1. **NDG Networking Labs - TCP and Virtual Routing**

**Preparations**

The preparations for doing the lab exercises are for all exercises the same steps:

1. Loading the lab configuration (A virtual machine on the NDG platform)
2. Log in to a Client
3. Open the chrome Bowser
4. Open the login menu of the firewall (with the firewall IP address)
5. Log into the firewall
6. Load the appropriate firewall configuration file for this exercise
7. Important> with the commit command of the FW the file will be transmitted and loaded into the firewall

**Port definition in the firewall**

After this work had be done, the exercise starts with a test of the configuration:

From the client we try to reach the ethernet Interface 192.168.1.1 with the **Ping** command of the windows Operating system.

This test failed, because we have not yet configured the firewall.

So first we had to configure the NIC interface of the firewall.

We select ETHERNET 1/2 (Interface card one, second port) and gave this port the layer 3 connectivity availabilities. With the definition of the port for a layer 3 connection, we are able to configure an IP Address, can assign a zone and can assign a virtual Route to the port. We gave the port the ethernet address 192.168.1.1/24. also we allow management for this port. e.g. to accept the ping command.

Finishing with the obligate commit command the configuration is stored and activated in the firewall for port ethernet 1/2.

**Virtual Router activation**

In the **Network>Virtual Router** Window of the firewall Admin console we add a virtual Router VR-1.

With adding ethernet 1/1 and ethernet 1/2 to the virtual router VR-1we have two network segments between now traffic can be routed in both directions. (An IP Address was already configured in earlier steps to the ports of the board). We also have to configure a static route and add a gateway of last resort.

After having committed the configuration we get no longer warnings from the commit status windows. So, the configuration should work

**Verify Network connectivity**

As final step we have to verify that the configuration will work.

Via the client log in, we again try to reach the address 192.168.1.1 and see on the screen, that the ping now did not fail. From a separate CMD window we also can log in to the firewall admin port 192.168.1.1

**Learnings**

There 3 main points, I can mention:

1. Ping command

Ping is a network utility used to test the reachability of a host. The ping command is very important test tool. This tool we help a lot in daily work of a cybersecurity specialist.

1. Configuring a virtual router on a firewall  
   this is be daily work of a network specialist and a must know of a cybersecurity specialist
2. Verifying a configuration   
   I think that is a must in the daily work. Everything a specialist configures has to be verified, to be sure, the configuration works in the right manner.

.

1. **NDG Networking Labs - Configuring DHCP**

2.1 **Configure a DHCP Server**   
After having set up of the lab environment as described above in step **Preparations** **a-g** we are going to the main point this exercise: **Configuring a DHCP Server.**

A DHCP Server administrated the IP addresses of a network. To communicate inside/outside a network segment, clients need an IP Address. The DHCP server manage this within a network. The alternative to a DHCP Server is to configure every client in a network with a fix address.

To activate DHCP in a network segment we first configure a DHCP server in the palo alto firewall for the Ethernet 1/2 port/segment with the **enable** command. Second, we have to configure the lease, e.g. in this exercise 2 days. That means, every two days the computer will get a new IP Address. Third we need to configure an adequate range of IP Addresses which suits to the network configuration, e.g. 192.168.1.100 – 110. In this configuration we have a DNS address 8.8.8.8 which is the google DNS Server. Every client will have this address too in his configuration from the FW DHCP Server.

The commit command in the FW will bring this configuration to work.

2.2 **Configure Client for DHCP**   
Then we also have to configure the client with the adequate functions (obtain an ip address automatically) in the Operating system, here Windows. First, we verify the client’s configuration with the command: ipconfig /all. We can now see what is configured. We see that DHCP is disabled, so we have to enable DHCP. We do this in the control panel> Network and sharing center>change adapter settings>internal. There we choose the point Internet protocol Version 4 and click properties: choose: obtain an IP address automatically/obtain an DNS Address automatically. With the click to ok we have enabled the DHCP Server of the firewall, and the client will obtain an IP address automatically. Even so the DNS address and the lease time.

We verify these settings with the ipconfig/ all command and see the change of the settings.

2.3 **DHCP Client Reservation**

We are also able to give a client a reserved IP Address. Therefore, we have to notice the MAC address of the client. We do this job in the DHCP Server window of the firewall. We add the IP address 192.168.1.51 and the MAC address: 00:50:56:8a:0d:49 and click ok and commit. We verify this changes on the client with the ipconfig/release and ipconfig /renew.

* 1. **Configure the firewall Outside Interface for DHCP**

A lot of Internet providers are working also with a DHCP Server. So we need to be able to configure the firewall *outside Side* with this function to get a an IP address from the provider.  
Therefore we use on the firewall the network>interfaces>Ethernet administration window and activate to the Ethernet 1/1 the point DHCP Client. This will make the firewall to a DHCP Client on the outside connection. We verify this configuration change on the interface with a double click to IP Address of the Interface. A separate window (Dynamic IP Interface Status) shows us the obtained IP address in this case: 203.0.113.51.

**Learnings**

We learned the different options available with the DHCP configurations and the necessary steps, both: on the firewall side and the client side. These all are basic knowledge of the network configuration possibilities and needs for network administrator and to a cybersecurity specialist. He needs this to have a basic understanding how a network works.

1. **NDG Networking Lab - Virtual Addressing**

3.0 First, I had to set up the Lab configuration with the steps **a-g** see point one.

* 1. **Configuring a virtual IP Address**

The second step is to configure a virtual IP address. Configuring a virtual IP address means, to give a physical Ethernet port an additional (virtual) IP address, for the communication with multiple IP networks.

Before starting the configuration work, we make a test with ping and try to reach the 192.168.20.1 (the planned virtual IP address). It is clear, that we cannot reach this address by the ping command, because it isn’t configured yet.

In the firewall administration window, we go to **Network>Interfaces>Ethernet>Ethernet 1/2** and add the new virtual IP address 192.168.20.1/24

With the ping command 192.168.20.1 we now receive replies form 192.168.20.1, because is a virtual network on the firewall. (Verification process of the done configuration changes).

Next step is to change the virtual IP address on the physical ethernet interface 1/2 from 192.168.20.1/**24** to 192.168.20.1/**29.** We also need to change the clientconfiguration in the windows operating system (control panel>network and sharing center> change adapter settings >internal>properties and Internet Protocol Version 4 >properties >use the following IP address from 192.168.1.20 to 192.168.20.20 and the default gateway to 192.168.20.1.

To verify the settings, we use a ping command to 192.168.20.1. We will get an answer “request timed out”, because the address 192.168.20.20 is out of range of the IP address range 192.168.20.0/29. The range only could be 192.168.20.0 – 192.168.20.7 being the **.0** for network address and **.7** the broadcast address. Available IP addresses only from 192.168.20.**1-.6.**

Now we change the client settings to IP address 192.168.20.6 the subnet mask to 255.255.255.248 and verify the configuration with a ping command to 192.168.20.1 and will get a reply from the 192.168.20.1. We get a response, because the IP address now is in the same range as the firewalls virtual IP address.

**Learnings**

In this lab I learned the meaning of a correct IP addressing and the possibilities of a firewall (virtual IP address on a physical board) beside the client setting work in windows operating system. These all are basics to a cybersecurity specialist work and knowledge.

1. **NDG Networking Lab - Creating Packet** **Captures**

4.1 After having set up of the lab environment as described above in step a-g we are going to the main point of the exercise: **Create a Wireshark packet capture.**

4.1 **Create a Wireshark Packet Capture**

Wireshark is a powerful tool to analyze network traffic e.g. from a client ‘s network interface, the use in this lab case. This tool is a most have for every network or security specialist.

After having started Wireshark on the client PC we select the internal interface in the Wireshark window and choose **Capture>Start**.

After having started the capture of packets we open chrome and generate a request to a website in the browser ([www.panlabs.com](http://www.panlabs.com)).

If the website has been opened in the browser, we wait 5-10 seconds and then change to Wireshark to press the stop capturing packets button from the capture window in Wireshark.

After having saved the captured packet file we can start examining the file. Main part of analyzing the file is the recognition of the following *steps* in the IP traffic communication process and the belonging steps in IP communication like ACK, Syn etc.:

Protocols we see in the captured files are: ARP Protocol, DNS Request, TCP Traffic, HTTP Traffic.

These are he most common protocols within the IP Traffic.

**Learning:**

First look to the Wireshark tool, examples of Protocols and Internet traffic like ARP,DNS, HTTP, TCP Traffic.

1. **NDG Networking Lab - Analyzing Packet Captures**

First, I had to set up the Lab configuration with the steps a-g see point one.

Second step is to create a packet capture on the firewall. The captured file then has to be downloaded to the client for inspection/ analyzation. On the Administration Window of the firewall we go to **Monitor>packet capture** and click **add** to create a packet capture stage. In the packet capture stage window, we choose from the stage field firewall and name the file pcap-1. In the configure Capturing window of the firewall we turn packet capture on.

We have to notice, that there is a warning, that in real life or action of a firewall this packet capture can have dramatically influence to the performance of the firewall.

In the chrome browser we then open [www.panlabs.com](http://www.panlabs.com). After having opened the website we change back to the packet capture window and stop the capturing. After saving the file on the desktop, we can open it with a double click, because the file will be opened with Wireshark automatically.

First, we have a lock in the DNS protocol. We see that a standard query was direct to the client connected DNS server. In this lab case the DNS Server is located in the DMZ Zone. The standard query is asking for the A record of the DNS protocol.

The DNS Server answers with the IP address where the Web Server is located. With this information the client can start to request a connection to the web server with the 3 way TCP handshake.

Next, we can see the 3-way TCP handshake for setting up to the connection client to Webserver. First the client sends a TCP packet with the flags SYN, ECN, and CWR in the header to the destination (Web Server in the DMZ Zone). This establishes a SYN packet along with the window size information. Second step of the 3-way handshake, the DMZ Server (with the Web Server in this configuration) sends a TCP Packet with SYN and ACK flags in the header to the Destination (Client).The DMZ server acknowledges the request from the client and sends back an own synchronization packet.

Packets 3-45 represents a TCP stream, which is presented in Wireshark with the command **follow>TCP Stream**. The stream represents the web site www.panlabs.com

1. PaloAlto Networks Gateway I Student Project

After having logged in to the NDG platform and after having chosen the Client Application of the platform, I choose Chrome Browser to work with.

Having opened chrome I logged in the firewall web interface for administration with the address 192.168.1.254.

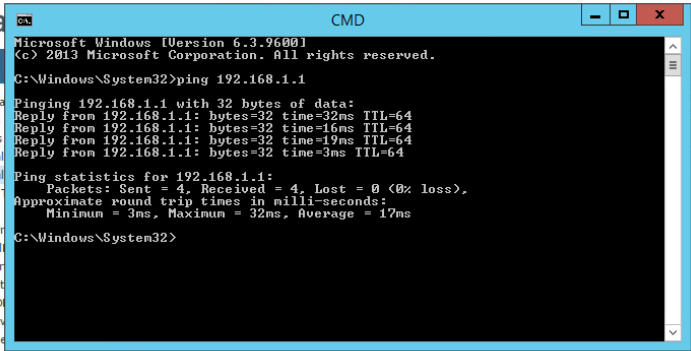
The next step was to load the configuration file of the firewall for this exercise pan8-cg-lab-01.

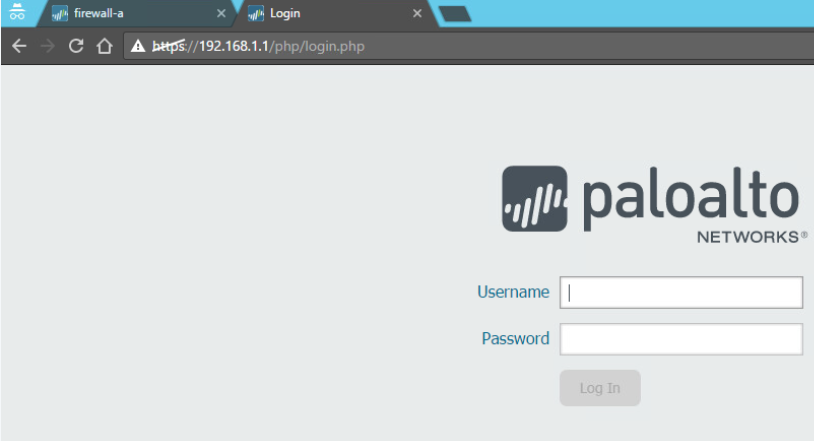
After loading the basic configuration, I was able to configure the routers Ethernet Interface 1/2 with the appropriate data. Layer 3, address 192.168.1.1/24, allow management for testing the configuration with ping. Very import is to click the commit command button, otherwise the configuration is lost

Next we had to configure the virtual Router named VR-1. With this step it is possible to route traffic from the inside to the outside network or via verse. I assigned Ethernet 1/1and 1/2 to the VR-1.

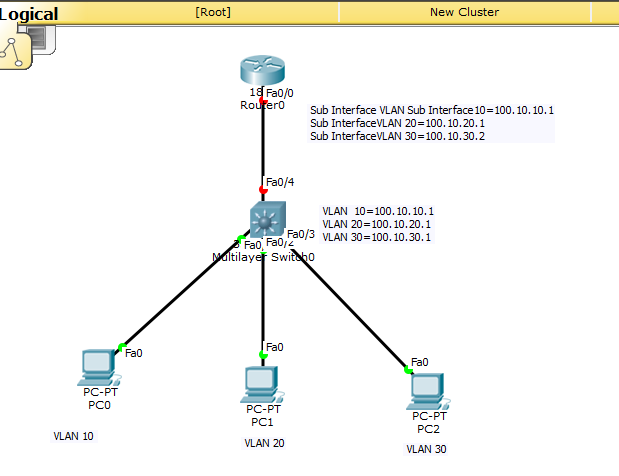
Having done all this stuff, I tested with the ping command of Windows if the router could route between the networks.

Please see the attached screen shots.





# Configure Layer 3 Interfaces



1. **Select an interface and configure it with a security zone.**

* Select Network Interfaces and either Ethernet, VLAN, loopback, or Tunnel, depending on what type of interface you want.
* Select the interface to configure.
* Select the Interface Type—Layer3.
* On the Config tab, for Virtual Router, select the virtual router you are configuring, such as default.
* For Virtual System, select the virtual system you are configuring if on a multi-virtual system firewall.
* For Security Zone, select the zone to which the interface belongs or create a New Zone
* Click OK.

1. **Configure an interface with an IPv4 address.**

There are three ways to assign an IPv4 address to a Layer 3 interface:

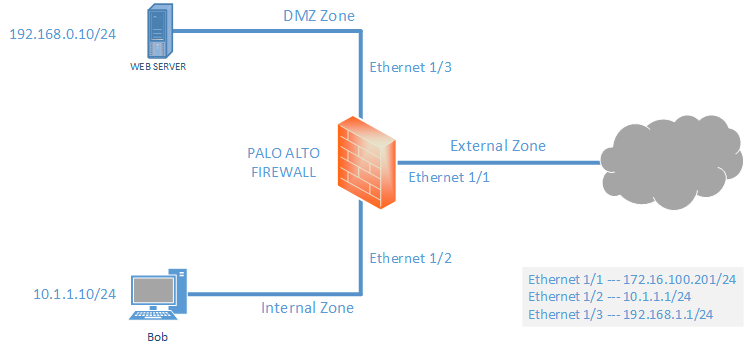
* Static
* DHCP Client—The firewall interface acts as a DHCP client and receives a dynamically assigned IP address. The firewall also provides the capability to propagate settings received by the DHCP client interface into a DHCP server operating on the firewall. This is most commonly used to propagate DNS server settings from an Internet service provider to client machines operating on the network protected by the firewall.
* PPPoE—Configure the interface as a Point-to-Point Protocol over Ethernet (PPPoE) termination point to support connectivity in a Digital Subscriber Line (DSL) environment where there is a DSL modem but no other PPPoE device to terminate the connection.
  + Select Network Interfaces and either Ethernet, VLAN, loopback, or Tunnel, depending on what type of interface you want.
  + Select the interface to configure.
  + To configure the interface with a static IPv4 address, on the IPv4 tab, set Type to Static.
  + Add a Name and optional Description for the address.
  + For Type, select one of the following:
    - IP Netmask
      * —Enter the IP address and network mask to assign to the interface, for example, 208.80.56.100/24.
      * If you’re using a /31 subnet mask for the Layer 3 interface address, the interface must be configured with the .1/31 address in order for utilities such as ping to work properly.
      * If you’re configuring a loopback interface with an IPv4 address, it must have a /32 subnet mask; for example, 192.168.2.1/32.
    - IP Range
      * —Enter an IP address range, such as 192.168.2.1-192.168.2.4.
  + FQDN—Enter a Fully Qualified Domain Name.
  + Select Tags to apply to the address.
  + Click OK.

1. **Configure an interface with Point-to-Point Protocol over Ethernet (PPPoE).**

* Select Network Interfaces and either Ethernet, VLAN, loopback, or Tunnel.
* Select the interface to configure.
* On the IPv4 tab, set Type to PPPoE.
* On the General tab, select Enable to activate the interface for PPPoE termination.
* Enter the Username for the point-to-point connection.
* Enter the Password for the username and Confirm Password
* Click OK.

1. **Configure an interface as a DHCP Client so that it receives a dynamically-assigned IPv4 address.**

* Select Network Interfaces and either Ethernet, VLAN, loopback, or Tunnel.
* Select the interface to configure.
* On the IPv4 tab, set Type to DHCP Client.
* Select Enable to activate the DHCP client on the interface.
* Select Automatically create default route pointing to default gateway provided by server to automatically create a default route that points to the default gateway that the DHCP server provides.
* (Optional) Enter a Default Route Metric (priority level) for the default route, which the firewall uses for path selection (range is 1-65,535; no default). The lower the value, the higher the priority level.
* Click OK.



1. **Configure an interface with a static IPv6 address**.

* Select Network Interfaces and either Ethernet, VLAN, loopback, or Tunnel.
* Select the interface to configure.
* On the IPv6 tab, select Enable IPv6 on the interface to enable IPv6 addressing on the interface.
* For Interface ID, enter the 64-bit extended unique identifier (EUI-64) in hexadecimal format (for example, 00:26:08:FF:FE:DE:4E:29). If you leave this field blank, the firewall uses the EUI-64 generated from the MAC address of the physical interface. If you enable the Use interface ID as host portion option when adding an address, the firewall uses the Interface ID as the host portion of that address.
* Add the IPv6 Address or select an address group.
* Select Enable address on interface to enable this IPv6 address on the interface.
* Select Use interface ID as host portion to use the Interface ID as the host portion of the IPv6 address.
* (Optional) Select Anycast to make the IPv6 address (route) an Anycast address (route), which means multiple locations can advertise the same prefix, and IPv6 sends the anycast traffic to the node it considers the nearest, based on routing protocol costs and other factors.
* (Ethernet interface only ) Select Send Router Advertisement (RA) to enable the firewall to send this address in Router Advertisements, in which case you must also enable the global
* Enable Router Advertisement option on the interface (next step).
* (Ethernet interface only) Enter the Valid Lifetime (sec), in seconds, that the firewall considers the address valid. The Valid Lifetime must equal or exceed the Preferred Lifetime (sec)(default is 2,592,000).
* (Ethernet interface only) Enter the Preferred Lifetime (sec)(in seconds) that the valid address is preferred, which means the firewall can use it to send and received traffic. After the Preferred Lifetime expires, the firewall can’t use the address to establish new connections, but any existing connections are valid until the Valid Lifetime expires (default is 604,800).
* (Ethernet interface only) Select On-link if systems that have addresses within the prefix are reachable without a router.
* (Ethernet interface only) Select Autonomous if systems can independently create an IP address by combining the advertised prefix with an Interface ID.
* Click OK

1. **(Ethernet or VLAN interface using IPv6 address only) Enable the firewall to send IPv6 Router Advertisements (RAs) from an interface, and optionally tune RA parameters.**

* Select Network Interfaces and Ethernet or VLAN.
* Select the interface you want to configure.
* Select IPv6.
* Select Enable IPv6 on the interface.
* On the Router Advertisement tab, select Enable Router Advertisement (default is disabled).
* (Optional) Set Min Interval (sec), the minimum interval, in seconds, between RAs the firewall sends (range is 3-1,350; default is 200). The firewall sends RAs at random intervals between the minimum and maximum values you set.
* (Optional) Set Max Interval (sec), the maximum interval, in seconds, between RAs the firewall sends (range is 4-1,800; default is 600). The firewall sends RAs at random intervals between the minimum and maximum values you set.
* (Optional) Set Hop Limit to apply to clients for outgoing packets (range is 1-255; default is 64). Enter 0 for no hop limit.
* (Optional) Set Link MTU, the link maximum transmission unit (MTU) to apply to clients (range is 1,280-9,192; default is unspecified).
* Select unspecified for no link MTU.
* (Optional) Set Reachable Time (ms), the reachable time, in milliseconds, that the client will use to assume a neighbor is reachable after receiving a Reachability Confirmation message.
* Select unspecified for no reachable time value (range is 0-3,600,000; default is unspecified).
* (Optional) Set Retrans Time (ms), the retransmission timer that determines how long the client will wait, in milliseconds, before retransmitting Neighbor Solicitation messages.
* Select unspecified for no retransmission time (range is 0-4,294,967,295; default is unspecified).
* (Optional) Set Router Lifetime (sec) to specify how long, in seconds, the client will use the firewall as the default gateway (range is 0-9,000; default is 1,800). Zero specifies that the firewall is not the default gateway. When the lifetime expires, the client removes the firewall entry from its Default Router List and uses another router as the default gateway.
* Set Router Preference , which the client uses to select a preferred router if the network segment has multiple IPv6 routers. High, Medium(default), or Low is the priority that the RA advertises indicating the relative priority of firewall virtual router relative to other routers on the segment.
* Select Managed Configuration to indicate to the client that addresses are vailable via DHCPv6.
* Select Other Configuration to indicate to the client that other address information (such as DNS-related settings) is available via DHCPv6.
* Select Consistency Check to have the firewall verify that RAs sent from other routers are advertising consistent information on the link. The firewall logs any inconsistencies.
* Click OK.
* (Ethernet or VLAN interface using IPv6 address only) Specify the Recursive DNS Server addresses and DNS Search List the firewall will advertise in ND Router Advertisements from this interface.
* The RDNS servers and DNS Search List are part of the DNS configuration for the DNS client so that the client can resolve IPv6 DNS requests.
* Select Network Interfaces and Ethernet or VLAN.
* Select the interface you are configuring.
* Select IPv6 DNS Support.
* Include DNS information in Router Advertisement to enable the firewall to send IPv6 DNS information.For DNS Server, Add the IPv6 address of a Recursive DNS Server. Add up to eight Recursive DNS servers. The firewall sends server addresses in an ICMPv6 Router Advertisement in order from top to bottom.
* Specify the Lifetime in seconds, which is the maximum length of time the client can use the specific RDNS Server to resolve domain names.
* The Lifetime range is any value equal to or between the Max Interval (that you configured on the Router Advertisement tab) and two times that Max Interval. For example, if your Max Interval is 600 seconds, the Lifetime range is 600-1,200 seconds.
* The default Lifetime is 1,200 seconds.For DNS Suffix, Add a DNS Suffix (domain name of a maximum of 255 bytes).
* Add up to eight DNS suffixes. The firewall sends suffixes in an ICMPv6 Router Advertisement in order from top to bottom.
* Specify the Lifetime in seconds, which is the maximum length of time the client can use the suffix. The Lifetime has the same range and default value as the Server
* Click OK

1. **(Ethernet or VLAN interface) Specify static ARP entries. Static ARP entries reduce ARP processing.**

* Select Network Interfaces and Ethernet or VLAN.
* Select the interface you are configuring.
* Select Advanced ARP Entries.
* Add an IP Address and its corresponding MAC Address(hardware or media access control address). For a VLAN interface, you must also select the Interface
* Static ARP entries do not time out. Auto learned ARP entries in the cache time out in 1,800 seconds by default; you can customize the ARP cache timeout; see [Configure Session Timeouts](https://docs.paloaltonetworks.com/content/techdocs/en_US/pan-os/8-1/pan-os-admin/networking/session-settings-and-timeouts/configure-session-timeouts.html" \l "idcb754987-865f-41a4-95cc-3348c266fdd2" \o "" \t "/home/kali/Documents\\x/_self).
* Click OK
* (Ethernet or VLAN interface) Specify static Neighbor Discovery Protocol (NDP) entries. NDP for IPv6 performs functions similar to those provided by ARP for IPv4.
* Select Network Interfaces and Ethernet or VLAN.
* Select the interface you are configuring.
* Select Advanced ND Entries.
* Add an IPv6 Address and its corresponding MAC Address.
* Click OK

1. **(Optional) Enable services on the interface.**

* To enable services on the interface, select Network Interfaces and Ethernet or VLAN.
* Select the interface you are configuring.
* Select Advanced Other Info.
* Expand the Management Profile drop-down, and select a profile or New Management Profile.
* Enter a Name for the profile.
* For Permitted Services, select services, such as Ping, and click OK

1. **Commit your changes.**
2. **Cable the interface.**

* Attach straight through cables from interfaces you configured to the corresponding switch or router on each network segment.

1. **Verify that the interface is active.**

* From the web interface, select Network Interfaces and verify that icon in the Link State column is green. You can also monitor link state from the Interfaces widget on the Dashboard