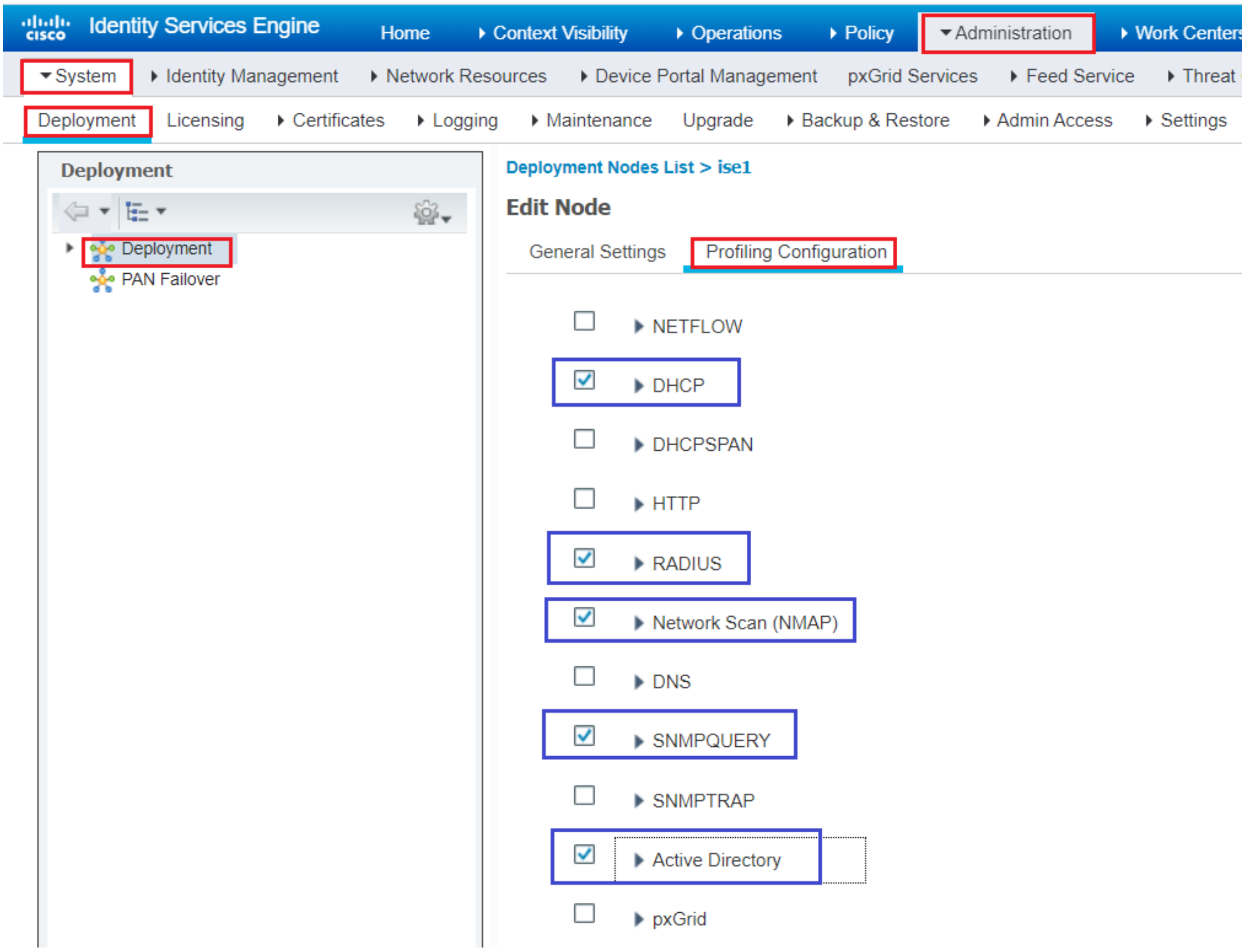
Probes Overview:

- An ISE probe is the component of ISE Profiling Services that collects endpoint attributes.
- Each probe uses different collection methods & can gather unique info about endpoints.
- Probe is method used to collect attribute or set of attributes from endpoint on network.
- By the help of Probe, Profile service collects an attribute or attributes of any endpoint.
- In Cisco ISE Probe is software designed to collect data to be used in a profiling decision.
- By the help of Probe, the Profile service create update or modify the profile in database.
- Different Probes are responsible for collection of different type of Endpoint attributes.
- There are many probes on each Policy Service Node NETFLOW, DHCP, DHCPSPAN, HTTP.
- Other probes are RADIUS, NETWORK SCAN (NMAP), DNS, SNMPQUERY and SNMPTRAP.
- The ISE probes are enabled on ISE Policy Service nodes configured for Profiling Services.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to the probes want to enable.

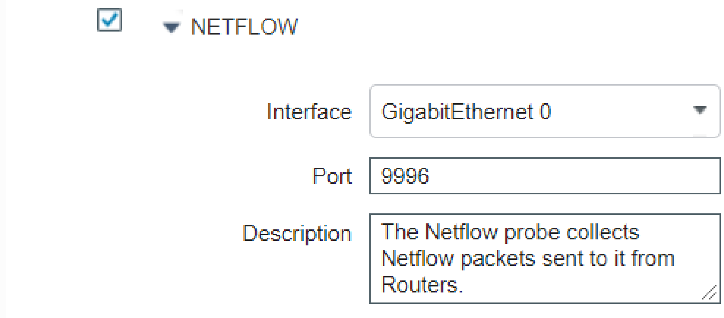


☐ NETFLOW
☑ DHCP
☐ DHCPSPAN
☐ HTTP
☑ RADIUS
☑ Network Scan (NMAP)
☐ DNS
☑ SNMPQUERY
☐ SNMPTRAP
☑ Active Directory
☐ pxGrid

NetFlow Probe:

- Just enabling NetFlow in infrastructure and forwarding it all to the Cisco ISE.
- It is recommended to perform extensive planning prior to use NetFlow probe.
- Enabling check box next to the NetFlow probe & selecting Gigabit 0 interface.
- Provides info about traffic passing through or directly to each router or switch.
- ISE NetFlow probe is cable of receiving flow records from NetFlow Version 5 & 9.
- It enabled devices to allow parsing of critical information for profiling purposes.
- NetFlow must be enabled on Devices that are in the path of interesting traffic.
- NetFlow is typically used to identify endpoints based on the traffic they generate.
- NetFlow records are based on communications between source and destination.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to NETFLOW probes want to enable.

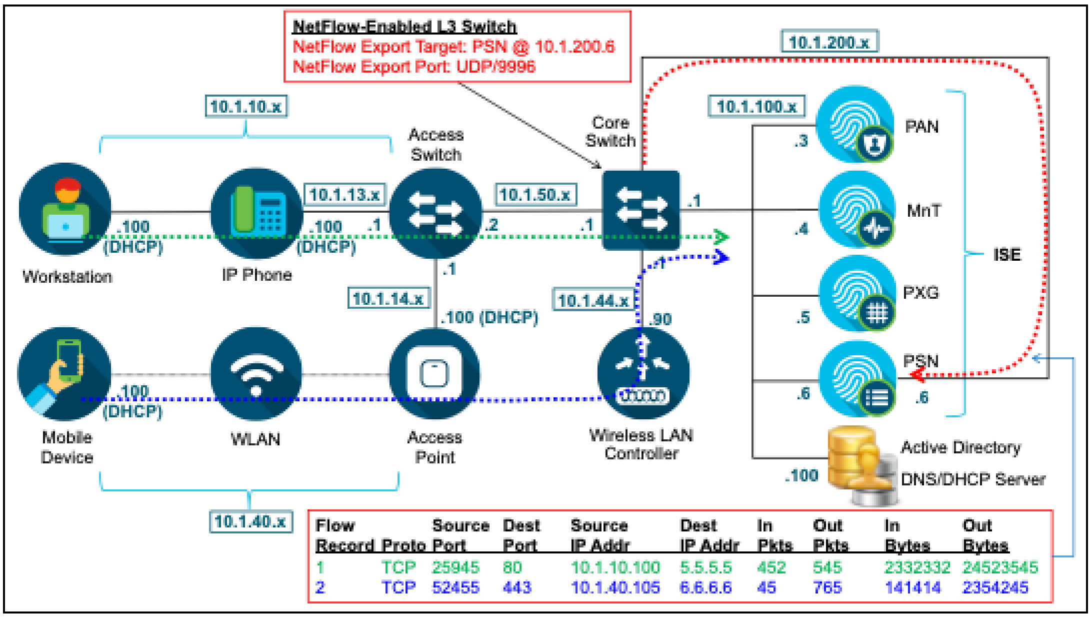


☑ ▾ NETFLOW

Interface: GigabitEthernet 0

Port: 9996

Description: The Netflow probe collects Netflow packets sent to it from Routers.



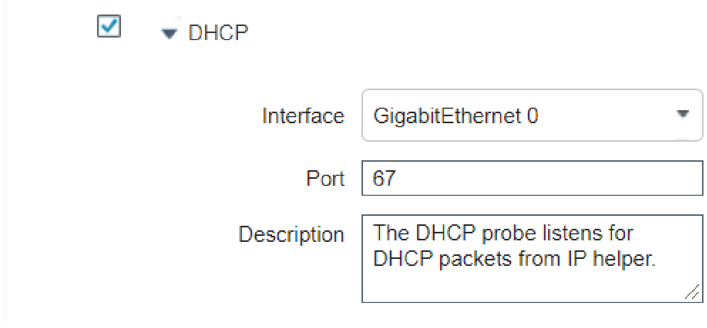
NetFlow-Enabled L3 Switch
NetFlow Export Target: PSN @ 10.1.200.6
NetFlow Export Port: UDP/9996

Flow Record	Proto	Source Port	Dest Port	Source IP Addr	Dest IP Addr	In Pkts	Out Pkts	In Bytes	Out Bytes
1	TCP	25945	80	10.1.10.100	5.5.5.5	452	545	2332332	24523545
2	TCP	52455	443	10.1.40.105	6.6.6.6	45	765	141414	2354245

DHCP Probe:

- Configuring DHCP Packets forwarding directly to the Identity Services Engine.
- The primary use of the DHCP in profiling is to capture the device MAC address.
- DHCP requests also carry User-Agent field that helps to identify OS of the device.
- The DHCP probe requires the DHCP requests to be sent directly to the Cisco ISE.
- Using ip helper-address interface configuration command to send request to ISE.
- Cisco ISE DHCP Probe collect DHCP request attribute from user, proxy and Helper.
- Identity Services Engine will only use incoming DHCP data to profile endpoints.
- Cisco ISE DHCP Probe collect DHCP request attribute from user, proxy & Helper.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to DHCP probes want to enable.

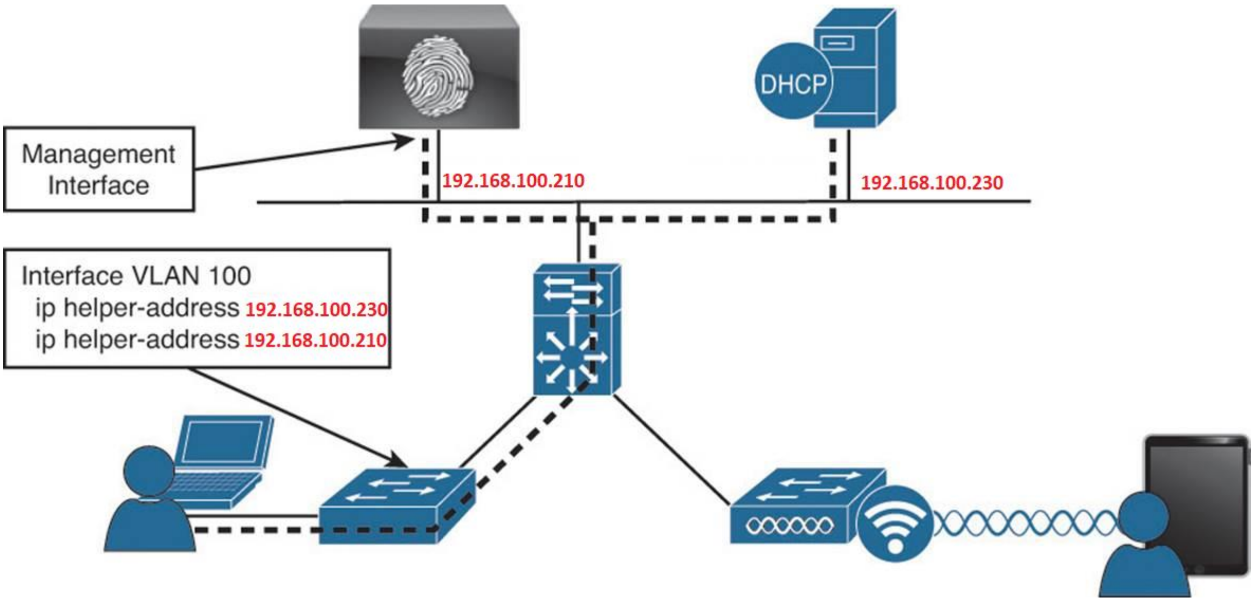


☑ ▾ DHCP

Interface: GigabitEthernet 0

Port: 67

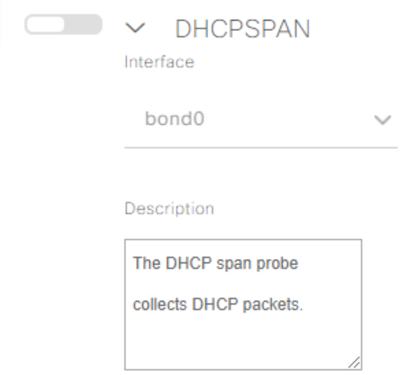
Description: The DHCP probe listens for DHCP packets from IP helper.



DHCP SPAN Probe:

- The DHCP SPAN Probe is not possible or required DHCP Relay agent to configure.
- SPAN session copies all traffic to/from source interface on a switch to a destination.
- DHCP Helper option is more preferred than SPAN because it has less traffic overhead.
- The DHCP SPAN probe is intended for use when traffic is mirrored to an interface.
- ISE Policy Service node using methods such as SPAN, RSPAN, or the network taps.
- This method is primarily used when DHCP probe using DHCP Relay is not available.
- If available, it is recommended to use DHCP probe rather than DHCP SPAN probe.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab Click the check box next to DHCPSPAN probes want to enable.

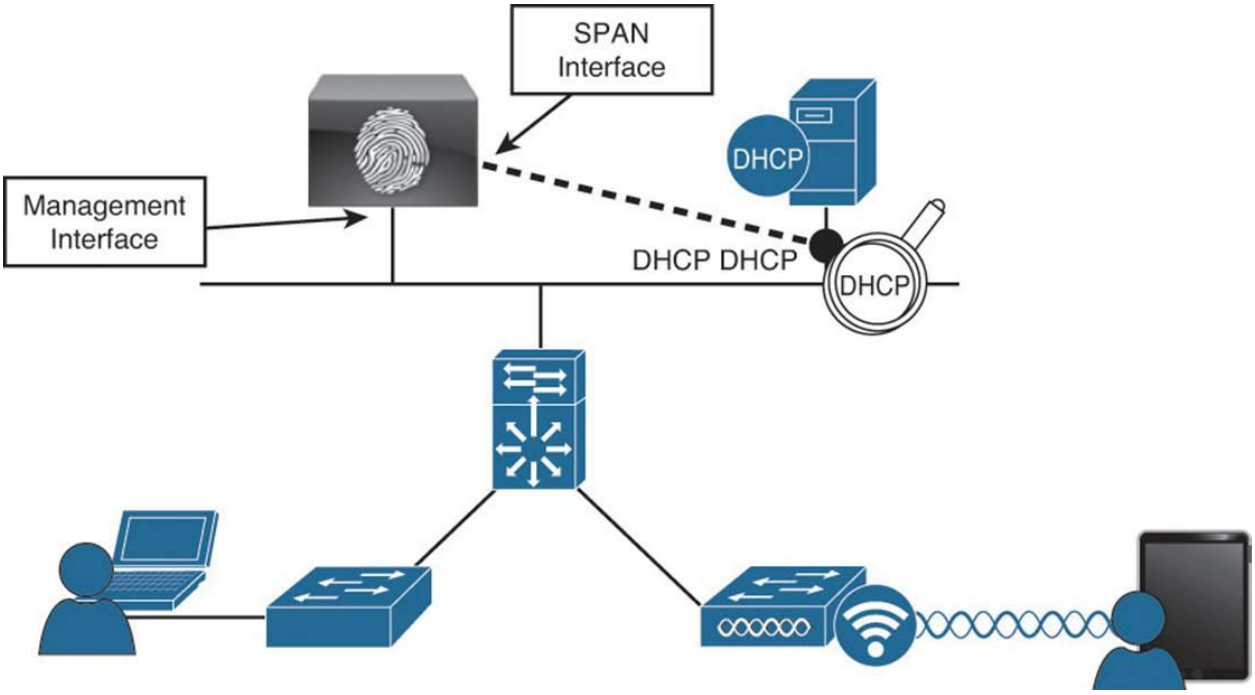

DHCPSPAN

Interface

bond0

Description

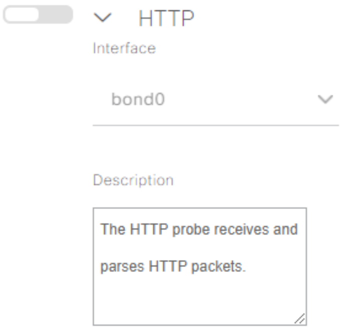
The DHCP span probe collects DHCP packets.



HTTP Probe:

- Information is transmitted in HTTP request-header field called User-Agent field.
- The Cisco Identity Services Engine uses the information in the HTTP packets.
- User-Agent field, to help match signatures of what profile a device belongs in.
- The User-Agent is the primary attribute collected using the HTTP probe in ISE.
- ISE profiling captures web browser information from the User-Agent attribute.
- Primary methods used to capture a client's User-Agent with URL Redirection.
- ISE uses URL redirection for a number of user session services includes CWA.
- Hotspot, Self-Register, Client Provisioning, Posture Assessment, and (NSP).
- During this process, it is possible for ISE to capture the User-Agent attribute.
- Use a Switched Port Analyzer (SPAN) session in true promiscuous mode.
- It listens to communications from web browsers on both TCP port 80 & 8080.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to HTTP probes want to enable.



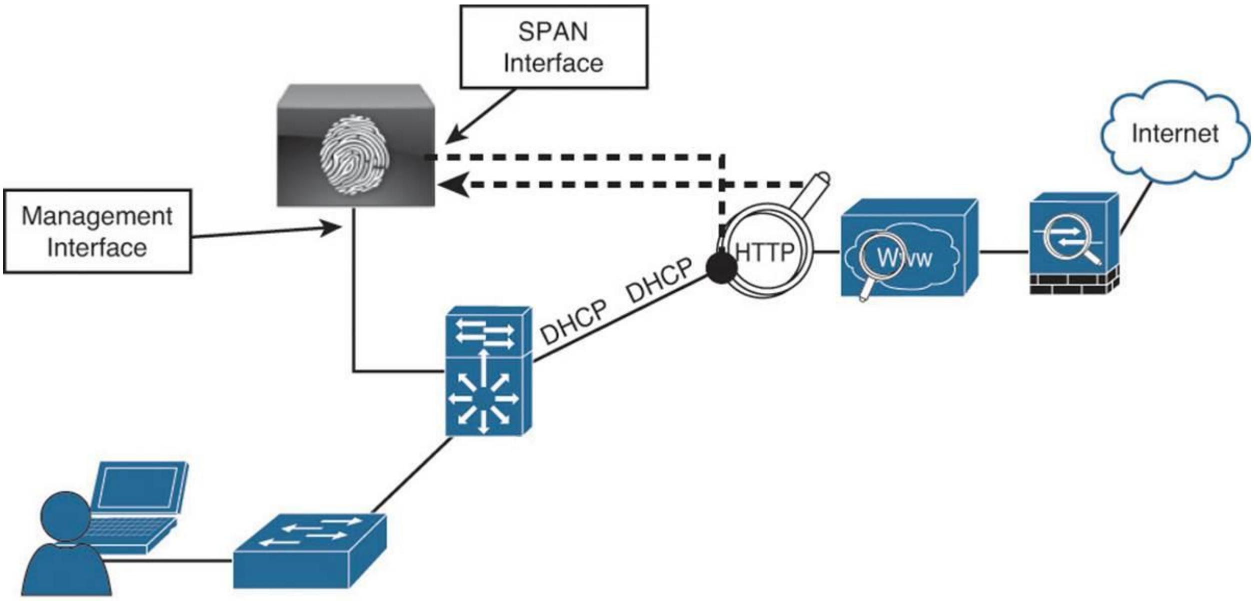
HTTP

Interface

bond0

Description

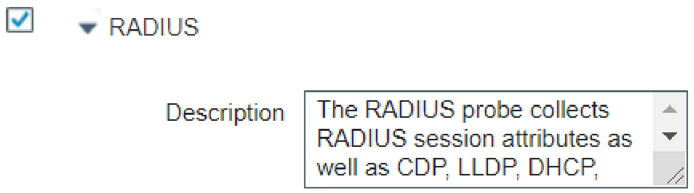
The HTTP probe receives and parses HTTP packets.



RADIUS Probe:

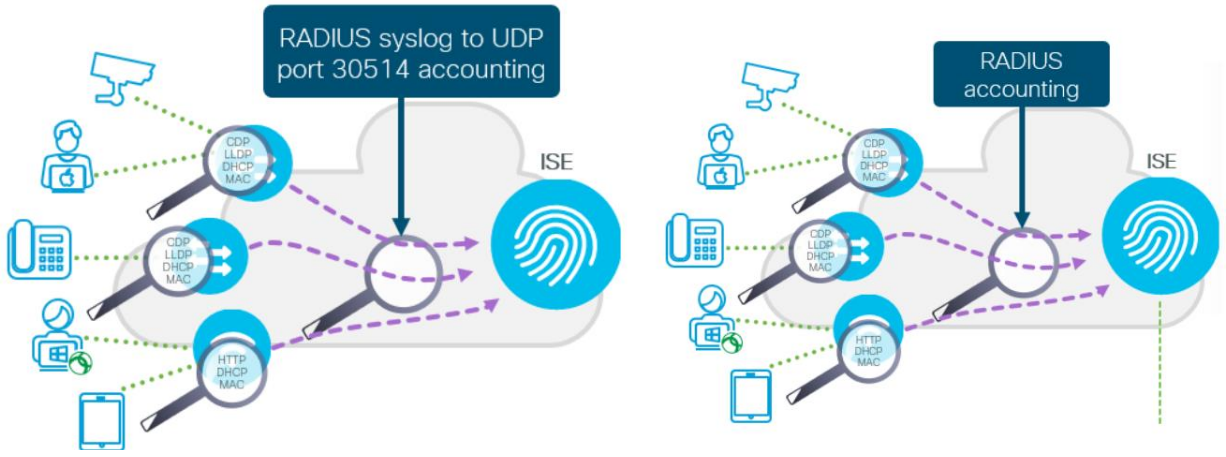
- RADIUS Probe is the most common probes using by ISE which is running by default.
- Cisco ISE profile based on RADIUS attributes collected from the RADIUS messages.
- This probe also listens to CDP & DHCP attributes send in RADIUS accounting packets.
- Such as User-Name, Calling-Station-ID, NAS-IP-Address, NAS-Port & Framed-IP-Address.
- There is a lot of more information that can be pulled from the RADIUS attributes as well.
- ISE can profile based on RADIUS attributes collected from request/response messages.
- The RADIUS probe is one of the simplest probes to enable and deploy it in Cisco ISE.
- The Calling-Station-ID field in RADIUS packet provides the endpoint’s MAC address.
- Framed-IP-Address field provides its IP address in the RADIUS accounting packet.
- RADIUS probe in Profiling is used to Collect attributes from the RADIUS Attributes.
- RADIUS Probe also collects other information like CDP, LLDP and DHCP attributes.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to RADIUS probes want to enable.



☑ ▾ RADIUS

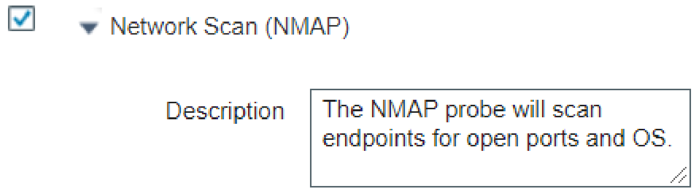
Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP,



Network Scan (NMAP) Probe:

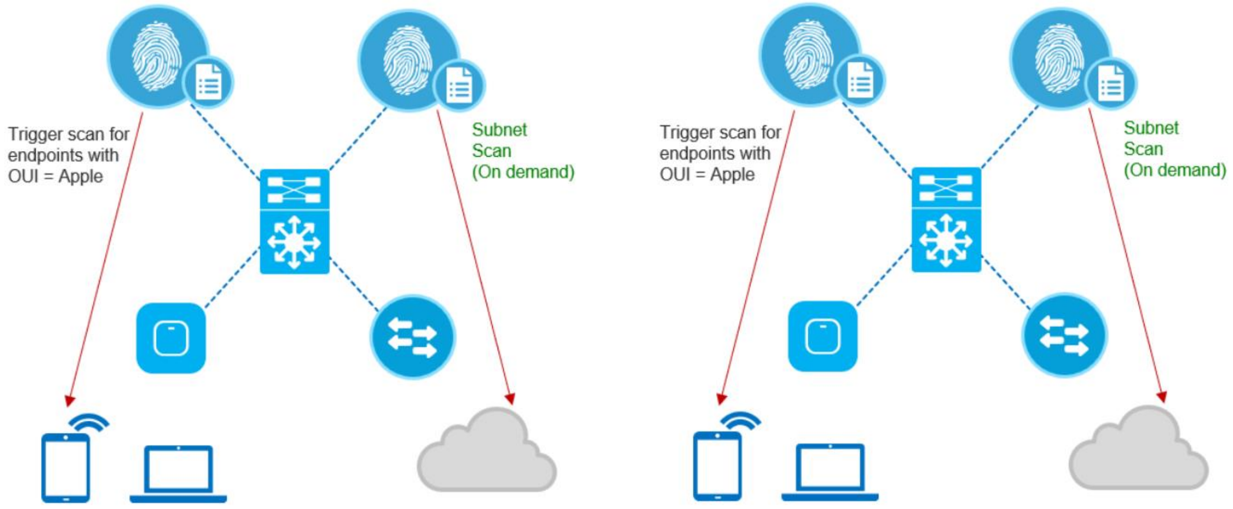
- Endpoint Scanning (NMAP) probe is executed against an IP Address or the subnet.
- NMAP is a tool uses port scans, to identity a device's OS or other attributes of device.
- Also, Endpoint Scan can run manual scan against a single node, or an entire network.
- NMAP Probe scan endpoints for open ports and Operating System to get information.
- This probe is based on an embedded version of open-source Network Mapper utility.
- Network Mapper (NMAP) is designed to scan large networks for connected endpoints.
- Perform the scans on individual hosts to detect their OS, OS version, & other services.
- The Network Scan (NMAP) probe is considered an "active" assessment mechanism.
- This is on-demand scan against one or multiple network endpoints based on IP subnet.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to Network Scan (NMAP) probes want to enable.



☑ ▾ Network Scan (NMAP)

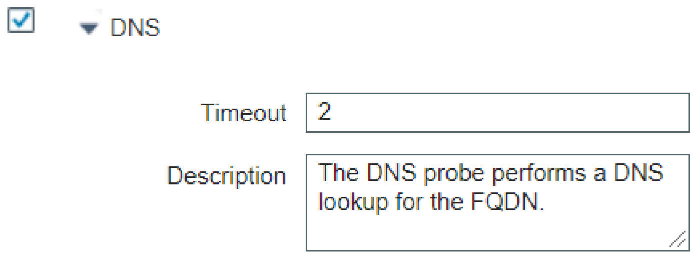
Description: The NMAP probe will scan endpoints for open ports and OS.


Trigger scan for endpoints with OUI = Apple
Subnet Scan (On demand)
Trigger scan for endpoints with OUI = Apple
Subnet Scan (On demand)

DNS Probe:

- DNS probe is used to collect the fully qualified domain name (FQDN) of endpoint.
- The DNS probe is used to acquire the DNS Fully Qualified Domain Name (FQDN).
- DNS probe cannot function unless IP address is known & associated with MAC address.
- It is useful looking for a specific DNS name format of assets Active Directory members.
- DNS probe in profiler does a reverse DNS lookup for IP addresses learnt by other means.
- DNS probe require anyone from these probe DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP.
- This allows DNS probe in the profiler to do a reverse DNS lookup against specified name.

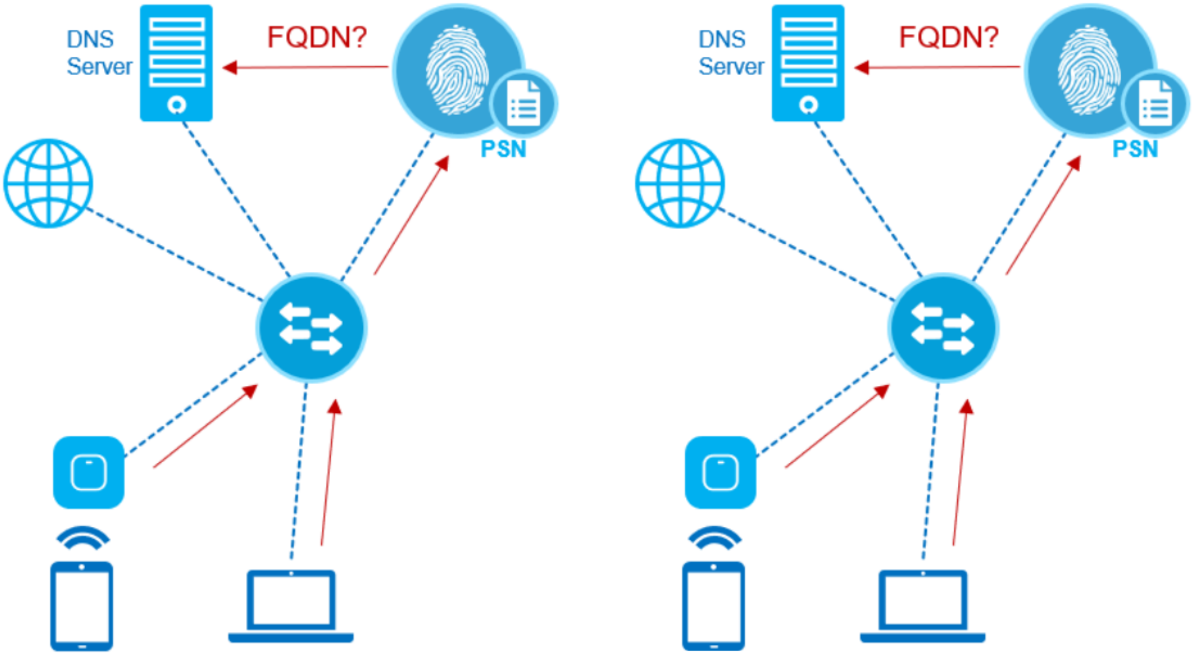
Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to DNS probes want to enable.



☑ ▾ DNS

Timeout: 2

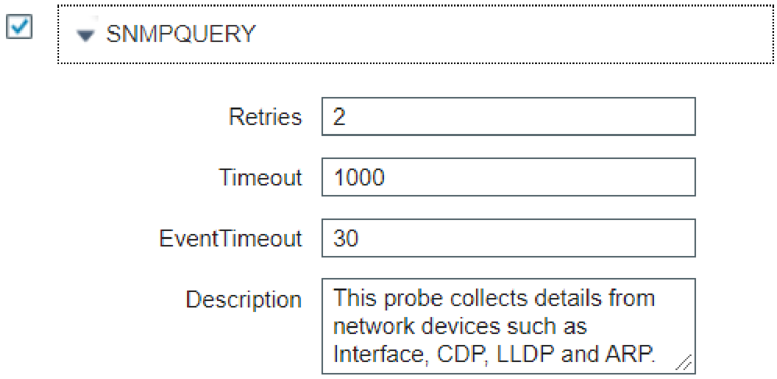
Description: The DNS probe performs a DNS lookup for the FQDN.



SNMPQUERY Probe:

- The SNMP Query Probe send query packets known as SNMP GET Requests.
- The System Queries are periodically depending upon the polling interval.
- System Queries collect Bridge, IP CDP Cache Entry LLDP Local System Data.
- The Interface Queries are generated when the RADIUS Accounting Starts.
- Interface Queries are generated when SNMP detect linkup or MAC Trap.
- The network device must be configured to accept the SNMP requests.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to SNMPQUERY probes want to enable.



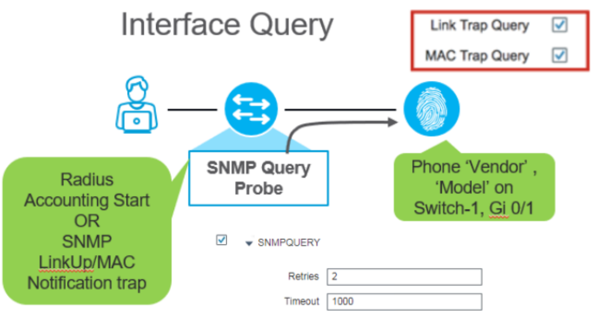
☑ ▾ SNMPQUERY

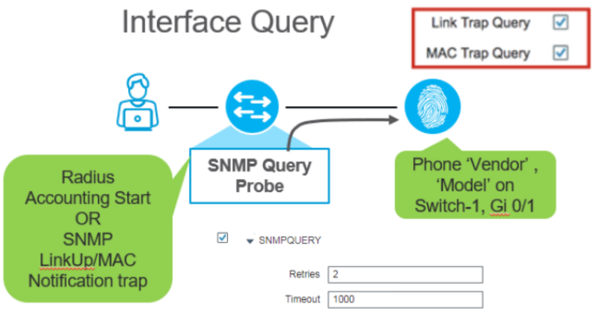
Retries: 2

Timeout: 1000

EventTimeout: 30

Description: This probe collects details from network devices such as Interface, CDP, LLDP and ARP.

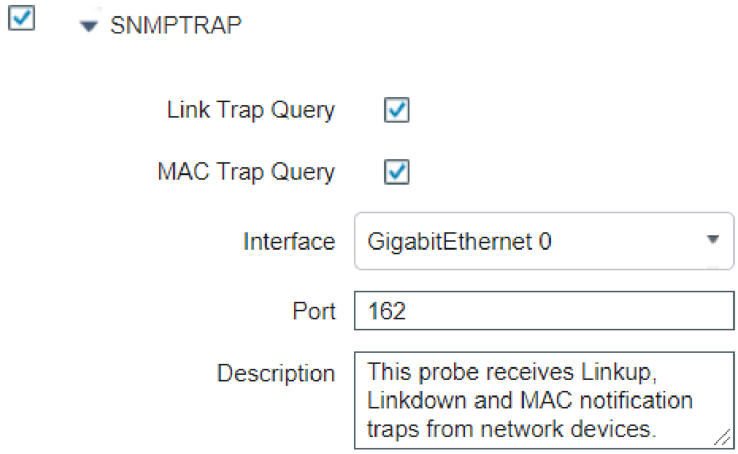

Interface Query
Link Trap Query ☑
MAC Trap Query ☑
Radius Accounting Start OR SNMP LinkUp/MAC Notification trap
SNMP Query Probe
Phone 'Vendor' , 'Model' on Switch-1, Gi 0/1
☑ ▾ SNMPQUERY
Retries 2
Timeout 1000


Interface Query
Link Trap Query ☑
MAC Trap Query ☑
Radius Accounting Start OR SNMP LinkUp/MAC Notification trap
SNMP Query Probe
Phone 'Vendor' , 'Model' on Switch-1, Gi 0/1
☑ ▾ SNMPQUERY
Retries 2
Timeout 1000

SNMP Trap Probe:

- SNMP Trap receives information from configured NAD support MAC notification.
- SNMP Trap receives info form configured NAD support linkup, linkdown & informs.
- For SNMPTRAP to be functional, you must also enable the SNMPQUERY probe.
- To make this feature functional, configure the NAD to send SNMP traps or informs.
- SNMP Trap probe receives information from the specific network access devices.
- When ports up or go down & endpoints disconnect from or connect to network.

Navigate to Administration > System > Deployment > Select the Profiling Configuration tab
Click the check box next to SNMPTRAP probes want to enable.



☑ ▾ SNMPTRAP

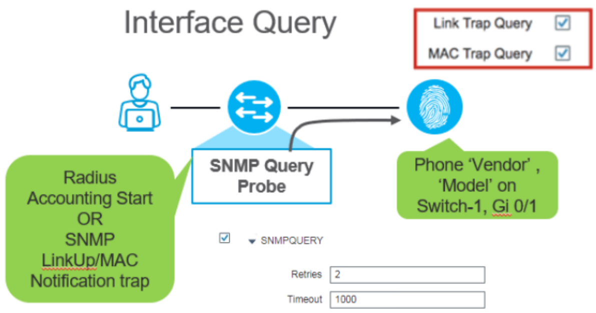
Link Trap Query ☑

MAC Trap Query ☑

Interface: GigabitEthernet 0

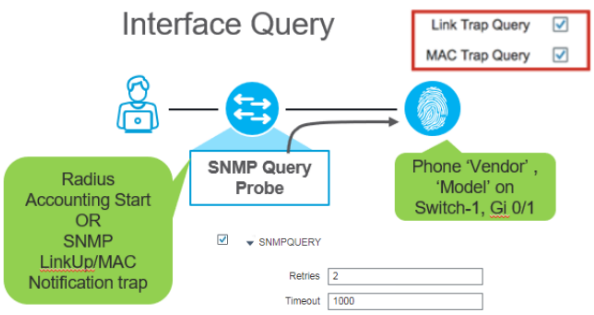
Port: 162

Description: This probe receives Linkup, Linkdown and MAC notification traps from network devices.


Interface Query
Link Trap Query ☑
MAC Trap Query ☑
Radius Accounting Start OR SNMP LinkUp/MAC Notification trap
SNMP Query Probe
Phone 'Vendor' , 'Model' on Switch-1, Gi 0/1
☑ ▾ SNMPQUERY

Retries 2

Timeout 1000


Interface Query
Link Trap Query ☑
MAC Trap Query ☑
Radius Accounting Start OR SNMP LinkUp/MAC Notification trap
SNMP Query Probe
Phone 'Vendor' , 'Model' on Switch-1, Gi 0/1
☑ ▾ SNMPQUERY

Retries 2

Timeout 1000