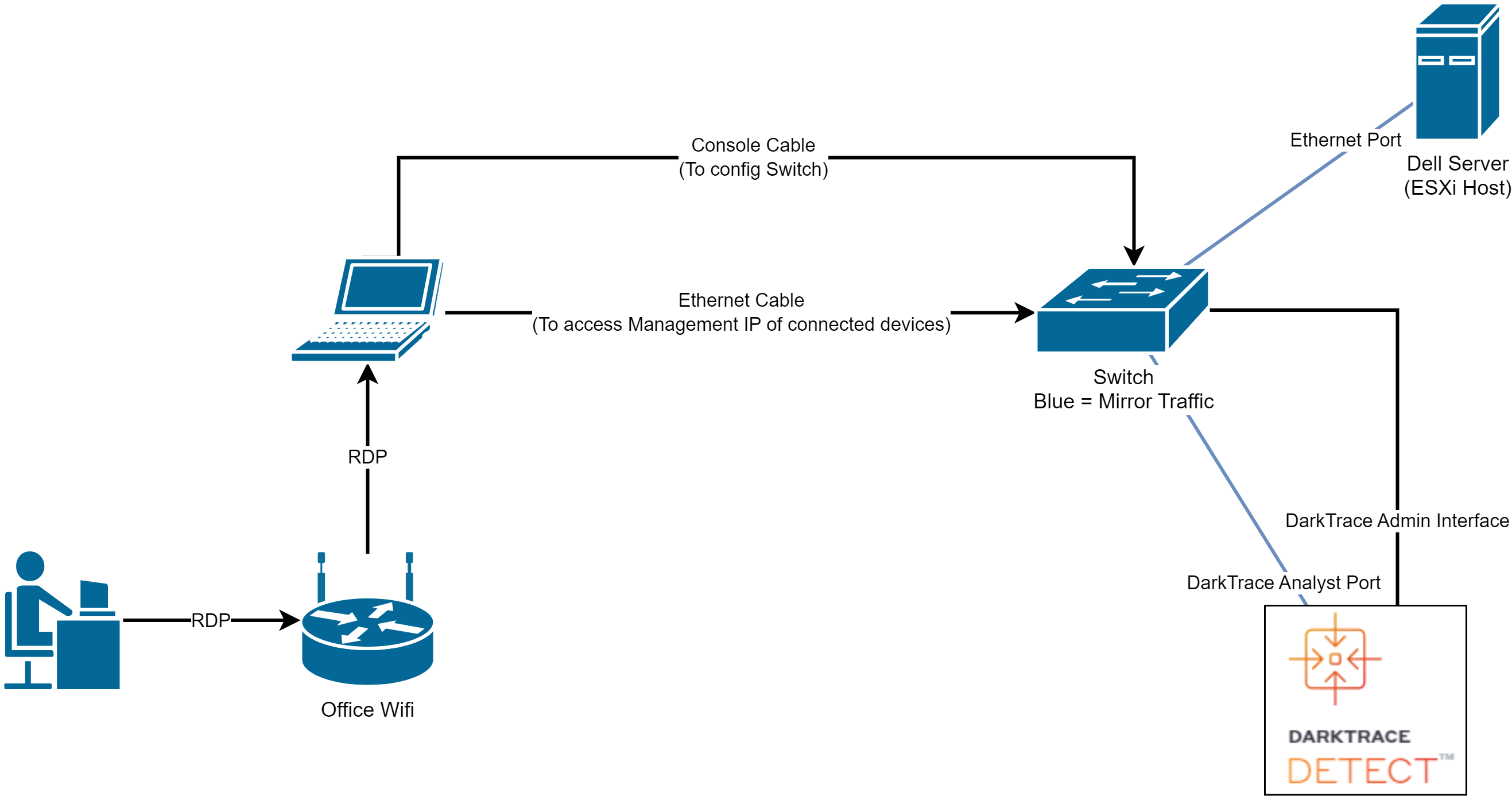
Roadmap

Thursday, May 25, 2023

11:44 AM

1. Cisco Switch [Page 2]
   1. Access Cisco CLI (Console cable/SSH)
   2. Check status & Configure port mirroring
2. DarkTrace [Page 9]
   1. Try to access the DarkTrace UI.
   2. Check if traffic has arrived
3. Dell Server [Page 11]
   1. Try to Generate some traffic
   2. Packet sniffing (Optional)

# Diagram of my test situation, for reference:



Cisco Switch: Configure port mirroring

Thursday, May 25, 2023

2:41 PM

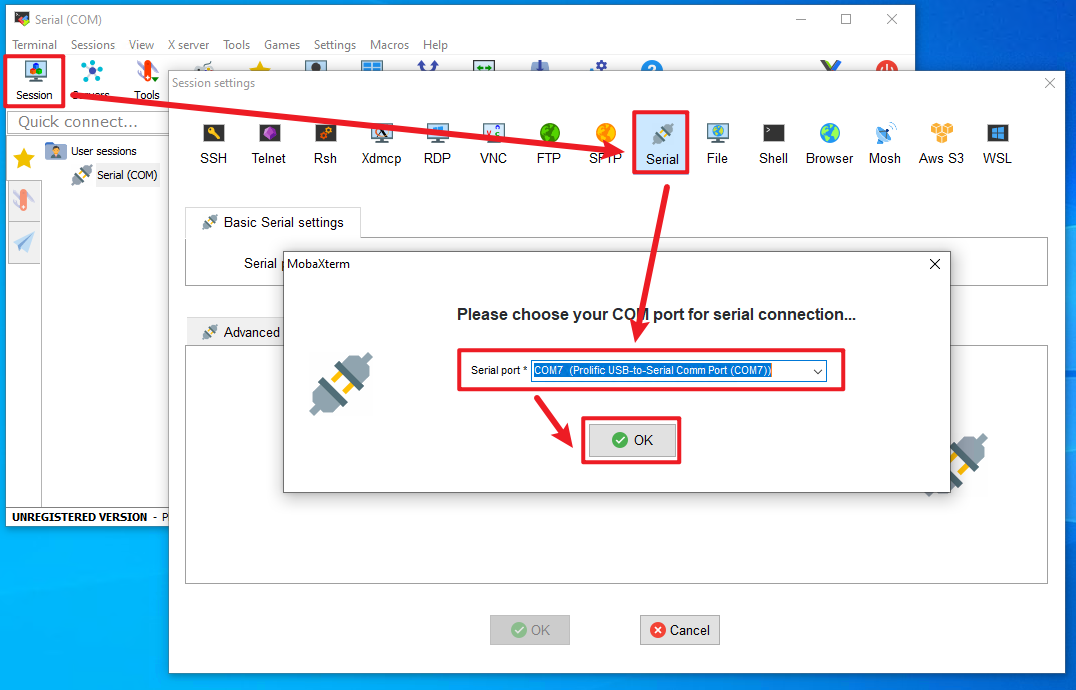
# How to Connect a console cable

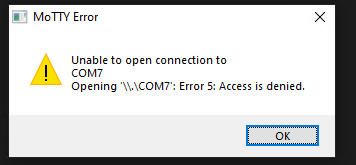


[What Are Console Cables and Why Do I Need Them? (cablesandkits.com)](https://www.cablesandkits.com/learning-center/what-are-console-cables-why-need-them)

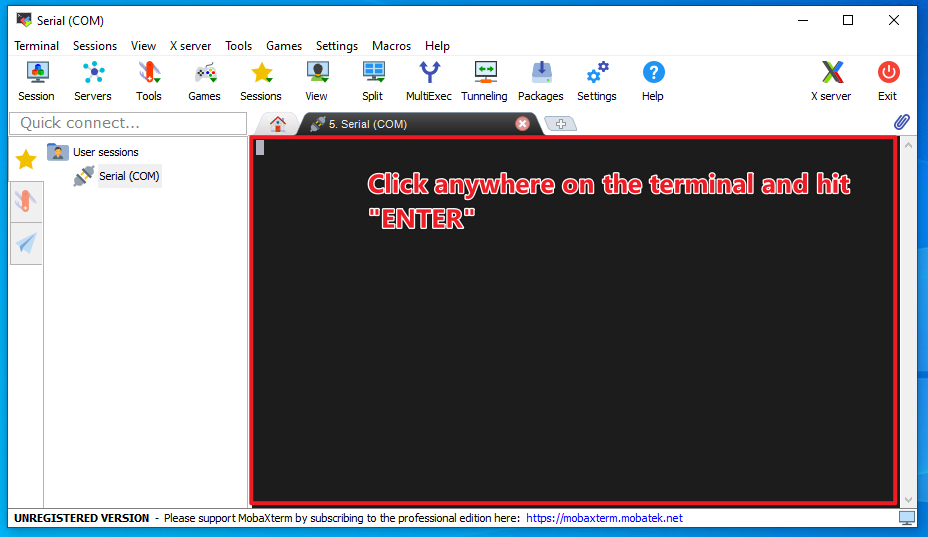
# Access Cisco CLI

After connected the console cable from Switch to the computer, open MobaXterm and establish a Serial session.

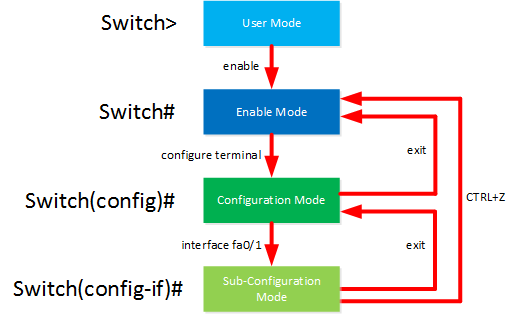




You may see an error message, but we can ignore it.



# General Guide (Skip if you know Cisco CLI)



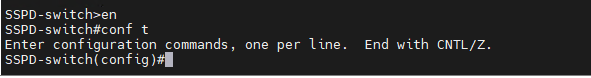
1. Check the above diagram for how to switch across three different modes of Cisco devices.
   1. In short, Enable mode allows us to READ settings only, Config mode allows us to WRITE settings only.
   2. In config mode, we can also READ by attaching "do" at the start of the Enable mode command. (Has a few exceptions like "copy run start").
      1. i.e., do show interface (If you see "do" , you know that "show interface" is an enable mode command)
2. You can Use Ctrl+Shift+6 to interrupt most commands.
3. Press "?" at anywhere if you need to see a list of possible commands.

# Now let's Start with exploring the switch port/interface status!

Enter config mode by typing the below: (Those are abbreviations that the CLI can recognize)

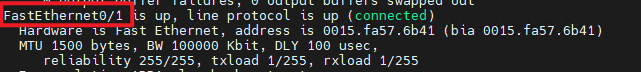
en

conf t



Check all interface status. You may hit SPACE to see more lines. If you want it to stop, press "Ctrl Shift 6" or Right arrow or Ctrl C.

do show interface





We can see that the FastEthernet 0/1 (DarkTrace) and 0/24 (Dell Server) are up.

FYI, the abbreviation for these two ports are: fa0/1 fa0/24

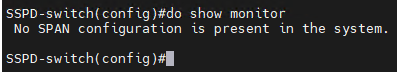
# Configure Port Mirroring (aka. Port Monitoring)

Ref: [How to configure port monitoring (SPAN) on a Catalyst 2940, 2950, 2955, 2970, 3550 or 3750 series sw... - Cisco Community](https://community.cisco.com/t5/networking-knowledge-base/how-to-configure-port-monitoring-span-on-a-catalyst-2940-2950/ta-p/3132032)

[Catalyst Switched Port Analyzer (SPAN) Configuration Example - Cisco](https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html#anc3)

Check if there is any port mirroring config in the system.

do show monitor

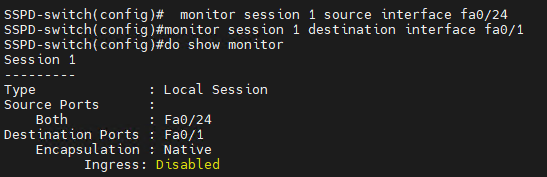


Configure source port for mirroring (Dell Server). This is the device being mirrored its traffic.

monitor session 1 source interface fa0/24

Configure destination port for mirroring (DarkTrace). This is the device that receives the mirrored traffic.

monitor session 1 destination interface fa0/1



Lastly, the two devices need to be in the same VLAN and have same access mode, use the below to find out:

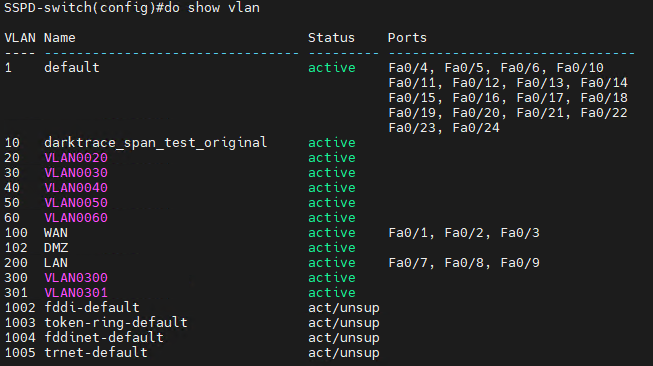
do show running-config





If you don’t see any setting for this port, this means that fa0/24 is connected to default VLAN and using default mode.

do show vlan



Unfortunately, above screenshots suggest that the Fa0/1 that connects DarkTrace actually belongs to the "WAN" VLAN (id:100)!

We need to change Fa0/1 from WAN to default VLAN. It is not required to be the same as Fa0/24, we just don't want it to be WAN to be safe.

# Configure port mode

Make sure you are at the config mode and type the below to enter sub-configuration mode. This allows you to perform interface settings (config-if):

interface fa0/1

Then please type below code in the screenshot:



We also want fa0/24 to use the "access" mode rather than default mode (dynamic desirable).





# Final Checking

You may run the below to do some **Final Checking** before we apply configuration:

do show vlan (Check VLAN allocation)

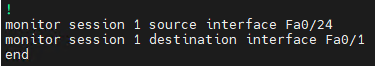
do show interface switchport (Check switch port mode)

do show running-config (Check all current settings in RAM)

As shown in "do show running-config" output, they are now both connected to default VLAN, and mode set to access. We can also see our monitoring settings.







# Saving the Configuration

Exit the config mode into enabled mode.

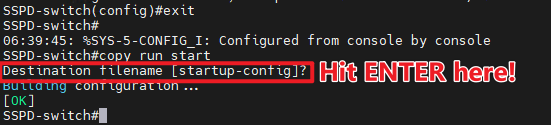
We must apply the settings by writing the running-config (RAM) to startup-config(ROM). And we must do it in Enable mode only.

Ref: [How to Manage and Save Running Config on Cisco Devices (netwrix.com)](https://blog.netwrix.com/2019/09/10/how-to-manage-and-save-running-config-on-cisco-devices/)

If you are still in config mode, you need to:

exit

copy run start



# Additional Information

For switch port monitoring, the source and destination ports can be in different modes, but there are some considerations to keep in mind:

Source Port:

The source port, from which you want to copy the traffic, can be in either access or trunk mode.

1. In access mode, the port will copy the traffic of a specific VLAN.
2. In trunk mode, the port will copy the traffic of multiple VLANs.

Destination Port:

1. The destination port, where you want to send the copied traffic for monitoring, should typically be in access mode.
2. The destination port does not participate in any VLANs but serves as the endpoint for receiving the copied traffic.

# Cisco Enable/Config/Config-if mode Abbreviations

en

conf t/m/n

int fa0/1

DarkTrace: Validate port mirroring

Monday, May 29, 2023

10:56 AM

# Finding the Management IP

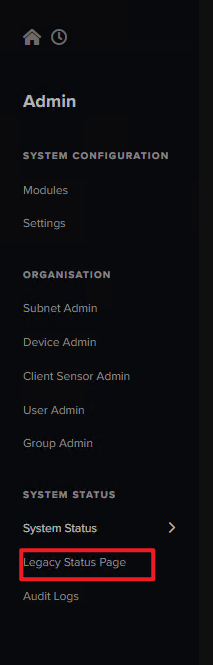
1. Connect Monitor (VGA) and Keyboard (USB-A) to the DarkTrace device
2. Login the local console using the credentials. Default username is "console". You will see the screen "Console Setup".
3. Select "Networking and Traffic Analysis"
4. Select "Configure network interfaces"
5. Select the interface with "Management" notation. It is usually eth0. If there is no “Management”, you might want to allocate one interface to be management.
6. Then you will be able to see the Management IP. If it is 0.0.0.0, you need to manually configure an IP.

# 

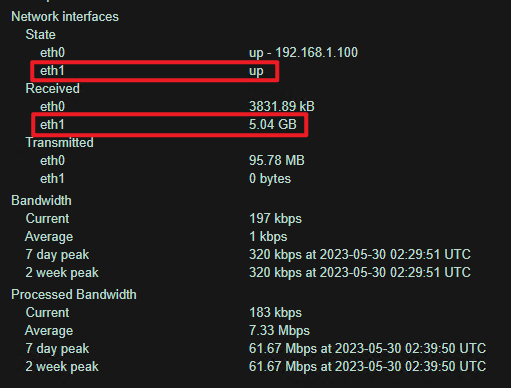
# Check DarkTrace interface status

Login to DarkTrace Web UI (Threat Visualizer) using the Management IP on any browser.

Go to Admin - System Status - Legacy Status Page

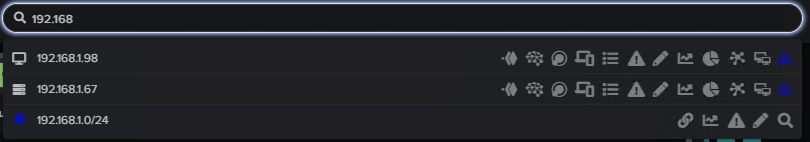


Scroll down and check the Network Interface statistics. You would need to look at the interface other than eth0 (which is the Default Management interface)

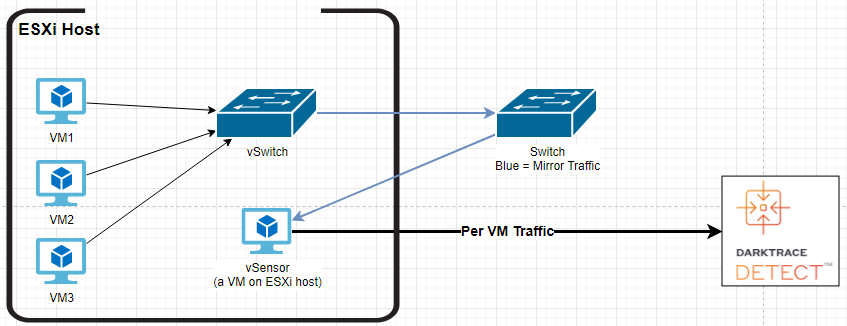


# Alternative Methods

1. You can also check more info by searching the device IP



1. You can also inspect interface stats on the local "Console Setup" when you are **Finding the Management IP**.
   1. Login the local console
   2. Select "Networking and Traffic Analysis"
   3. Select "Interface stats"
2. Use vSensor to receive mirrored traffic, then check it using Advanced Search in DarkTrace UI.



# Suggested actions to generate some traffic

1. Upload an ISO from the laptop to the ESXi datastore, and check traffic on DarkTrace.
2. Use the laptop to ping the Dell Server and see if DarkTrace can get it.

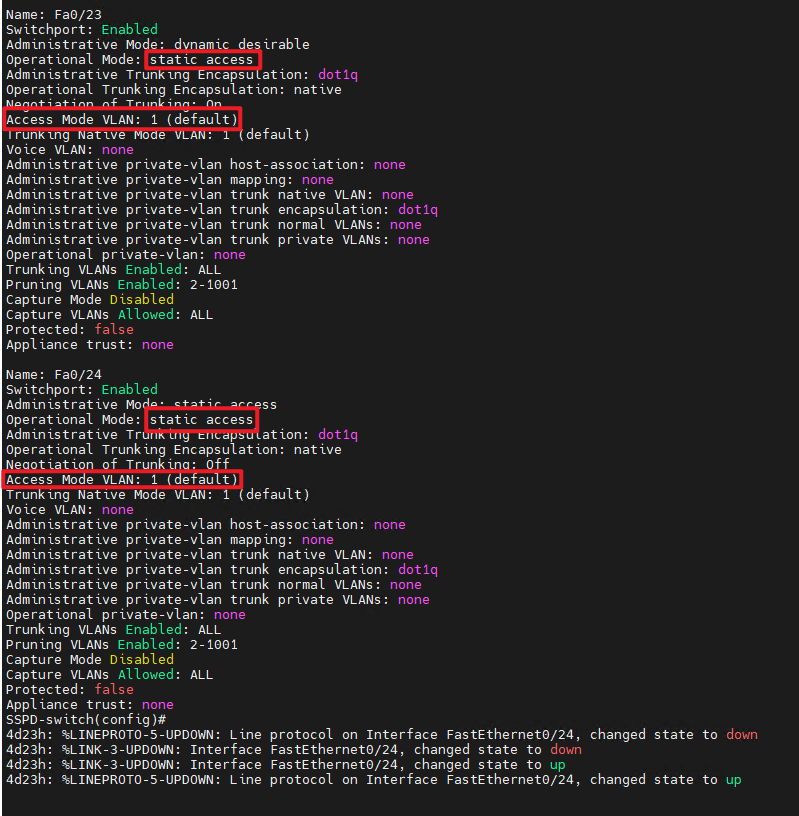
# Additional Information

## Configure Dell Server via Switch

If the Dell Server is in a disconnected network and you want to use your PC to configure the Dell Server via the switch, they need to be in the same VLAN and have switchport mode set to default / access.

Enter enable mode, and run the below:

show interface switchport



If they are not in same VLAN, or having switch port modes other than access/default, change the settings according to "Cisco Switch" section.

## Check ESXi connectivity

