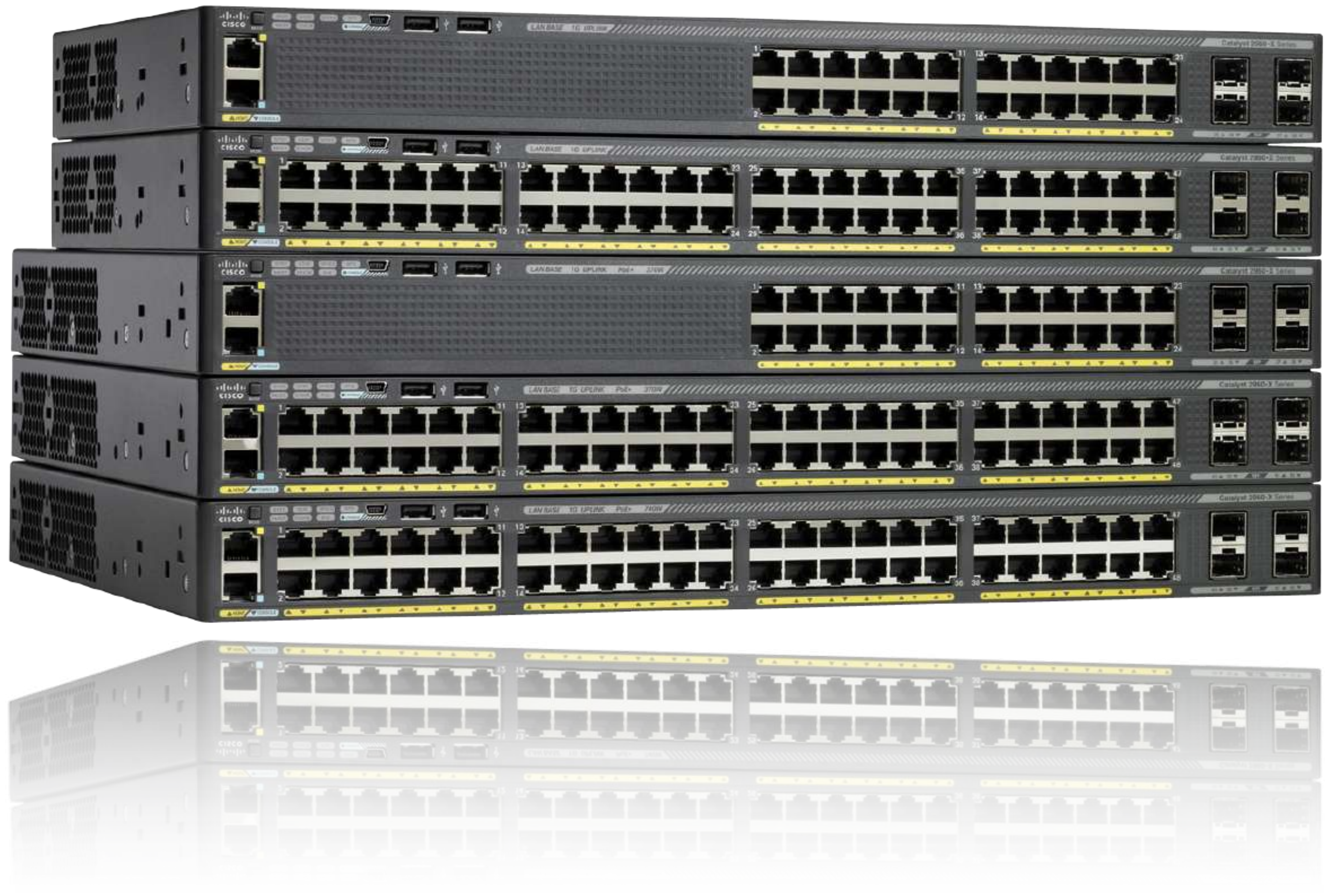
CLI Command Demos

SNMP

Simple Network Management Protocol (SNMP) Operation



SNMP Security Options



Version	Security
1	Community Strings
2c	Community Strings
3	Encryption, Integrity Checking, and Authentication Services

SNMP Demos

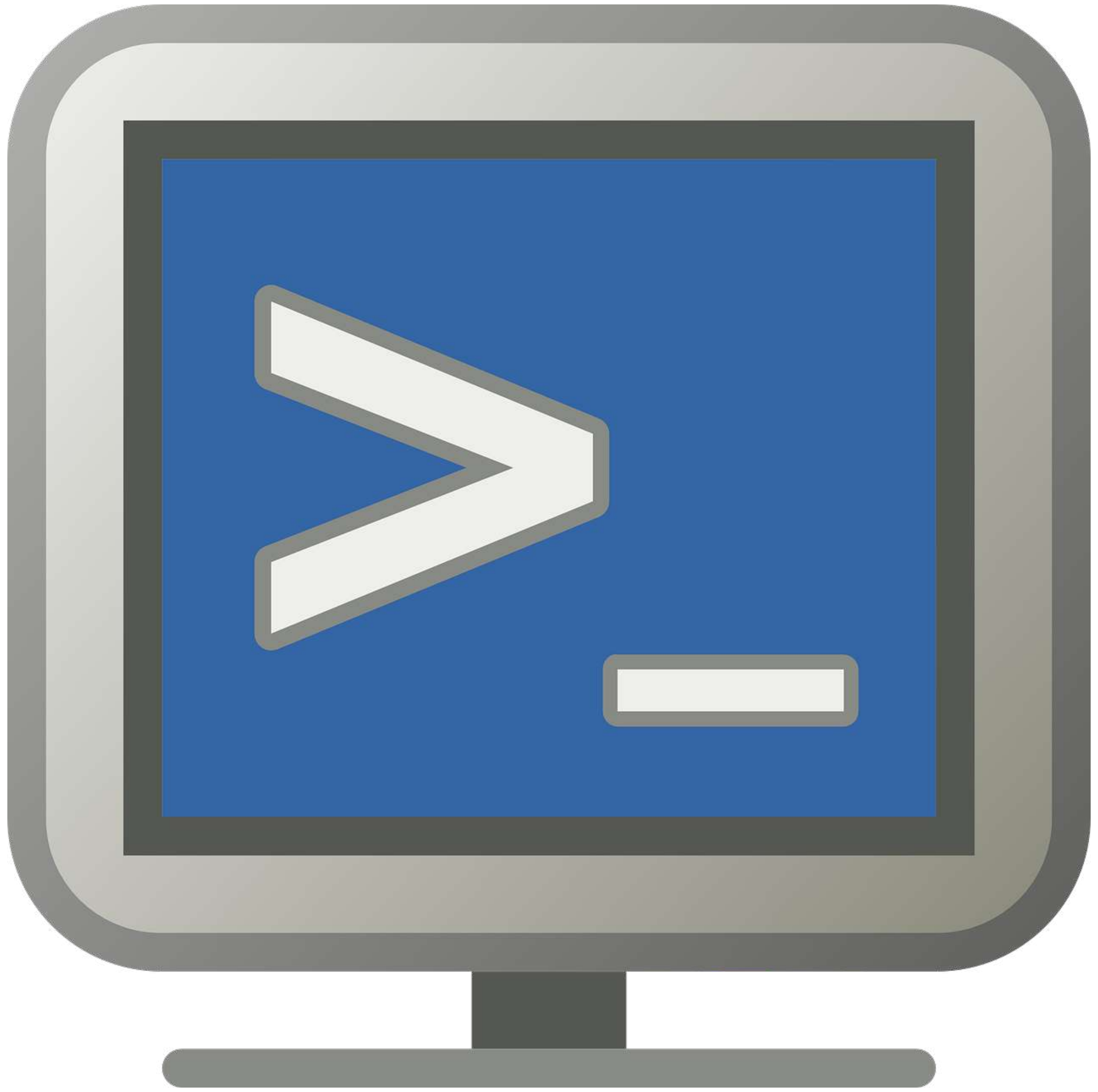
Syslog

Syslog Theory

Syslog Theory

Syslog:

- Standardized in RFC 5424
- Widely supported on most OS platforms
- Centralized servers are ideal for enterprise networks
- Centralized tools provide event correlation



Syslog Theory

Syslog:

- Standardized in RFC 5424
- most OS p
- re ideal for
- vide event c

Syslog Theory

Code	Severity	Description
0	Emergency	System is unstable
1	Alert	Immediate action needed
2	Critical	Critical conditions exist
3	Error	Error conditions exist
4	Warning	Warning conditions exist
5	Notice	Normal but significant conditions
6	Informational	Informational messages
7	Debug	Debug-level messages

Syslog Theory

Number	Facility Description
0	Kernel message
1	User-level message
2	Mail system
3	System daemons
4	Security messages
5	Syslogd messages
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem

Number	Facility Description
9	Clock daemon
10	Authorization messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Clock daemon
16 - 23	Local use

Syslog Theory

```
<100>1 2019-12-06-02T10:53:23.001Z ubuntu-server apache 200-20031 - “The Apache Server has encountered an error.”
```

🟨 **PRI**: Priority value - contains facility and severity codes

🟩 **Header**: Timestamp and hostname from generating device

🟪 **Message**: Tag containing application and process ID, and the contents of the message output

Syslog Demo

NetFlow

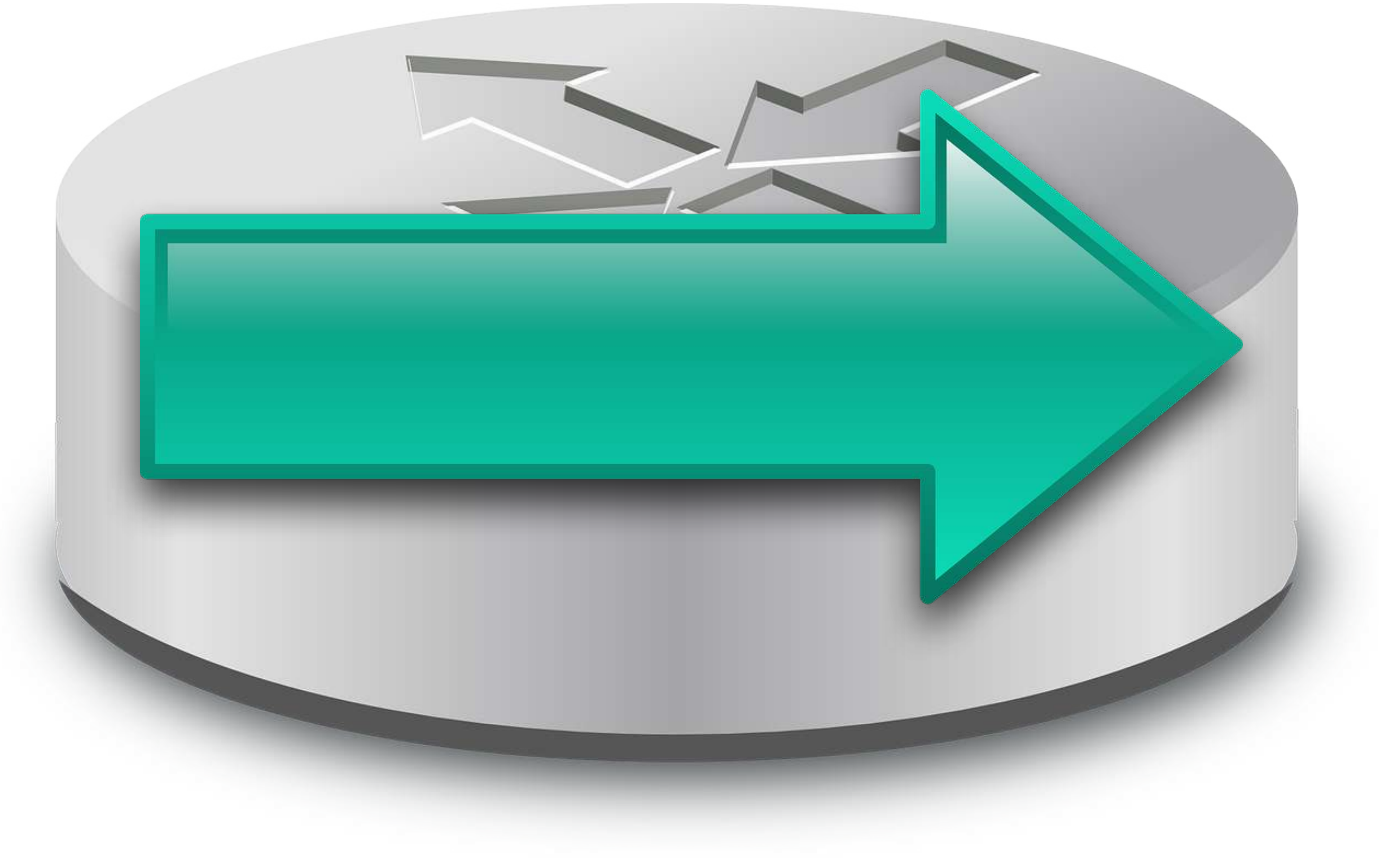
NetFlow Theory

NetFlow:

- Collects IP traffic information

Helps identify:

- Network traffic bottleneck areas
- Effects of policy changes and new applications
- Unauthorized/problematic traffic
- Security vulnerabilities and anomalies



NetFlow Theory

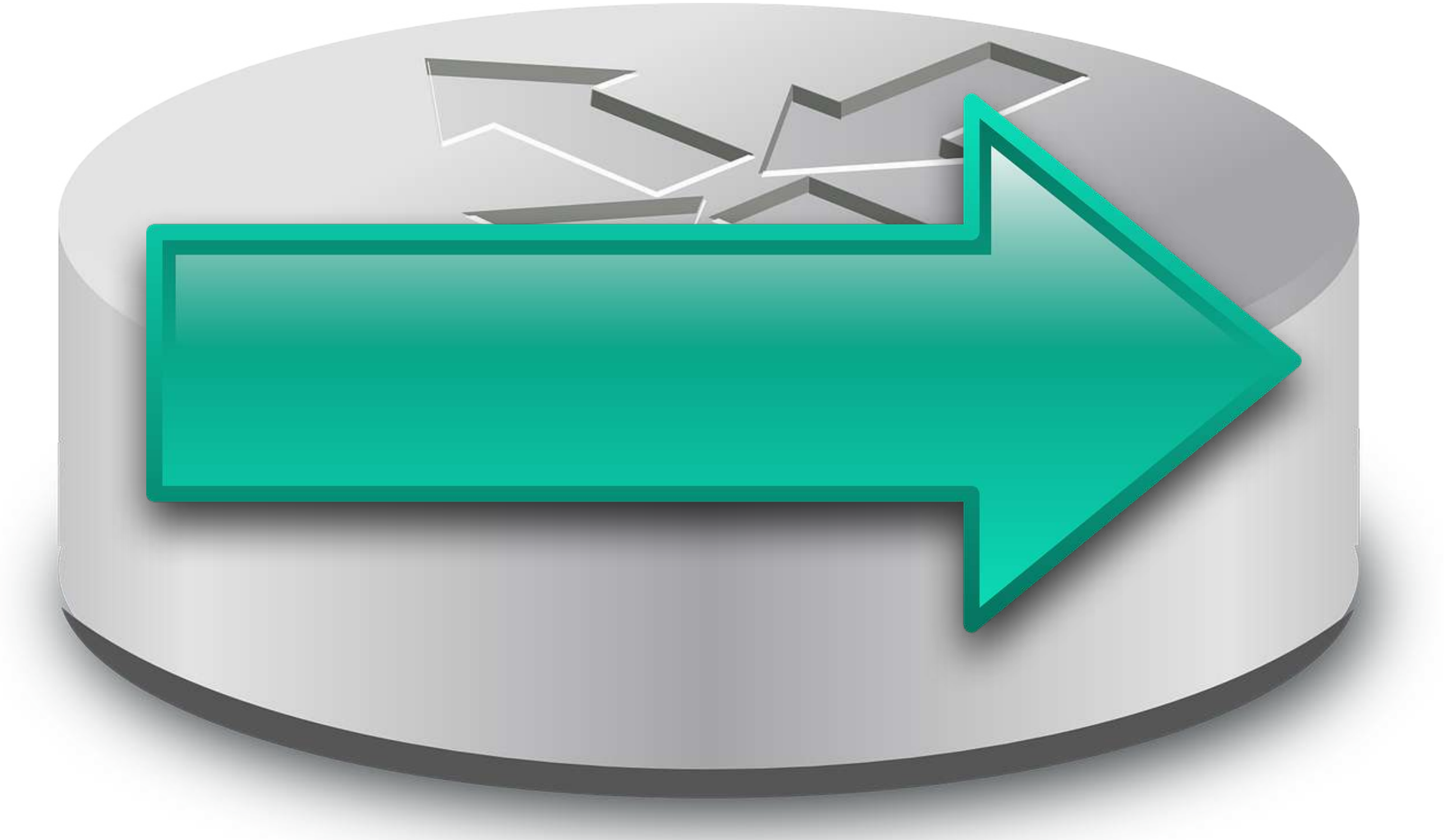
- Packet “fingerprints” collected by NetFlow
- Similar packets are grouped together into a flow record

NetFlow Theory

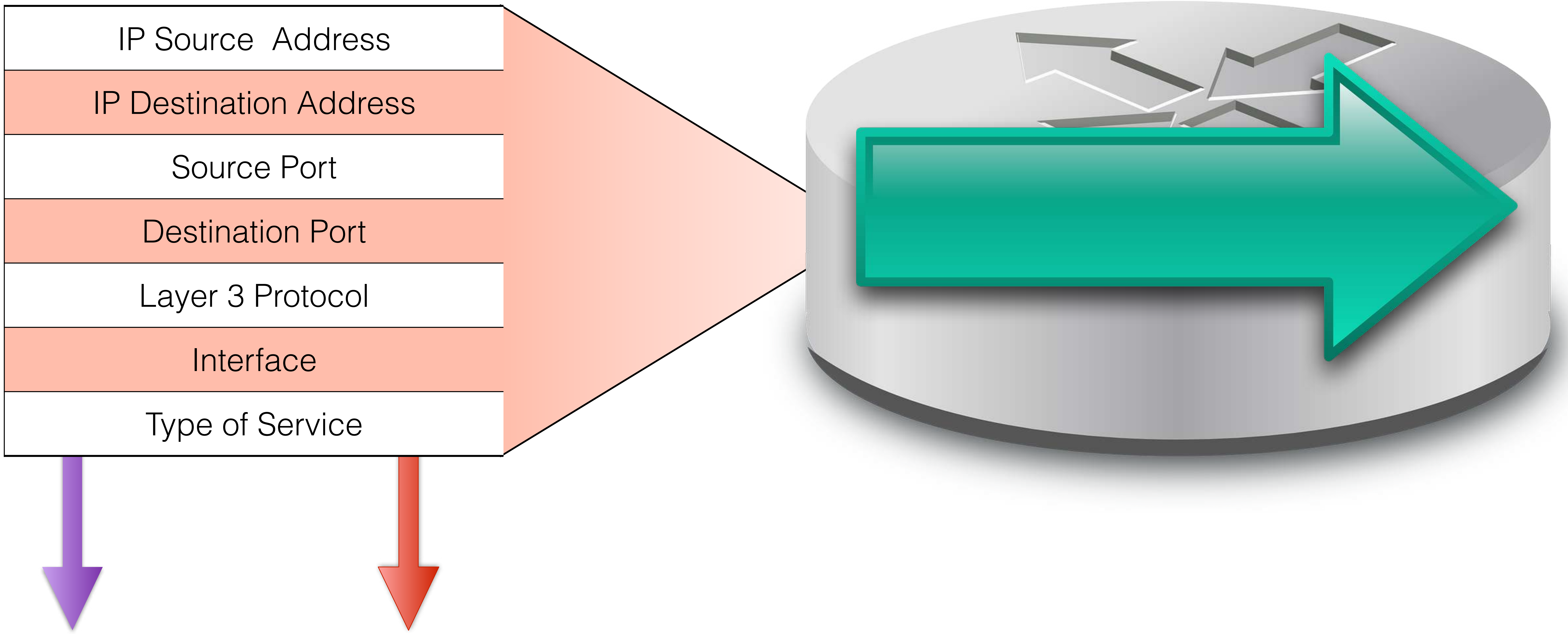
NetFlow Cache:

- IP source and destination address
- Source and destination port
- Layer 3 protocol type
- Router or switch interface
- Type of Service (ToS)

- Capture can happen on ingress and/or egress



NetFlow Theory



IP Source Address

IP Destination Address

Source Port

Destination Port

Layer 3 Protocol

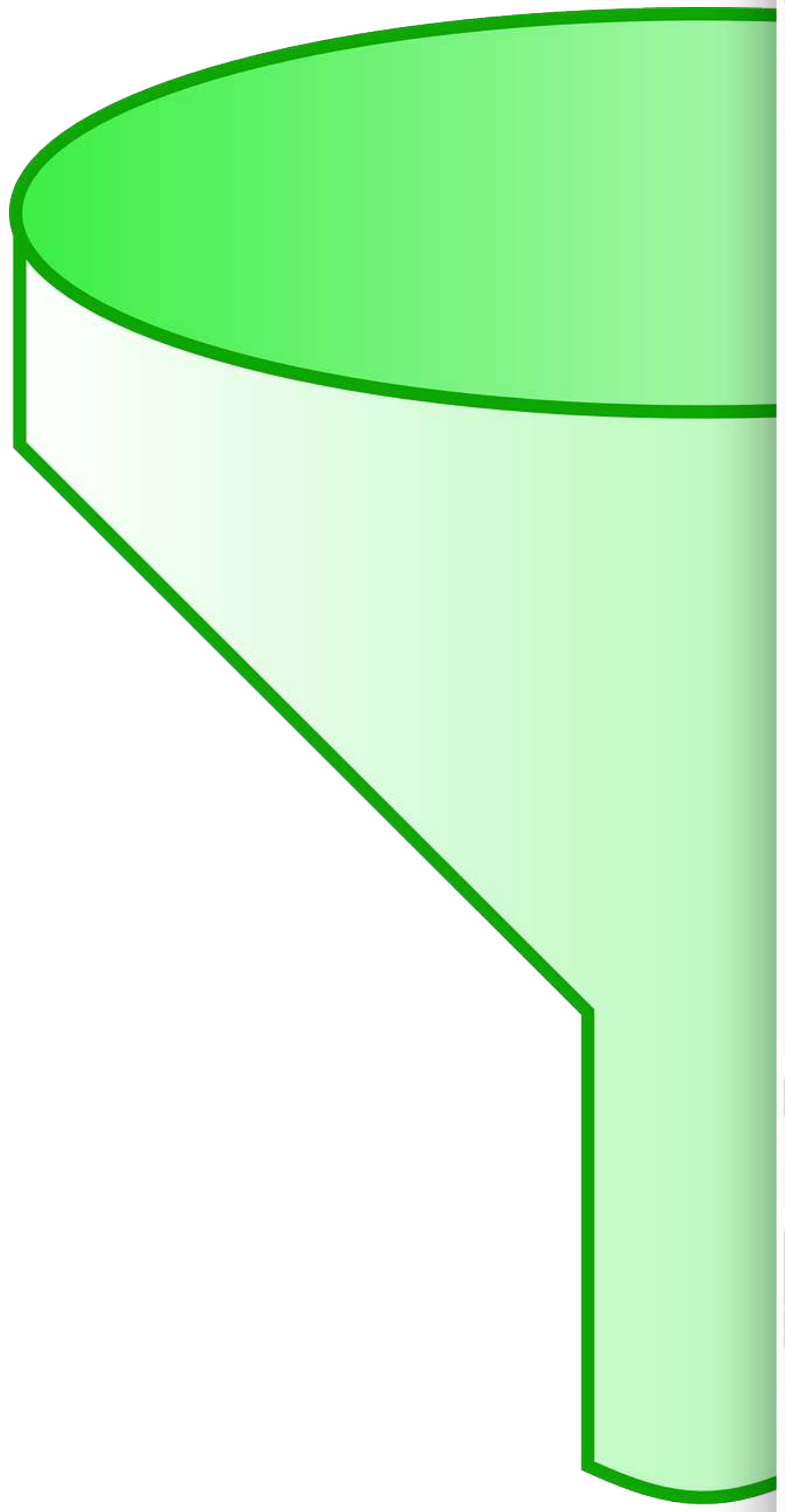
Interface

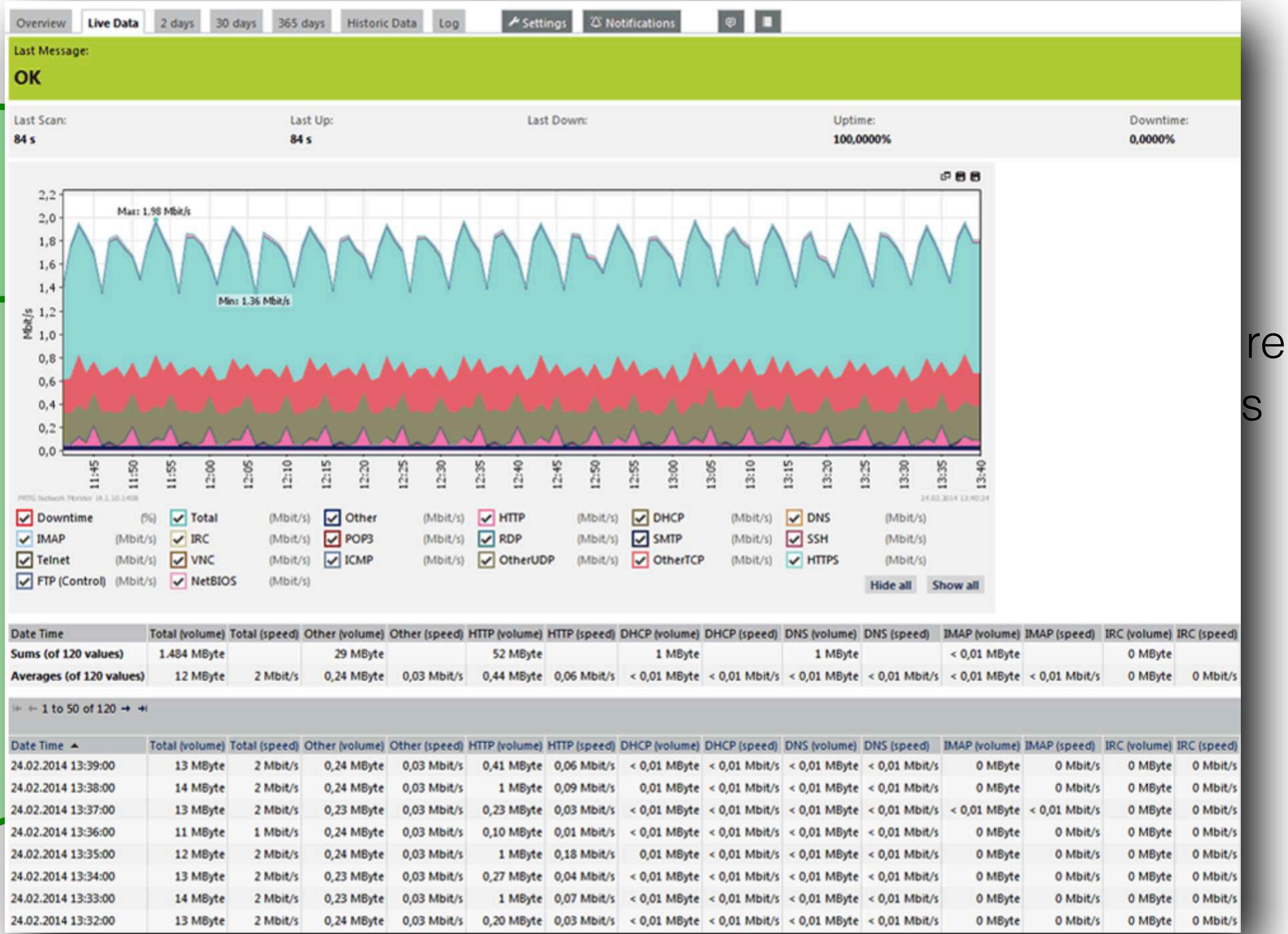
Type of Service

CLI view

Export to external NetFlow Collector

NetFlow Theory





Last Message:

OK

Last Scan:	Last Up:	Last Down:	Uptime:	Downtime:
84 s	84 s		100,0000%	0,0000%

☑ Downtime	(%)	☑ Total	(Mbit/s)	☑ Other	(Mbit/s)	☑ HTTP	(Mbit/s)	☑ DHCP	(Mbit/s)	☑ DNS	(Mbit/s)
☑ IMAP	(Mbit/s)	☑ IRC	(Mbit/s)	☑ POP3	(Mbit/s)	☑ RDP	(Mbit/s)	☑ SMTP	(Mbit/s)	☑ SSH	(Mbit/s)
☑ Telnet	(Mbit/s)	☑ VNC	(Mbit/s)	☑ ICMP	(Mbit/s)	☑ OtherUDP	(Mbit/s)	☑ OtherTCP	(Mbit/s)	☑ HTTPS	(Mbit/s)
☑ FTP (Control)	(Mbit/s)	☑ NetBIOS	(Mbit/s)								

Date Time	Total (volume)	Total (speed)	Other (volume)	Other (speed)	HTTP (volume)	HTTP (speed)	DHCP (volume)	DHCP (speed)	DNS (volume)	DNS (speed)	IMAP (volume)	IMAP (speed)	IRC (volume)	IRC (speed)
Sums (of 120 values)	1.484 MByte		29 MByte		52 MByte		1 MByte		1 MByte		< 0,01 MByte		0 MByte	
Averages (of 120 values)	12 MByte	2 Mbit/s	0,24 MByte	0,03 Mbit/s	0,44 MByte	0,06 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s

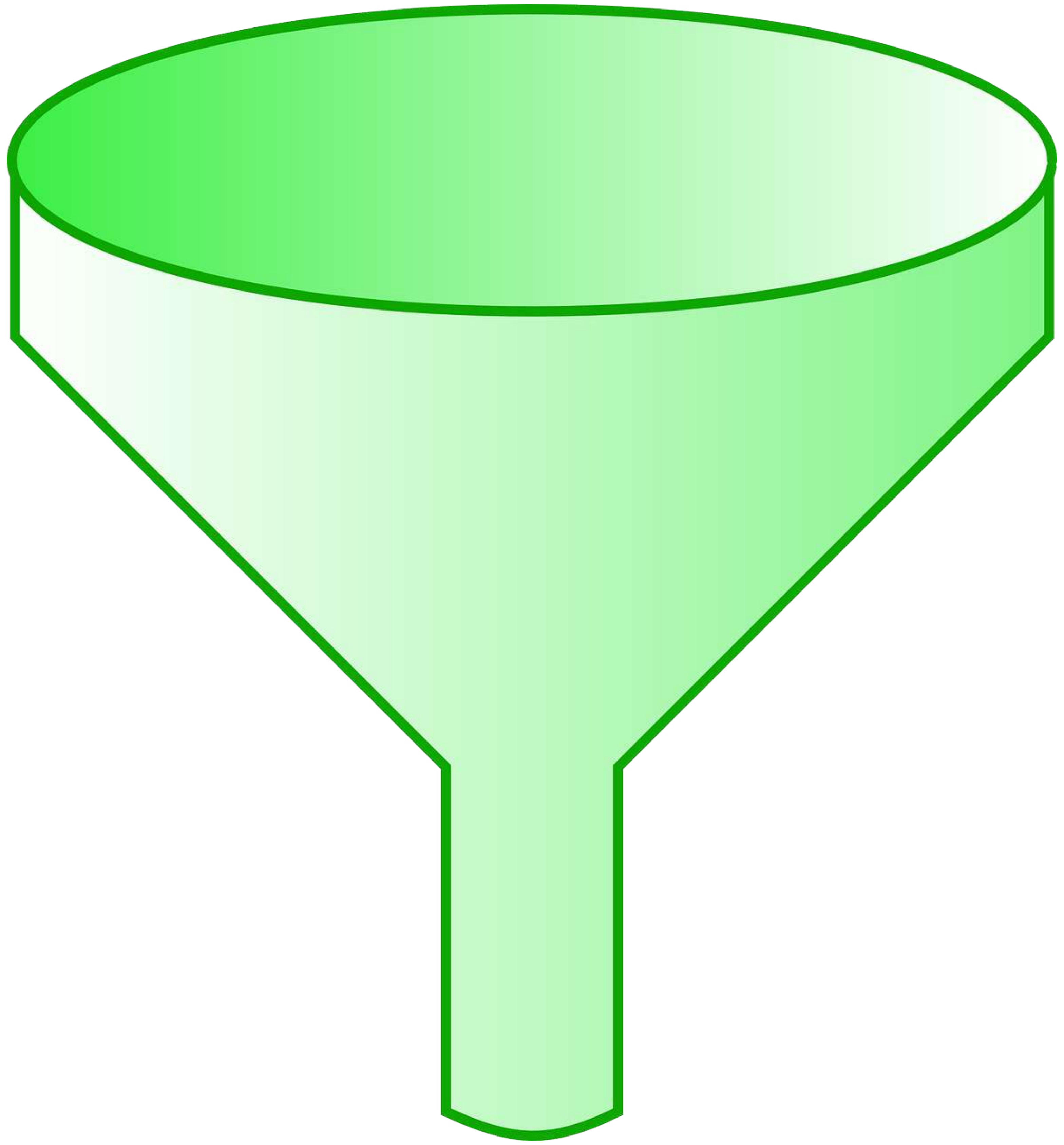
1 to 50 of 120

Date Time ▲	Total (volume)	Total (speed)	Other (volume)	Other (speed)	HTTP (volume)	HTTP (speed)	DHCP (volume)	DHCP (speed)	DNS (volume)	DNS (speed)	IMAP (volume)	IMAP (speed)	IRC (volume)	IRC (speed)
24.02.2014 13:39:00	13 MByte	2 Mbit/s	0,24 MByte	0,03 Mbit/s	0,41 MByte	0,06 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:38:00	14 MByte	2 Mbit/s	0,24 MByte	0,03 Mbit/s	1 MByte	0,09 Mbit/s	0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:37:00	13 MByte	2 Mbit/s	0,23 MByte	0,03 Mbit/s	0,23 MByte	0,03 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:36:00	11 MByte	1 Mbit/s	0,24 MByte	0,03 Mbit/s	0,10 MByte	0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:35:00	12 MByte	2 Mbit/s	0,24 MByte	0,03 Mbit/s	1 MByte	0,18 Mbit/s	0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:34:00	13 MByte	2 Mbit/s	0,23 MByte	0,03 Mbit/s	0,27 MByte	0,04 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:33:00	14 MByte	2 Mbit/s	0,23 MByte	0,03 Mbit/s	1 MByte	0,07 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s
24.02.2014 13:32:00	13 MByte	2 Mbit/s	0,24 MByte	0,03 Mbit/s	0,20 MByte	0,03 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	< 0,01 MByte	< 0,01 Mbit/s	0 MByte	0 Mbit/s	0 MByte	0 Mbit/s

records

s

NetFlow Theory



NetFlow Collector:

- Exporter bundles 30-50 similar flows
- Flow data transported over UDP to collector
- Provides real-time and historical data

NetFlow v5:

- Most popular version due to wide compatibility
- Uses a fixed data format

NetFlow v9:

- Most recent version with added security and analysis
- Uses a dynamic data format with templates

NetFlow Demo

SPAN Theory

Switched Port Analyzer (SPAN):

- Also referred to as port mirroring
- Packet copies are sent to a traffic analyzer
- Analyzers aggregate and sort data in a visual manner

SPAN Theory

Local SPAN:

- Traffic captured and mirrored locally

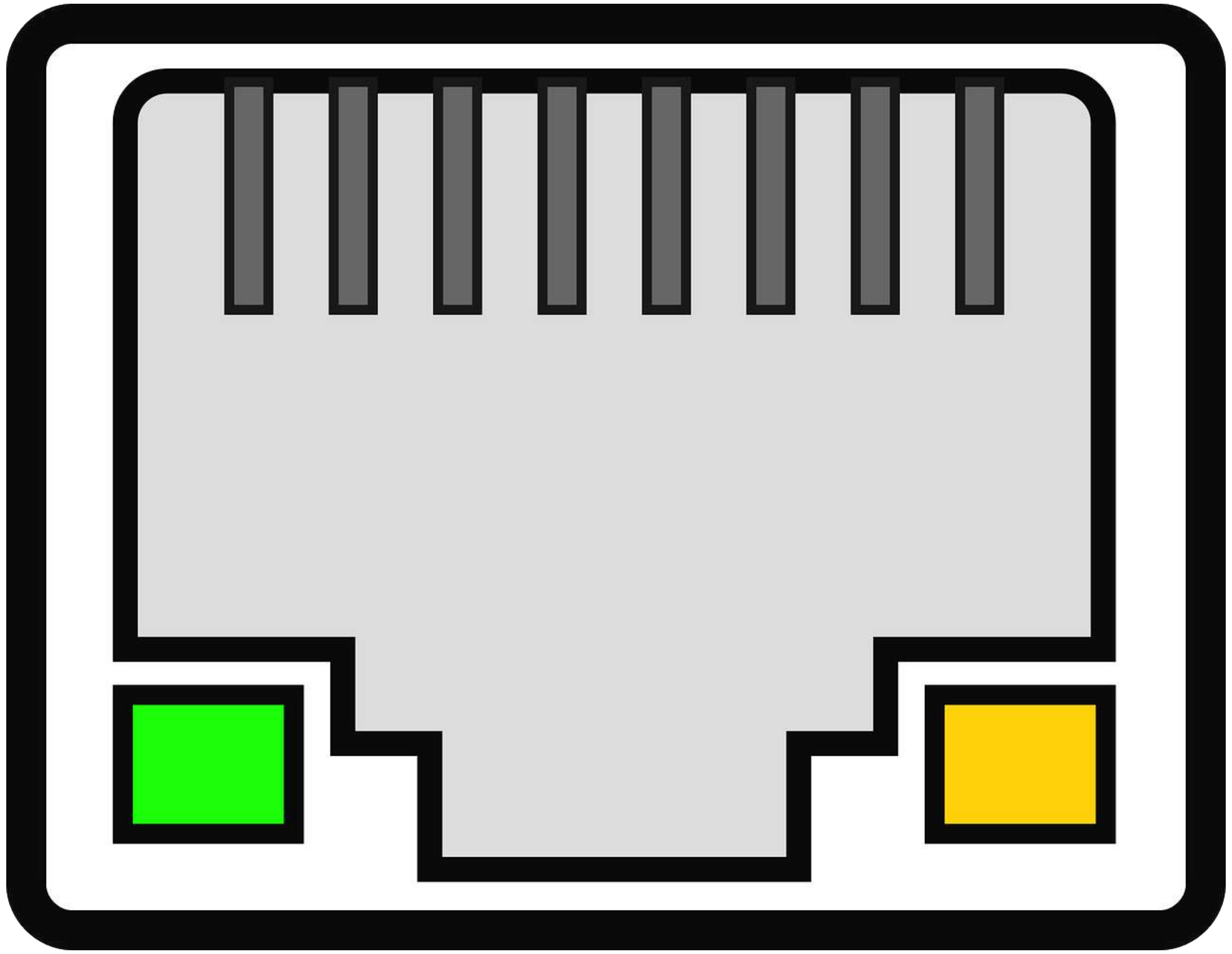
Remote SPAN (RSPAN):

- Monitor multiple remote switches
- Traffic copied to a central traffic analyzer

Encapsulated Remote SPAN (ERSPAN):

- Cisco proprietary version
- Uses generic routing encapsulation (GRE)

SPAN Theory

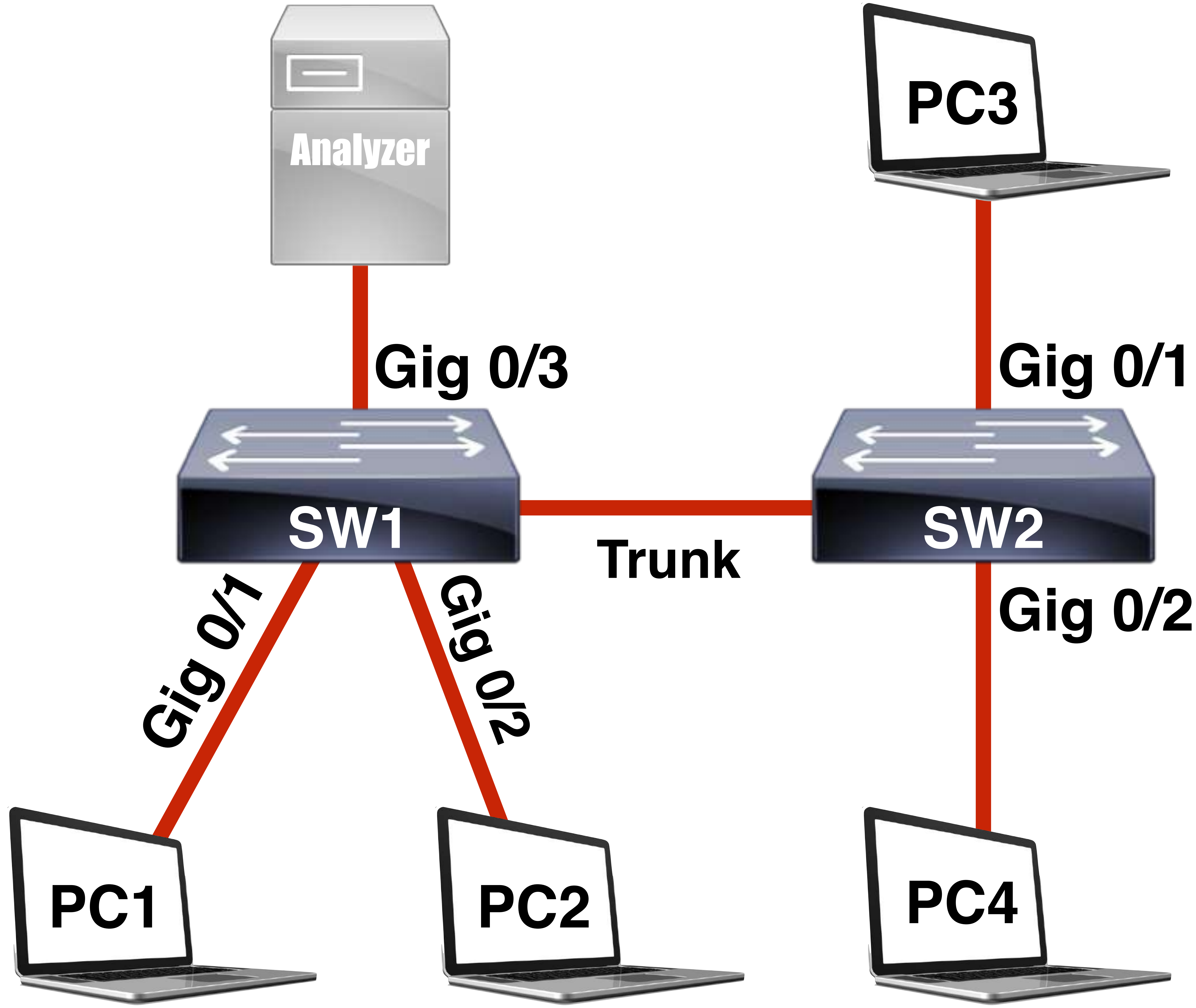


SPAN Monitoring

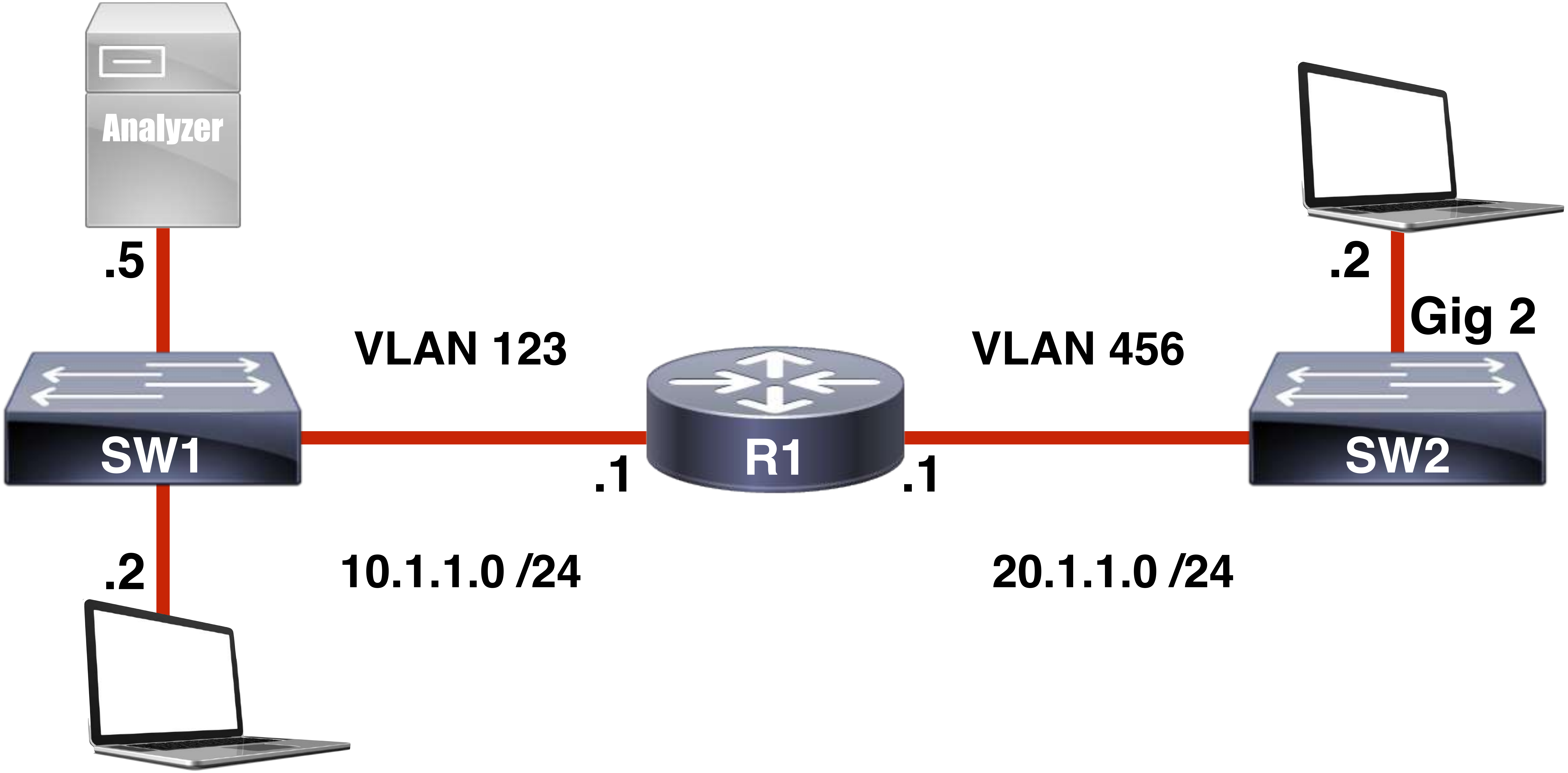
- Monitored ports referred to as SPAN source
- Monitor transmit, receive, or both
- Transmit (Tx) | Receive (Rx)
- The mirrored traffic source could be a VLAN
- Can reside in separate VLANs
- Source and destination cannot be the same port

*** Be aware of the potential for link saturation when using SPAN**

Local SPAN and RSPAN Topology



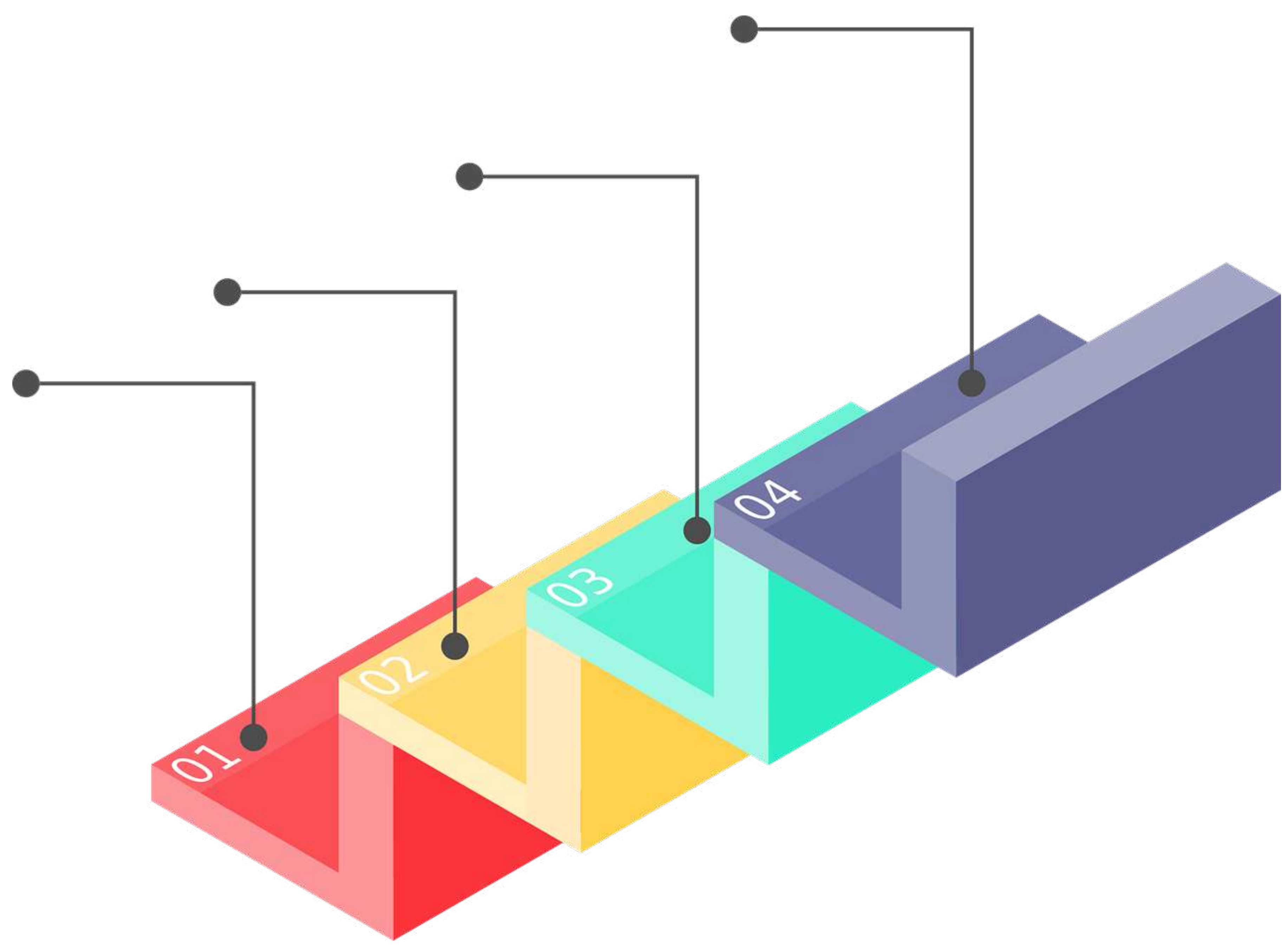
ERSPAN Topology



SPAN Demos

IP SLA

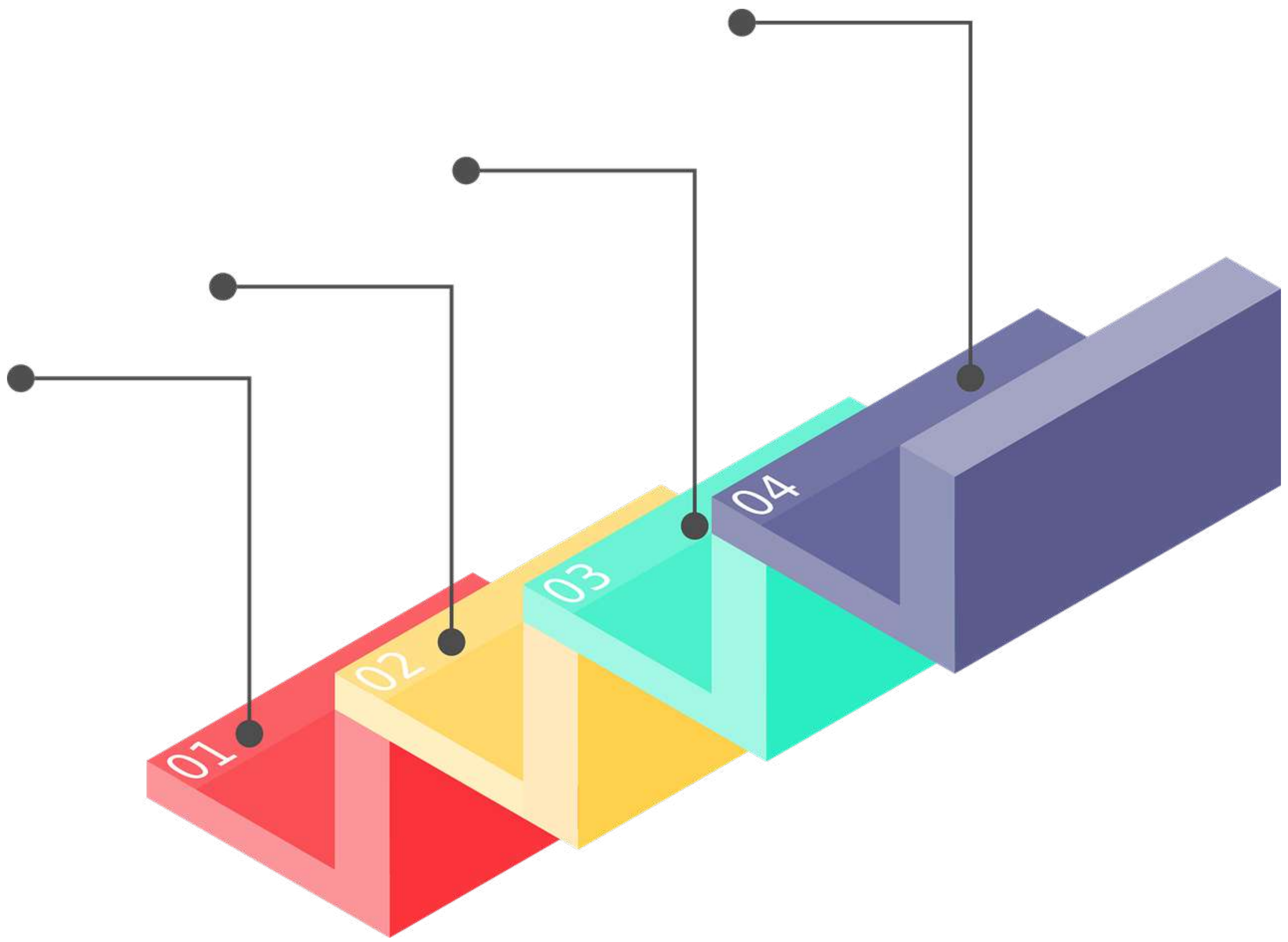
IP SLA Theory



IP SLA:

- Active monitoring and reporting
- Connectivity, delay, jitter, packet loss, etc.
- Common tool for service providers

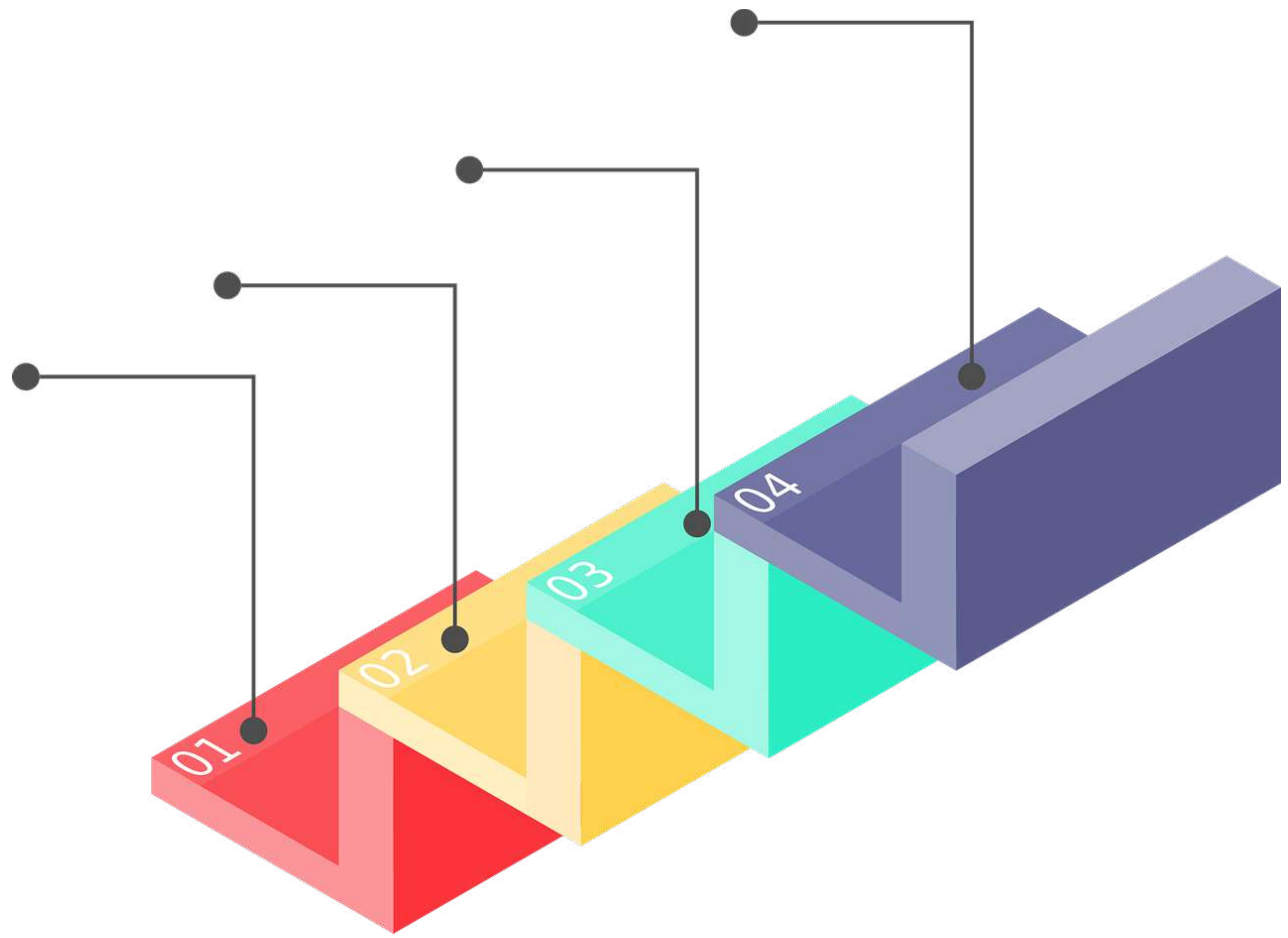
IP SLA Theory



IP SLA Source:

- Generates packets and sends to destination
- ICMP echo is an example of a probe
- Response would include time-stamps and other info

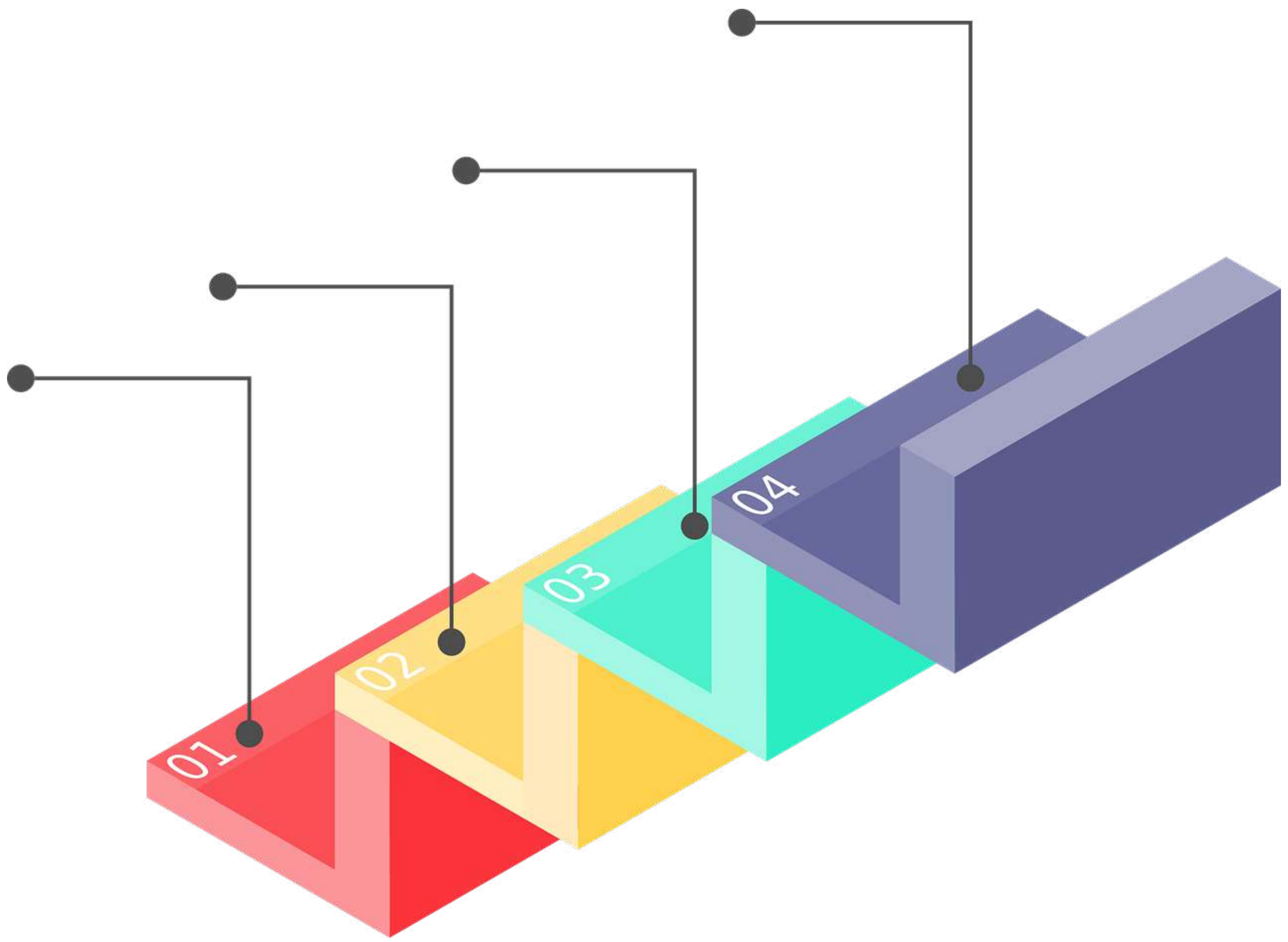
IP SLA Theory



IP SLA Responder:

- Provides more advanced response metrics
- Some IP SLA operations require a responder

IP SLA Theory



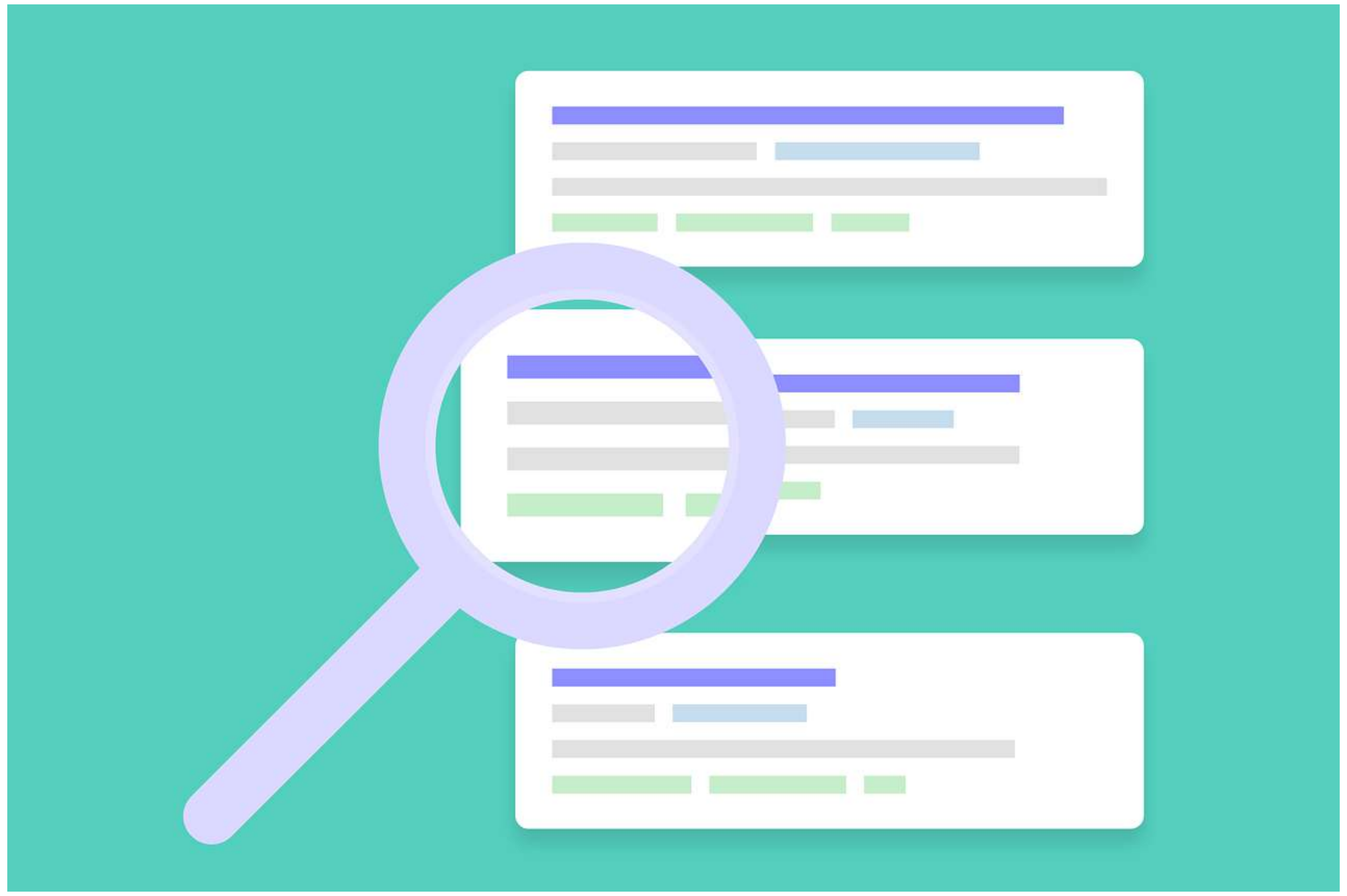
IP SLA:

- Leverages SNMP traps triggered by events
- Threshold violations trigger alerts
- Violations can also trigger other IP SLA operations

IP SLA Demos

Embedded Event Manager (EEM)

EEM Theory



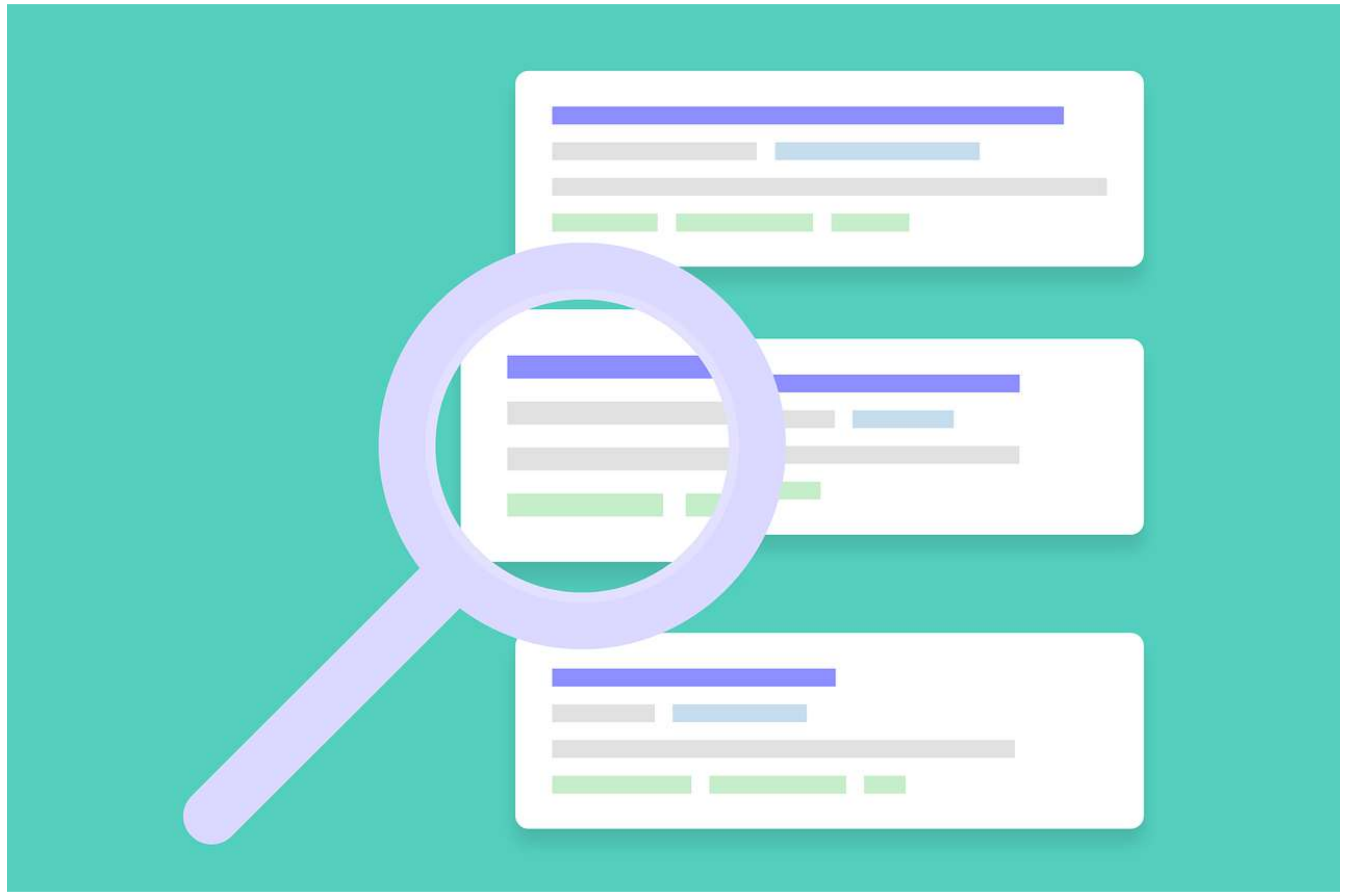
Applets:

- More simplified option using CLI

Scripts:

- Created with an interpreter language
- Tcl programming language

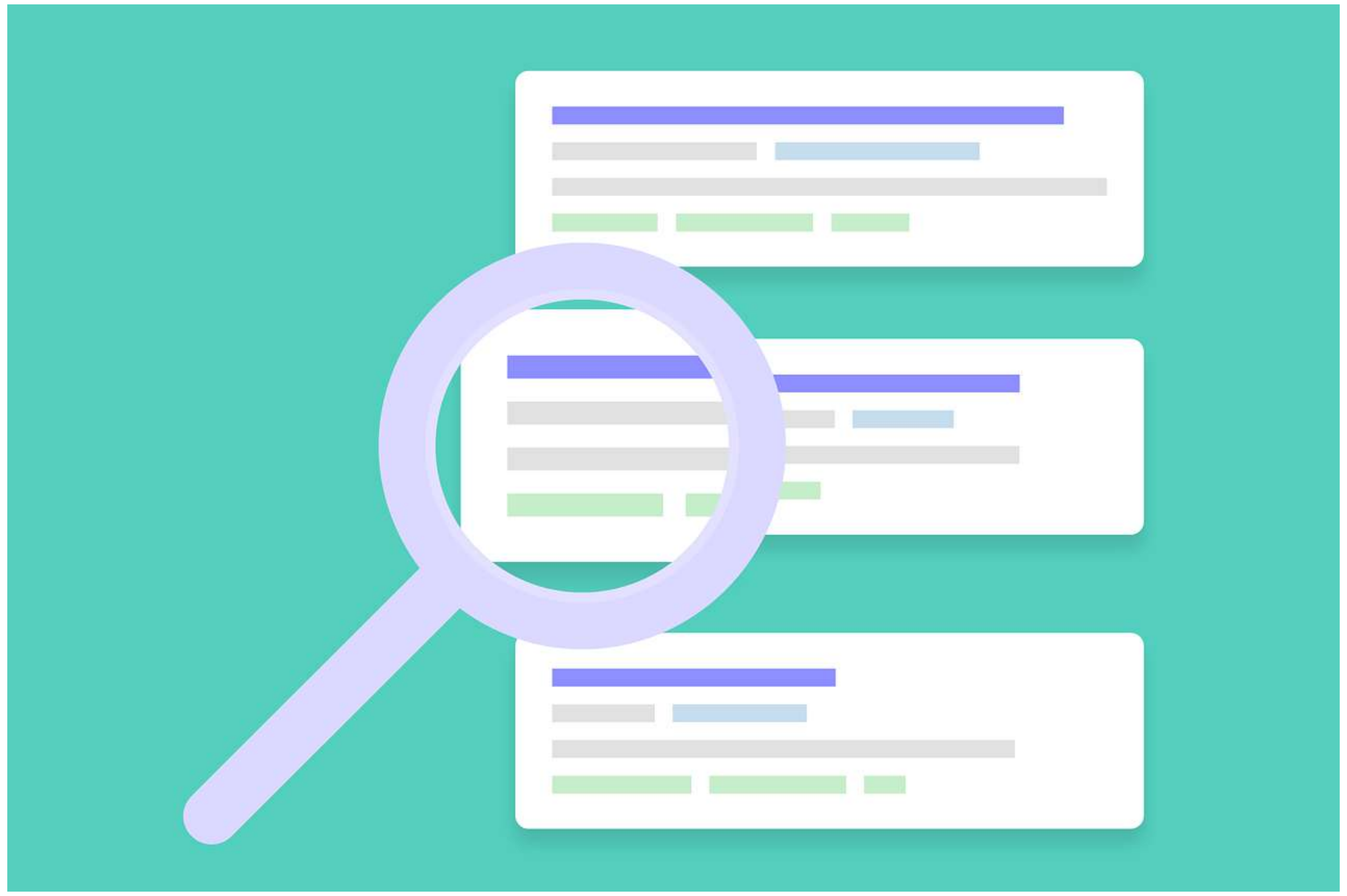
EEM Theory



EEM Event Detectors:

- Determines when notable events occur
- SNMP, Syslog, Counters, Timers, IP SLA, etc.
- Trigger an EEM event action
- Applet and actions vary based on Cisco IOS version

EEM Theory



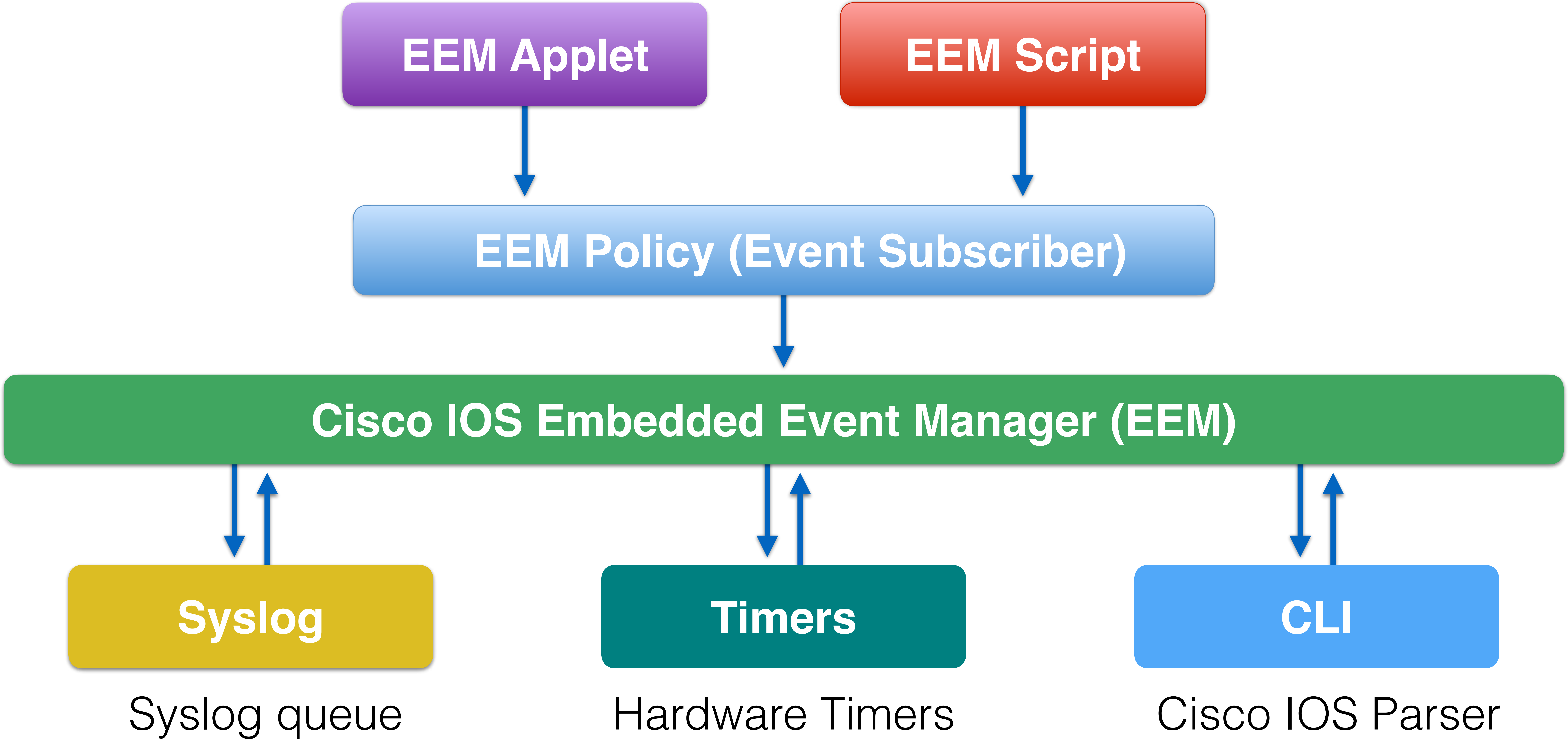
EEM Policy:

- Also called an Event Subscriber

Steps:

- Define specific events to monitor
- Define event detector for monitoring
- Define action to be taken upon detection

EEM Theory


EEM Applet

EEM Script

EEM Policy (Event Subscriber)

Cisco IOS Embedded Event Manager (EEM)

Syslog

Timers

CLI

Syslog queue

Hardware Timers

Cisco IOS Parser

EEM Demo