

Jack-Daniyel Strong

Jack is the President of J-D Strong Consulting, Inc. and Strong Solutions. As a member of the Apple Consultants Network, grew from a one-man consultancy into an Apple Authorized Reseller and Service Provider for the Eastern Washington and Northern Idaho area.

Strong Solutions' sole focus is on MacOS and iOS solutions for Small and Medium Business.



**STRONG
SOLUTIONS**



Authorized
Reseller

Authorized
Service Provider



Authorized
Reseller
Authorized
Service Provider



**STRONG
SOLUTIONS**



Authorized
Reseller

Authorized
Service Provider

Networking: Discover, Map and Reporting Essentials

Networks

Map

Detect

Report

snmp

Simple Network Management Protocol

SNMP

Yeah, you know me

- Protocol to transmit device data
 - Performance
 - Health Status
 - Event Notification
- Supported by 99% of devices
- Mostly implemented in Data Centers
- Device Independent

SNMP

Yeah, you know me

- SNMPv1
- SNMPv2c
- SNMPv3

SNMP

Yeah, you know me

- SNMP Manager
- Devices
- SNMP Agents
- Management Information Bases (MIBs)

SNMP Manager

- Queries agents
- Gets responses from agents
- Sets variables in agents
- Acknowledges asynchronous events from agents

Managed Devices

- Routers
- Switches
- Servers
- Workstations
- Printers
- UPSs
- etc...

SNMP Agent

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non-SNMP manageable network node.

MIB



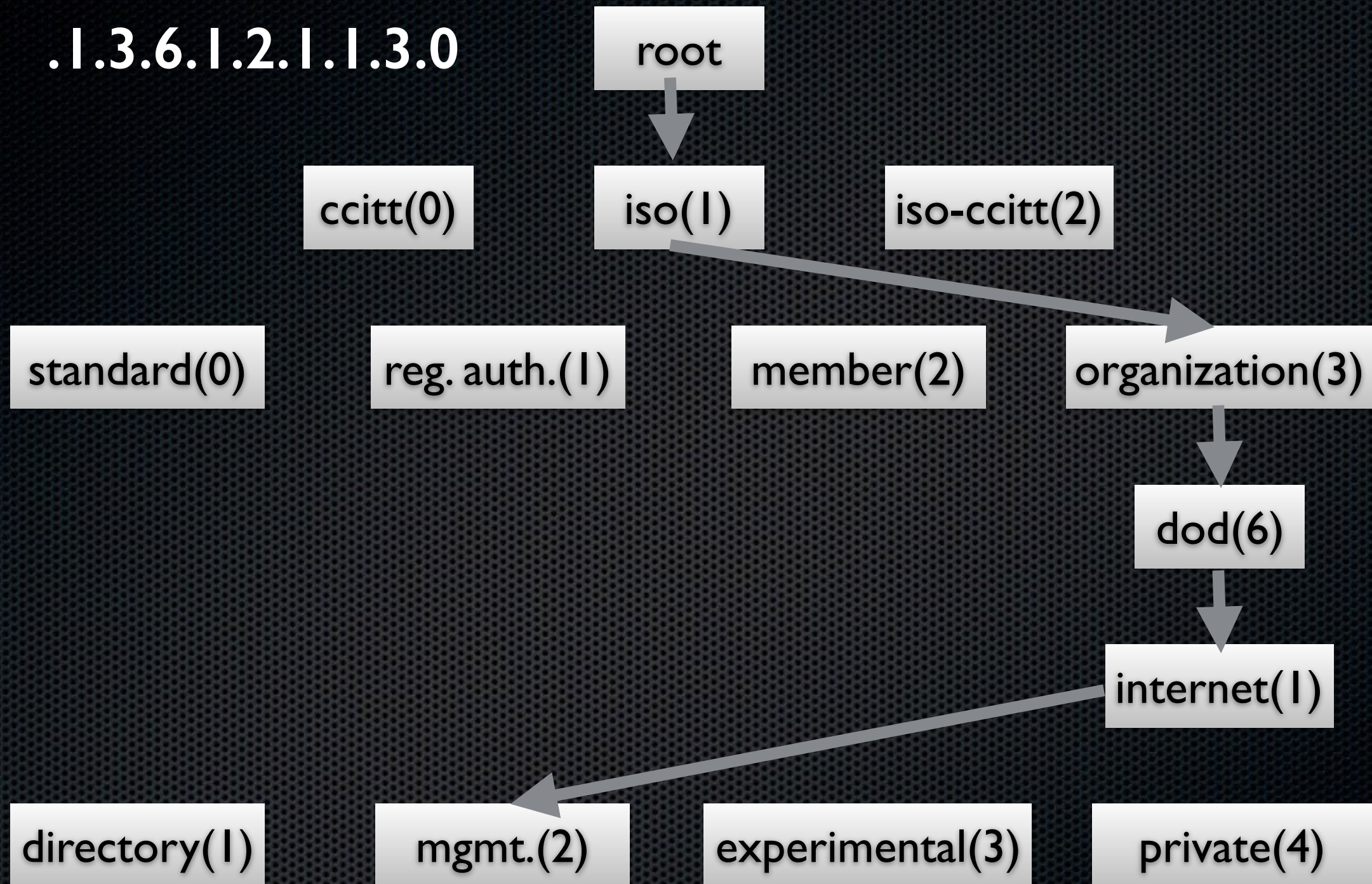
MIB

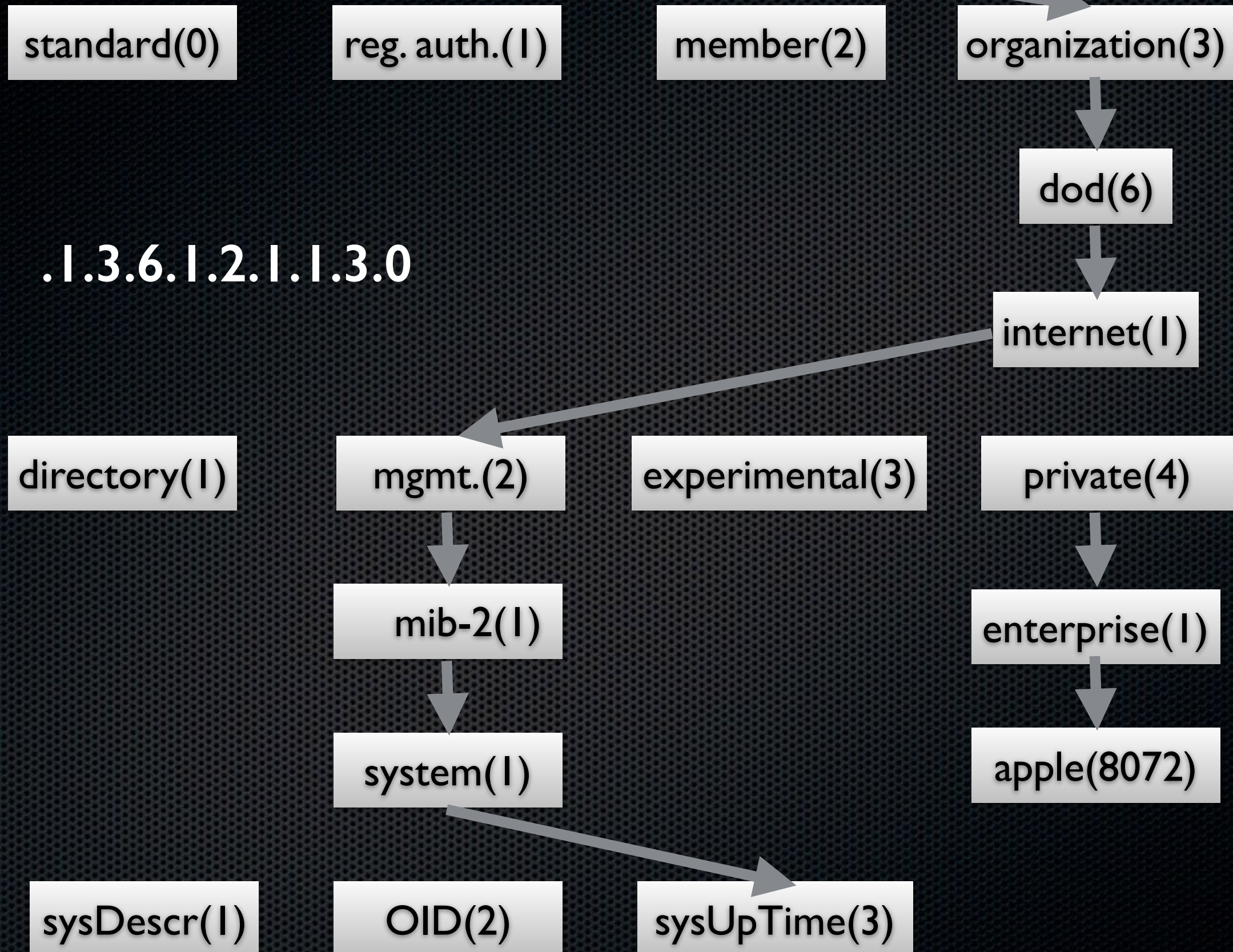
- Dictionary for managing network element
- Each defines a unique Object Identifier (OID)
- OIDs can be Scalar or Tabular
- Every OID is organized hierarchically in MIB

sysUpTime

- OID for the object sysUpTime is .1.3.6.1.2.1.1.3.0
- textual description of sysUpTime OID is
iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.

.1.3.6.1.2.1.1.3.0

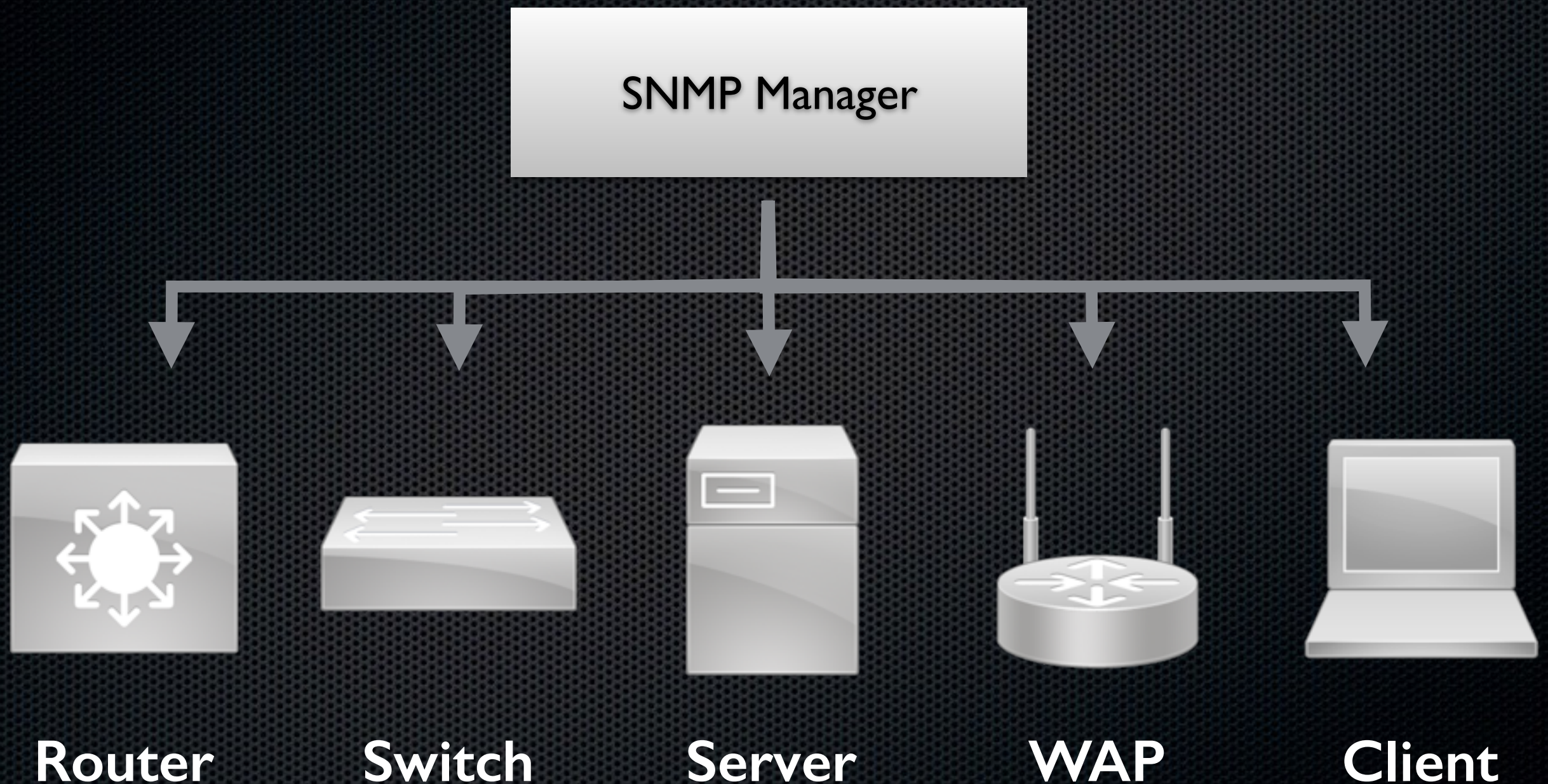




SNMP Messages

- SNMP GET
- SNMP GET-NEXT
- SNMP GET-RESPONSE
- SNMP SET
- SNMP TRAP

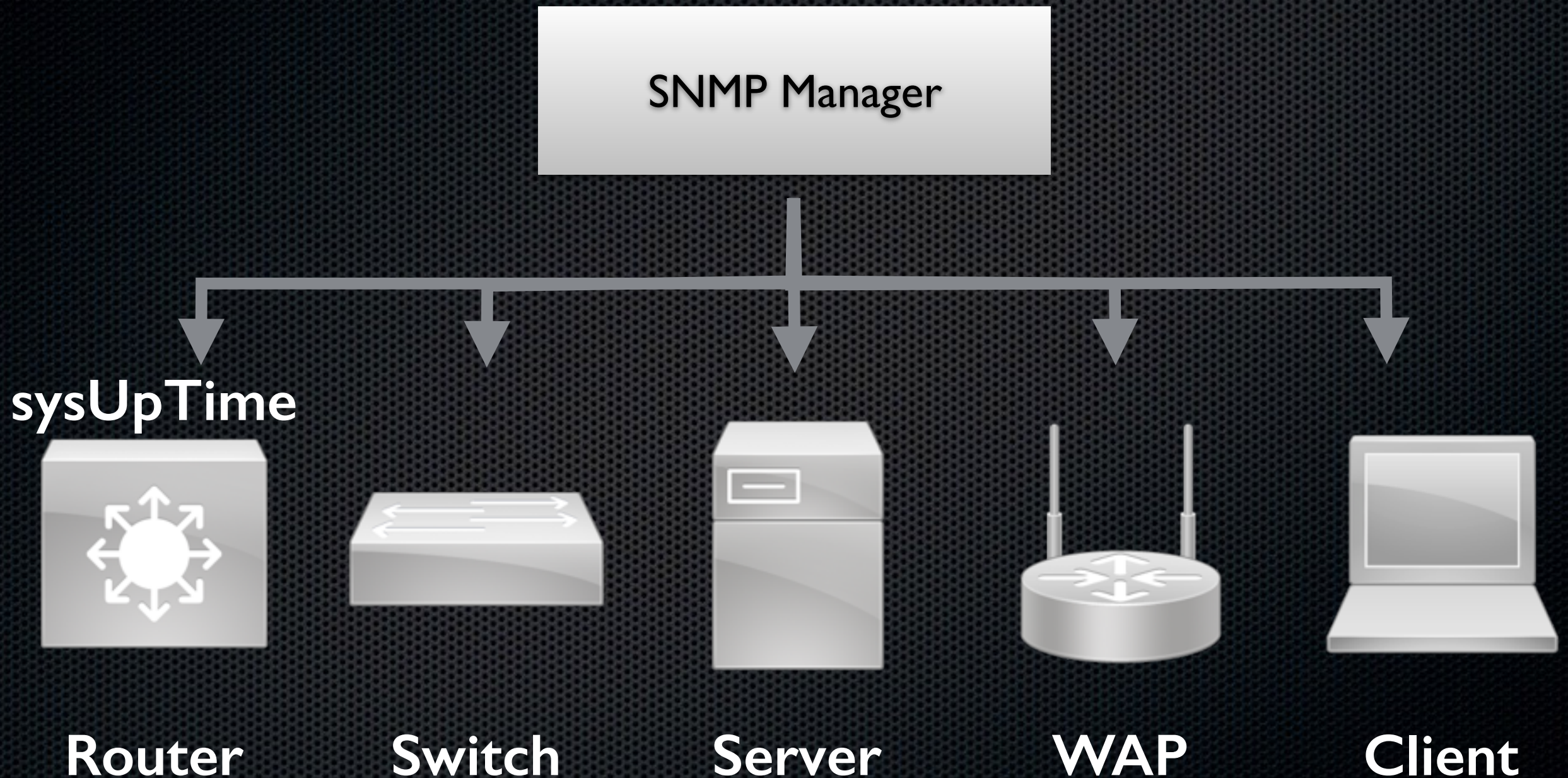
SNMP Communication



SNMP Communication



SNMP Communication



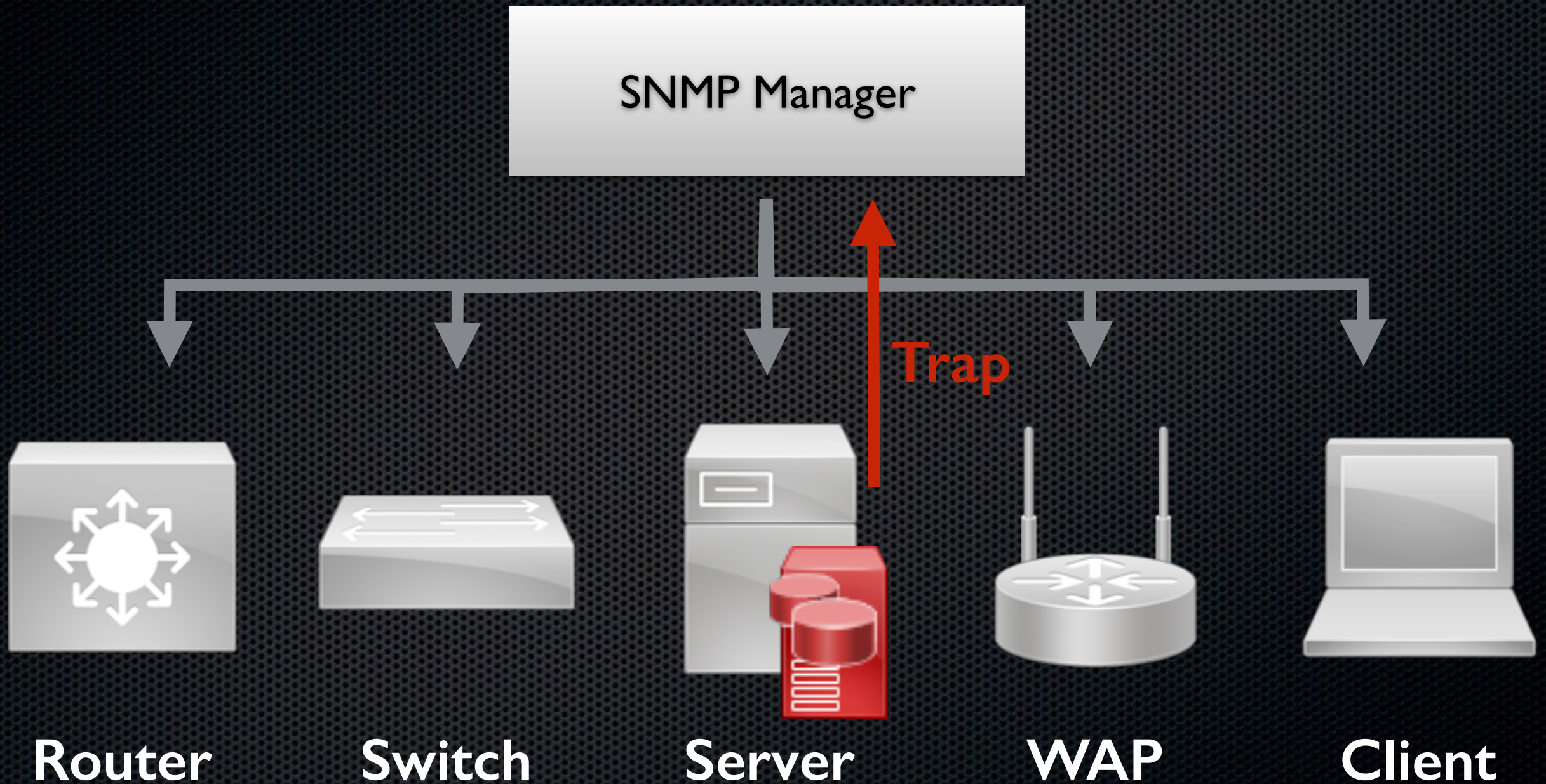
snmpwalk

uses SNMP GETNEXT requests to query a network entity for a tree of information

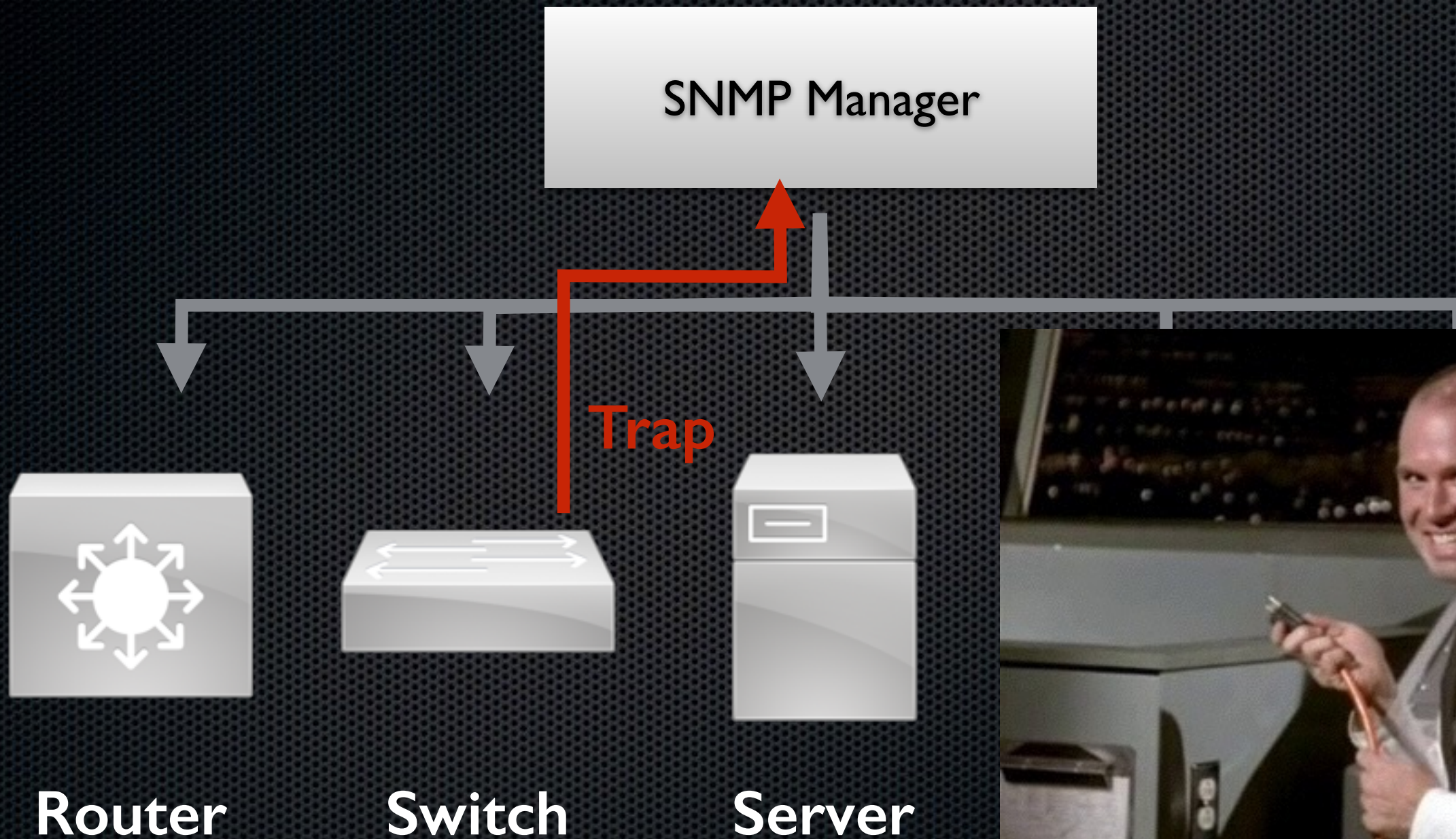
```
sudo snmpwalk -v 2c -c public -On  
10.0.1.1 .1.3.6.1.2.1.1.1
```

```
.1.3.6.1.2.1.1.1.0 = STRING: Apple  
AirPort – Apple Inc., 2006–2012. All  
rights Reserved.
```


SNMP Communication



SNMP Communication



nmap

Network Mapper

nmap

- Free and Open Sourced
- Network Discovery
- Security Auditing
- Rapidly Scans
 - Large Network
 - Single Host
- Download from nmap.org

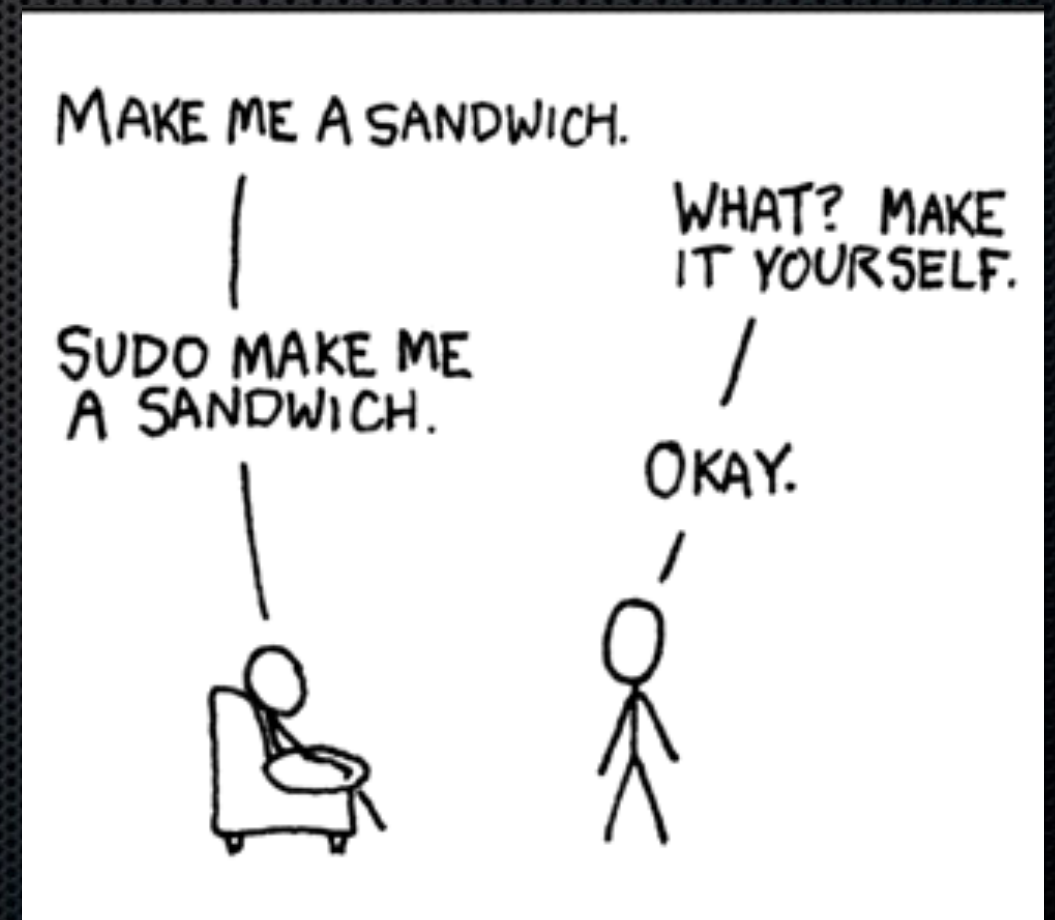
nmap Data Collection

- Available Hosts
- Services Offered
 - Application Name
 - Version
- Operating System
- Packet Filter & Firewall Definition

sudo nmap

Calling nmap

`sudo nmap [commands]`



nmap --iflist

Pull routing table

Starting Nmap 7.01 (<https://nmap.org>) at 2016-03-13 11:04 PDT

*****INTERFACES*****

DEV	(SHORT)	IP/MASK	TYPE	UP	MTU	MAC
lo0	(lo0)	127.0.0.1/8	loopback	up	16384	

...

*****ROUTES*****

DST/MASK	DEV	METRIC	GATEWAY
10.0.1.1/32	en1	0	
162.222.40.209/32	en1	0	10.0.1.1

Similar to ping 255.255.255.255; arp -a

nmap [fqdn | ip]

Shows ports, states, services (for the ports)
and a MAC address for each IP being scanned

Starting Nmap 7.01 (<https://nmap.org>) at 2016-03-13 12:14 PDT

Nmap scan report for apple.com (17.172.224.47)

Host is up (0.19s latency).

Other addresses for apple.com (not scanned): 17.178.96.59

17.142.160.59

Not shown: 995 filtered ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

554/tcp	open	rtsp
---------	------	------

7070/tcp	open	realserver
----------	------	------------

Nmap done: 1 IP address (1 host up) scanned in 28.11 seconds

scan a subnet

```
nmap 192.168.0.*
```

```
nmap 192.168.0.1/24
```

scan a range

```
nmap 192.168.0.1-20
```

exclude an IP

```
nmap 192.168.0.1-20 --exclude 192.168.0.10
```

a few hosts within that range

```
nmap 192.168.210.1,10,254
```


nmap ports

- Default Scans All Ports
- Specify port(s) with -p
 - T: for only TCP
 - U: for only UDP
 - Neither for both
- Range, Individual, etc.
- `nmap -p 22-25,80,110,143,443`

nmap -A [fqdn]

Operating System Detection

```
...  
Warning: OSScan results may be unreliable because we could not  
find at least 1 open and 1 closed port  
Device type: WAP|storage-misc  
Running: Apple embedded  
...
```


nmap -v -O -oosscan-guess

True Operating System Detection

...

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: WAP|storage-misc

Running: Apple embedded, Peplink embedded

...

nmap --dns-servers 8.8.8.8

Override System DNS

```
...  
Nmap scan report for yahoo.com (206.190.36.45)  
Host is up (0.073s latency).  
Other addresses for yahoo.com (not scanned): 98.138.253.109  
98.139.183.24 2001:4998:58:c02::a9 2001:4998:c:a06::2:4008  
2001:4998:44:204::a7  
rDNS record for 206.190.36.45: ir1.fp.vip.gq1.yahoo.com  
Not shown: 995 filtered ports  
...
```


Firewall Detection/Evasion

- Firewalls can make mapping difficult
- intrusion detection systems (IDS)
- intrusion *prevention* systems (IPS)

nmap -sA [fqdn]

Firewall Detection

Nmap scan report for www.apple.com (23.4.129.93)
Host is up (0.025s latency).
Other addresses for www.apple.com (not scanned): 2001:418:142b:
280::1aca 2001:418:142b:298::1aca
rDNS record for 23.4.129.93:
a23-4-129-93.deploy.static.akamaitechnologies.com
Not shown: 997 filtered ports

PORT	STATE	SERVICE
21/tcp	unfiltered	ftp
554/tcp	unfiltered	rtsp
7070/tcp	unfiltered	realserver

nmap -PN [fqdn]

Firewall Detection

Nmap scan report for www.apple.com (23.200.94.74)
Host is up (0.055s latency).
Other addresses for www.apple.com (not scanned):
2001:428:7000:49a::1aca 2001:428:7000:486::1aca
rDNS record for 23.200.94.74:
a23-200-94-74.deploy.static.akamaitechnologies.com
Not shown: 995 filtered ports

PORT	STATE	SERVICE
21/tcp	open	ftp
80/tcp	open	http
443/tcp	open	https
554/tcp	open	rtsp
7070/tcp	open	realserver

See if some devices are up even if behind a firewall

```
nmap -sP 192.168.210.10-20
```

Run a scan using SYN and ACK scans

```
nmap -PS 443 www.apple.com
```

```
nmap -PA 443 www.apple.com
```

determine port state

```
nmap -reason www.apple.com
```

Show all sent/received packets

```
nmap --packet-trace www.apple.com
```

determine version of software of remote ports from header

```
nmap -sV www.apple.com
```


nmap Security Scanning

- Test Attacking Your Server (white hat)
- Port Scanning
 - Are Available Ports Expected?
 - Are Filters Working?
 - Survive Brute Force attack?

`nmap -v -sT --spoof-mac 0 fqdn`

Spoof a MAC Address

```
Spoofting MAC address 71:8A:97:9B:FA:A2 (No registered vendor)
Initiating Ping Scan at 15:14
Scanning www.apple.com (104.66.211.3) [4 ports]
Completed Ping Scan at 15:14, 3.02s elapsed (1 total hosts)
Nmap scan report for www.apple.com (104.66.211.3) [host down]
Other addresses for www.apple.com (not scanned):
2001:428:7000:486::1aca 2001:428:7000:49a::1aca
Read data files from: /usr/local/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping
probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```



```
nmap -v -sT -Pn --spoof-mac 0 fqdn
```

Spoof a MAC Address, No Ping

Spoofing MAC address 63:E2:89:88:1E:AB (No registered vendor)

Initiating Parallel DNS resolution of 1 host. at 15:15

Completed Parallel DNS resolution of 1 host. at 15:15, 0.03s elapsed

Initiating Connect Scan at 15:15

Scanning www.apple.com (104.66.211.3) [1000 ports]

Discovered open port 21/tcp on 104.66.211.3

Discovered open port 554/tcp on 104.66.211.3

Discovered open port 443/tcp on 104.66.211.3

Discovered open port 80/tcp on 104.66.211.3

Discovered open port 7070/tcp on 104.66.211.3

Completed Connect Scan at 15:16, 10.47s elapsed (1000 total ports)

Nmap scan report for www.apple.com (104.66.211.3)

Use decoys to avoid scan detection

```
nmap -n -D 10.0.1.10,10.0.1.54,10.0.1.210
```

SYN-Flood Attack

```
nmap -sX www.apple.com
```

Use a custom MTU (Maximum Transmission Unit)

```
nmap -mtu 64 www.apple.com
```

Use fragment packets for TCP header

```
nmap -f www.apple.com
```


ZenMap



- GUI for nmap
- Build nmap commands
- Topology Map
- Requires X11 (XQuartz)
- ZenMap Included with nmap installer

ZenMap



Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS	Host
	10.0.1.1
	www.apple.com (

Nmap Output Ports / Hosts Topology Host Details Scans

```
Retrying OS detection (try #2) against www.apple.com (23.4.129.93)
Initiating Traceroute at 16:42
Completed Traceroute at 16:42, 0.02s elapsed
NSE: Script scanning 23.4.129.93.
Initiating NSE at 16:42
Completed NSE at 16:43, 32.00s elapsed
Initiating NSE at 16:43
Completed NSE at 16:43, 0.00s elapsed
Nmap scan report for www.apple.com (23.4.129.93)
Host is up (0.019s latency).
Other addresses for www.apple.com (not scanned): 2001:428:7000:486::laca
2001:428:7000:49a::laca
rDNS record for 23.4.129.93: a23-4-129-93.deploy.static.akamaitechnologies.com
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
| ftp-bounce: no banner
80/tcp    open  http         AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-favicon: Unknown favicon MD5: 28EC4EABA5AE210B98A11257CAF5BADE
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 180 disallowed entries (15 shown)
| /*/includes/* /*/retail/availability*
| /*/retail/availabilitySearch* /*/retail/pickupEligibility* /*/search/*
| /*/shop/signed in account* /*/shop/sign in* /*/shop/sign out*
| /*/shop/*WebObjects/* /*/shop/1-800-MY-APPLE/* /*/shop/answer/vote*
| /*/shop/bag* /*/shop/browse/campaigns/mobile overlay*
| /*/shop/button availability* /*/shop/favorites*
| http-server-header:
|   AkamaiGHost
|   Apache
| http-title: Apple
443/tcp   open  ssl/http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-favicon: Unknown favicon MD5: 28EC4EABA5AE210B98A11257CAF5BADE
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
```


ZenMap



Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

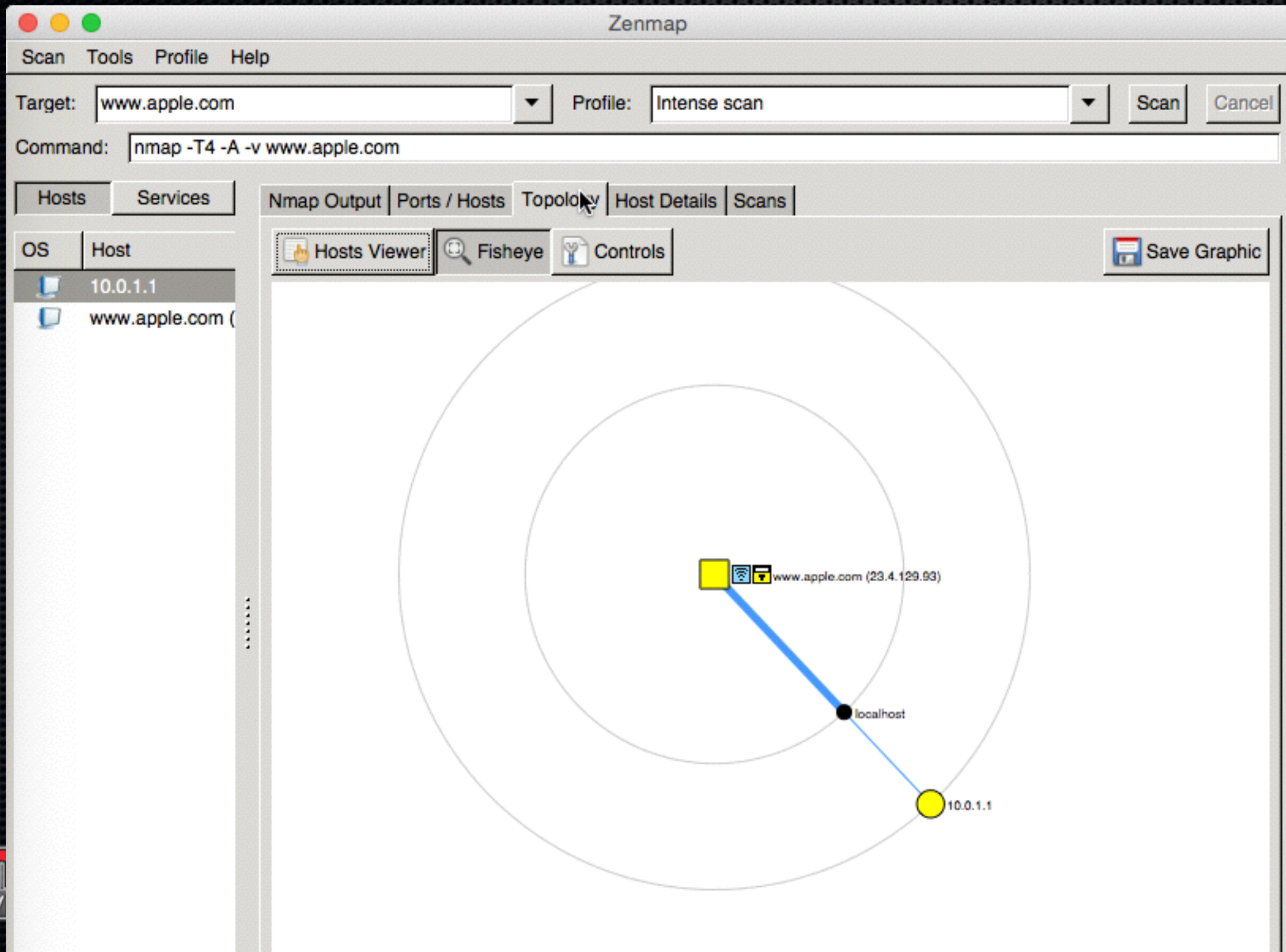
Hosts Services

OS	Host
	10.0.1.1
	www.apple.com (

Nmap Output Ports / Hosts Topology Host Details Scans

	Port	Protocol	State	Service	Version
	53	tcp	open	domain	
	5000	tcp	open	rtsp	Apple iTunes rtspd 105.1 (Apple TV)
	5009	tcp	open	airport-admin	Apple AirPort or Time Capsule admin
	10000	tcp	open	set-sensor-mgmt	

ZenMap



ZenMap



Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host
	10.0.1.1
	www.apple.com (

10.0.1.1

- Host Status
 - State: up
 - Open ports: 4
 - Filtered ports: 0
 - Closed ports: 996
 - Scanned ports: 1000
 - Up time: Not available
 - Last boot: Not available
- Addresses
 - IPv4: 10.0.1.1
 - IPv6: Not available
 - MAC: 00:F7:6F:D4:D0:C9
- Operating System
 - Name: Apple AirPort Extreme WAP or Time Capsule NAS device (NetBSD 4.99), or QNX 6.5.0
 - Accuracy:

100%
 - Ports used
 - OS Classes
 - TCP Sequence
 - IP ID Sequence
 - TCP TS Sequence

Fing



- (D)iscover

- (S)can

- (F)ingbox

- (P)ing

- display (I)nfos

- (Free)

2016/03/14 22:50:19 overlook fing discovery re

State	Host	MAC Address
-------	------	-------------

UP	10.0.2.1	50:3D:E5:83:61:3F (Cisco)
----	----------	---------------------------

UP	10.0.2.8	F4:CE:46:3E:BB:AB (HP)
----	----------	------------------------

UP	10.0.2.11	00:1E:8F:2E:DE:A6 (CANON)
----	-----------	---------------------------

UP	10.0.2.13	F4:CE:46:3F:18:A6 (HP)
----	-----------	------------------------

UP	10.0.2.16	00:80:87:C2:53:49 (OKI EL)
----	-----------	----------------------------

Scan result for 10.0.2.69 (00:11:32:4A:4A:DB)

Port	Service	Description
------	---------	-------------

80	http	World Wide Web HTTP
----	------	---------------------

139	netbios-ssn	NETBIOS Session Serv
-----	-------------	----------------------

161	snmp	
-----	------	--

445	microsoft-ds	SMB direct host over IP
-----	--------------	-------------------------

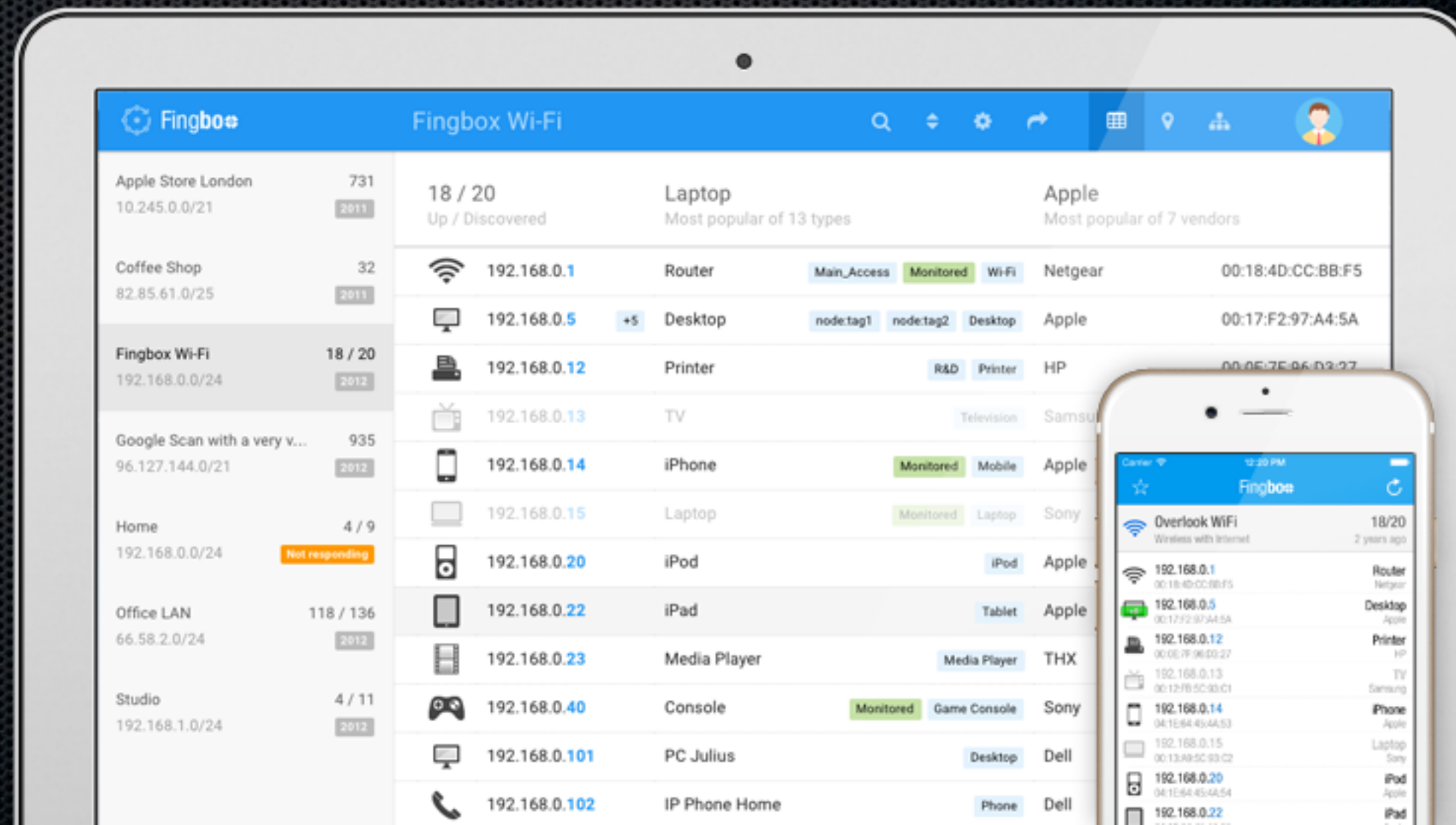
515	printer	spooler (Lpd)
-----	---------	---------------

548	afp	AFP over TCP
-----	-----	--------------

FingBox



- Cloud-based GUI for fing
- Central Administration for multiple Networks



SNMP Managers

- Cacti
- OiDVIEW
- Manage Engine
- Nagios
- Zenoss
- InterMapper
- OpenNMS
- Observium
- MRTG - Multi Router Traffic Grapher

Tools - Subnet Calculator



- SubnetCalc or SubnetMask.info
- Endless Mask Calculations
- See ranges, see broadcast.

SubnetCalc

IP Address: 10.0.1.1 [Calc]

Address Subnets Subnets/Hosts CIDR

Subnet Bits: 16 Mask Bits: 24 Subnet Mask: 255.255.255.0

Max Subnets: 65536 Max Hosts / Subnets: 254

Subnet Host Address Range: 10.0.1.1 - 10.0.1.254

Subnet ID: 10.0.1.0 Subnet Broadcast: 10.0.1.255

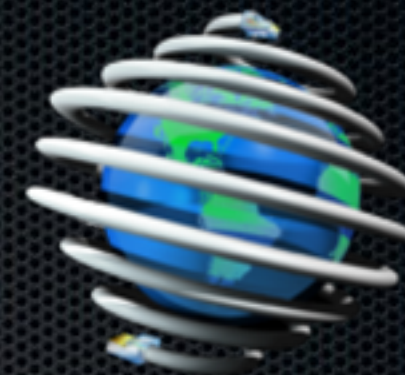
Configure IPv4: Manually

IP Address: 10.0.1.1/24

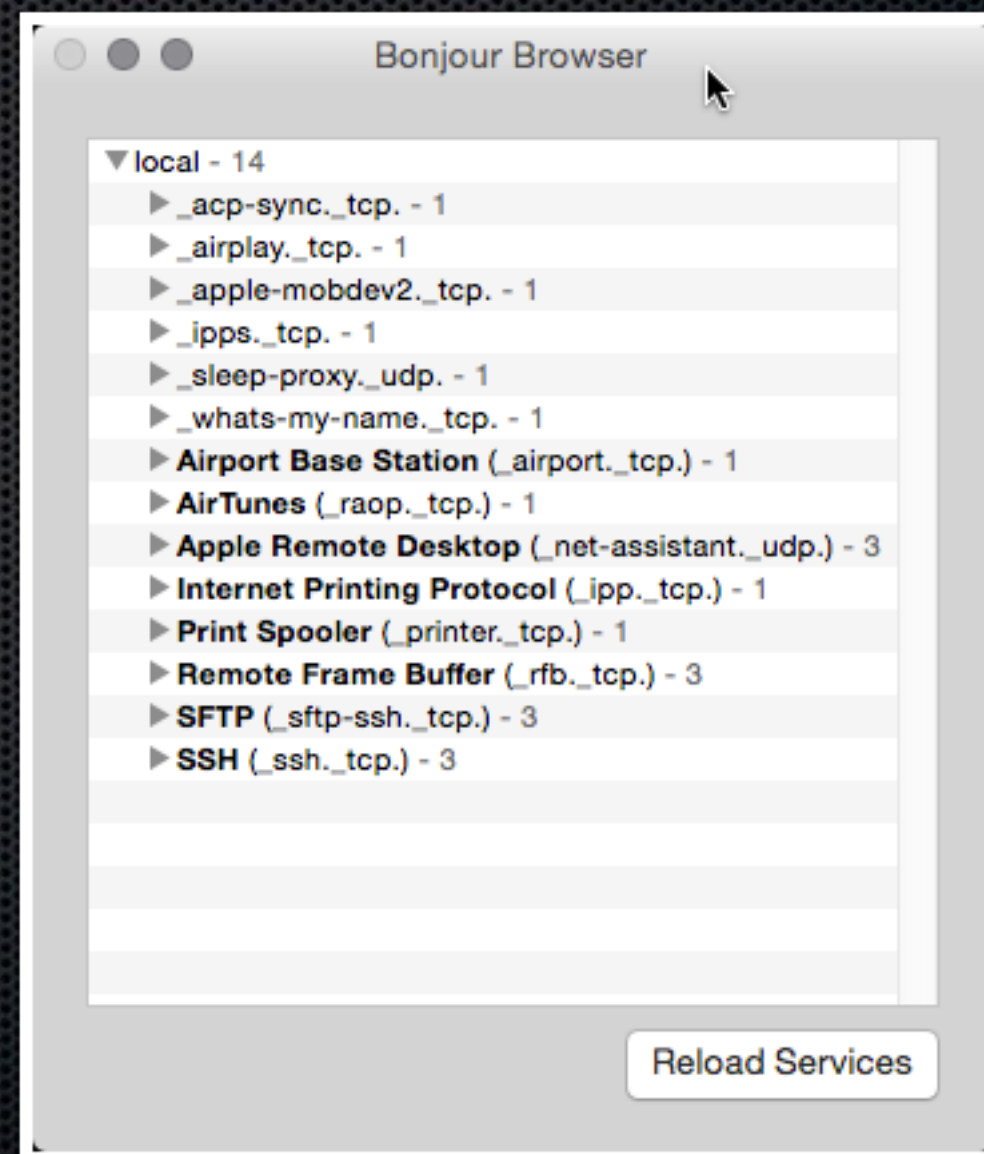
Subnet Mask:

Router:

Bonjour Browser



- Effortlessly discovers Macs and recent printers on your LAN.
- Displays great information for locating devices.
- Bring your copy & paste!



Resources

- CMAP - construct, navigate, share concept maps
- WiFi Explorer
- AngryIP Scanner

More Resources

- [Enabling SNMPv3 on OS X Server](#)
- [krypted: Configure SNMP](#)
- [Monitoring OS X Servers with Observium](#)
- [SNMP Test Utility](#)
- [NetUse Traffic Monitor](#)
- [PeakHour](#)

Questions?



Jack-Daniyel Strong
jack@spokanemac.com
@SpokaneMac