

Contents

1. Introduction:	2
2. Policies:	2
2.1 User policy:.....	2
2.1.1 Company network usage:	2
2.1.2 Non Discloser Agreements (NDAs):	2
2.2 Device management policy:.....	2
2.2.1 User responsibility [1]:.....	2
2.2.2 Device wipe:.....	2
2.2.3 Device Application management:.....	2
2.2.4 Automatic app installation:.....	3
2.2.5 BYOT analytics:.....	3
2.3 Security policy [2] [3]:	3
2.3.1 Safe Data-In-Transit:	3
2.3.2 Secured personal device:	3
2.3.3 Accidental data sharing.....	3
2.3.4 Employee Privacy:	4
2.3.5 User authentication:	4
2.3.6 Data encryption:	4
2.3.7 Network security:.....	4
3. Data Flow Diagram (DFD):.....	4
4. Mobile device management software [4]:.....	7
5. Advantages and disadvantages of BYOT:.....	7
5.1 Advantages [5]:	8
5.1.1 Work from home:.....	8
5.1.2 Productivity:.....	8
5.1.3 Ownership:.....	8
5.2 Disadvantages:	8
5.2.1 Cost to the employee:.....	8
5.2.2 Privacy [6]:	8
6. Issues with proposed BYOT:.....	9
Bibliography:	10

1. Introduction:

The purpose of this framework is to suggest policies that the company “Hyper-fort” could utilize in order to satisfy security needs of data controllers so that BYOT (Bring Your Own Technology) can become, not only a valid option, but a safe one.

2. Policies:

2.1 User policy:

2.1.1 Company network usage:

The use of the company network for personal activity (E.G. social media) would be strictly prohibited. In order to uphold this policy website Facebook or twitter would be black listed on the hyper fort network meaning employees would have to find other methods of internet browsing.

2.1.2 Non Discloser Agreements (NDAs):

All employees will be made to sign an NDA, which would be an agreement prohibiting employees from disclosing any hyper fort data to rival companies. The punishment of breaking an NDA can mean being sued by the company and would certainly result in the employee being fired.

2.2 Device management policy:

2.2.1 User responsibility [1]:

When dealing with BYOT it is important to note that a user would have full responsibility over their own devices. This means that if a piece of equipment is lost or stolen the company may decide that the employee responsible should have to pay for damages or even to replace the device.

<https://uk.sans.org/security-resources/policies/general/pdf/acceptable-use-policy>

2.2.2 Device wipe:

If a hyper fort owned device was ever discovered to be stolen or missing, once the responsible employee had reported the theft / loss, the company would have to remotely wipe the device to be sure that no company data was leaked.

2.2.3 Device Application management:

Much like the “Company network usage” policy, if there is an application which hyper fort feels that they want to ban from being accessed by their BYOT devices, they may place it on a blacklist which blocks it on said company hardware.

On the hand hyper fort may wish to restrict the user to only being allowed to install certain applications to their device. If this is the case then they may wish to set up a whitelist made up of only pre-approved, work related applications.

2.2.4 Automatic app installation:

Hyper fort may also want to make some application mandatory on devices. This can be achieved by automatically, remotely installing applications onto user devices. This could be useful for new devices, to equip them with the required tools to carry out certain tasks, or to equip devices with applications as they are discovered.

2.2.5 BYOT analytics:

With any business, the company would want some manner of an over view as to the goings on of its work force. It is for this reason that a dashboard could be put in place which records activity such as the kind of data employees are utilizing and what websites and app they are using.

2.3 Security policy [2] [3]:

2.3.1 Safe Data-In-Transit:

Given that around 95% of Hyper-fort's global network is wireless, it is imperative that the protection of Data-In-Transit is assured. This means that all of the confidential wireless transaction of data (which may well occur over the internet, through unsafe channels such as Wi-Fi, 3G or 4G) would require protection supplied by a dependable VPN (virtual private network) which would encrypt any data transfers, shielding them from being intercepted via MITM (Man In The Middle) attacks attempted by third parties.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf

2.3.2 Secured personal device:

If a user was to store sensitive work related data on their BYOT device as well as personal data it is of the utmost importance that said device be protected with the same level of security that a device such as a company pc would to prevent easily avoidable data leakage.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf

2.3.3 Accidental data sharing

Many apps share certain pieces of information depending on the device that they are downloaded to (for example: social media applications tend to share details such as phone numbers). It is for this reason that users would have to use work profiles which separate to their normal profiles so that such data cannot be leaked via these means.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf

2.3.4 Employee Privacy:

Although all activity, which takes place on a company own device, would be recorded, out of respect for an employee's privacy, Hyper-fort would only ever gain access to those records if they had good reason. One example of "good reason" would be if I.T. technicians had reported that the user had been trying to access blacklisted sites.

<https://www.docracy.com/0to97btx120/bring-your-own-device-policy-sample>

2.3.5 User authentication:

For a user to be granted access to a device they would have to identify themselves. This could be through user assigned passwords. In order to make these passwords as secure as possible they would all have to have a minimum of six characters, contain at least one capital letter, at least one number and at least one alphanumeric character. Also, for protecting a device with some of the company's more private data, a finger print scanner or even an eye scanner could be used. These can also be used for locking certain apps within a device.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf

2.3.6 Data encryption:

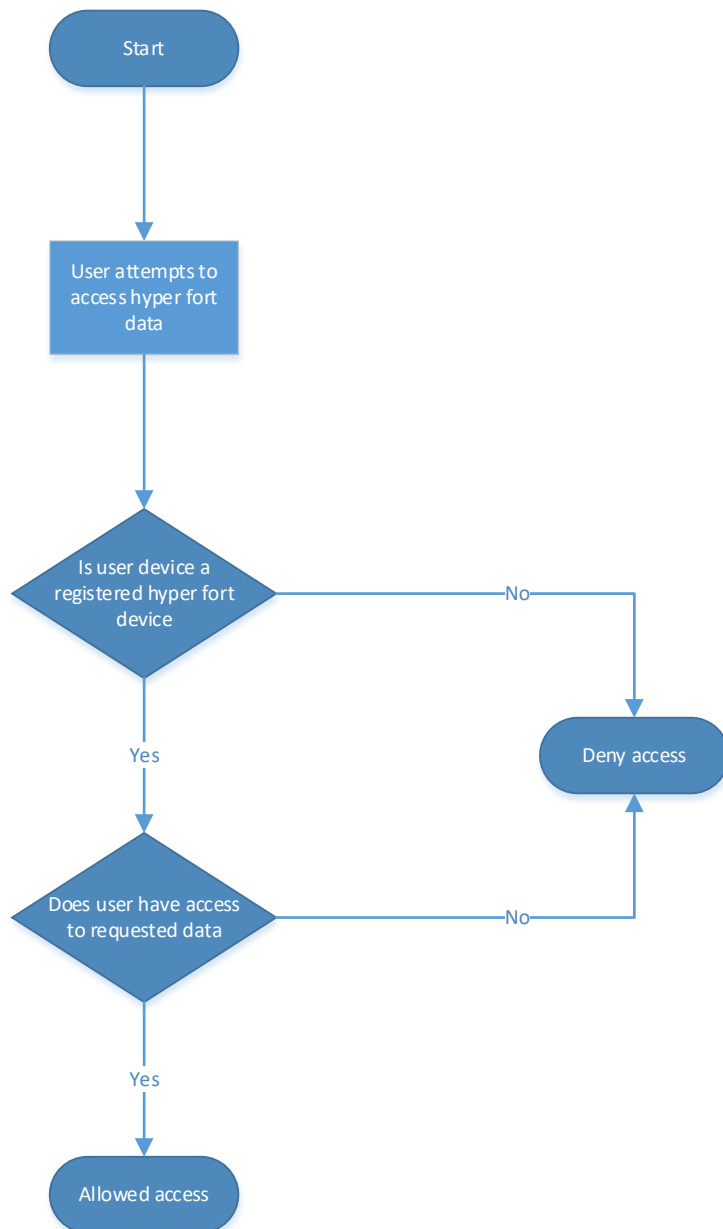
In the case of storing sensitive data on one's device, a secure space will be established within all BYOT devices which would encrypt any data stored within it, to avoid any worries about data being accessed by prying eyes. Also, as discussed previously, a VPN would be put in place to encrypt any wireless data transfers.

2.3.7 Network security:

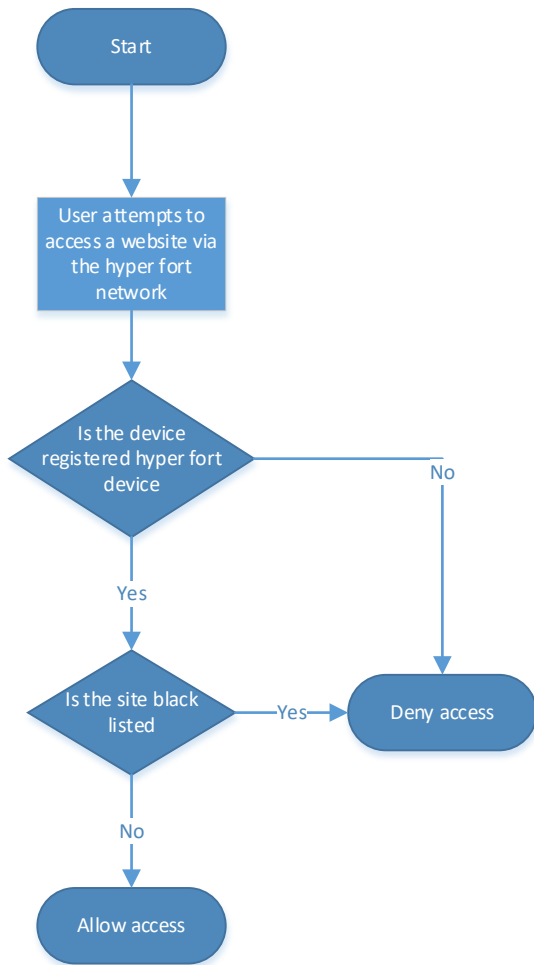
As with any secure network, hyper fort would want a fire wall in place to block any un-authorized access to the network. To avoid any easy-to-avoid data leakage by rival companies.

3. Data Flow Diagram (DFD):

The following DFD depicts what checks are made if a user attempts to access data through to hyper fort network:



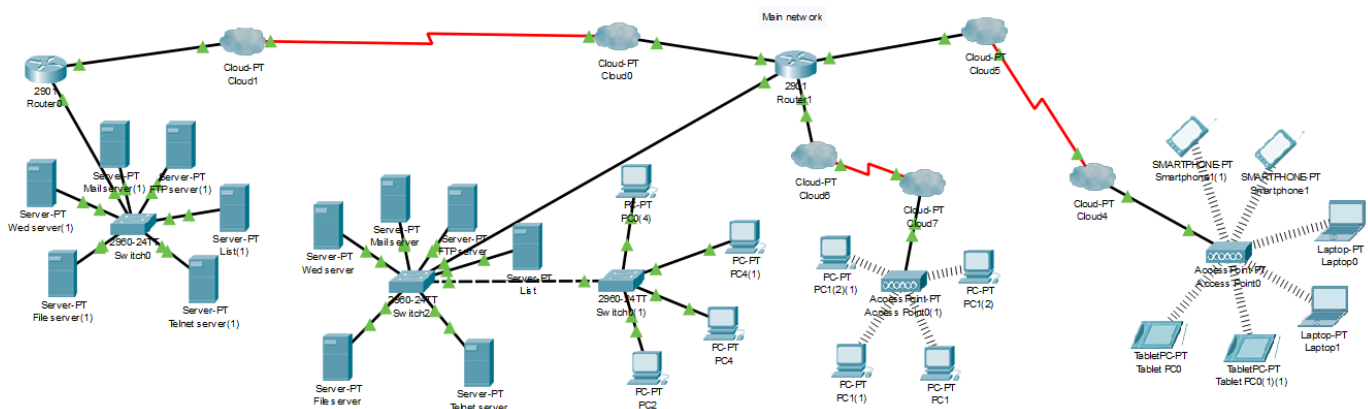
The following DFD shows what processes are deployed to validate whether, on the hyper fort network, a user should be allowed to access a website:



4. Network mock-up [See Appendix A]:

A mock-up network was developed in order to demonstrate how the network would be set out.

The screen shot depicts the network. The entire network runs through a central router. The router to off-site backup servers, customers and employees wireless via the cloud. It also connects to the main hyper fort network, meaning that, once connected to the network, users will be able to access company data wherever they are, depending on their privileges.



5. Mobile device management software [4]:

The mobile device management software that has been decided upon as Hyper fort's BYOT system is "Miradore" as it aligns well with the above BYOT framework. Although a VPN would have to be installed separately. Common themes between the above framework and Miradore's policies:

Password policy:

A policy which Miradore and the frame work above each agree upon is that all hyper fort devices should be have some extra levels of security, whether that be password protection or other kinds of protection such as figure print scanning or eye scanning.

Device wipe:

Both framework's device policies, also concur that any lost or stolen devices should be immediately reported and should then have their data remotely wiped to prevent any data leakage. As stated above, if a device was to be lost or stolen, the employee responsible for it would likely be charged for damages or to replace the device.

Data encryption:

Another match between the two policies is to equip all BYOT devices with secure areas which would encrypt any data stored within them. This means that if any BYOT devices were ever to be stolen, the thief would be unable to access the data stored upon it without knowing its passwords.

Accidental data sharing:

The two policies also agreed that users must use company provided profiles when accessing devices to avoid data leakage via apps such as social media.

Device Application management:

Both BYOT frame works also concur that a policy should be put in place, which allows hyper fort to black list certain applications if they feel that they feel could curb workflow of said devices. These applications could include social media or games.

They also agree that a whitelist could be put in place to restrict users to only downloading apps which have already been approved by hyper fort as work related.

Automatic app installation:

Miradore agrees that it could be highly productive to automatically install apps on all company own devices in order to keep device up to date with recent software which could be greatly beneficial to hyper fort line of work.

6. Advantages and disadvantages of BYOT:

Although BYOT has many advantages it also has its fair share of disadvantages, some these are listed below:

6.1 Advantages [5]:

6.1.1 Work from home:

The main advantage of BYOT is that it gives users the option to carry out work related tasks where ever they are, meaning that they would not have to worry about having to get to their place of occupation in order to do any work. Not only does this make it a lot easier for employees to get work done but it would also dramatically cut down on travel cost.

6.1.2 Productivity:

It's not too much of a stretch to believe that an employee can work far better on a personal device such as a smart phone. This is mainly to do with the fact that modern mobile devices are becoming incredibly easy to use. BYOT also allows for much more time for employees to carry out tasks, which also adds to the overall productivity levels.

<https://www.techopedia.com/6/28293/it-business/it-management/byot-what-it-means-for-it/4>

6.1.3 Ownership:

Even if an employee does not purchase a device them self (E.G. if the device was supplied by the company) they would still feel a sense of ownership for it, especially as they may well use the device for personal as well. Consequently, an employee would take far great care with the device than if it was simply the work PC they sat at all day. Also the possibility that the employee may well have to pay for any damages done to the device would add to their sense of caution around it.

<https://www.techopedia.com/6/28293/it-business/it-management/byot-what-it-means-for-it/4>

6.2 Disadvantages:

6.2.1 Cost to the employee:

Although BYOT devices would usually be supplied by the employer, any damages inflicted upon the device would likely be charge to the employee. This may not cost very much depending on the damage but if the device was to be lost or stolen then costs could be substantially high which would likely heavily inconvenience.

6.2.2 Privacy [6]:

A problem which some employees may have is that the company may well monitor all activity carried out on the devices. This could be seen as a breach of privacy by some employees and could turn them away from BYOT.

<https://www.thewindowsclub.com/bring-your-own-device-byod>

7. Issues with proposed BYOT:

What type of data is retained by the mobile devices connecting to hyper-fort network?

The devices could retain any data on the network chosen by the user, as long as the user has access to it, this would mean that a higher level worker such as the hyper fort manager has access to far more data than a lower level works such as a business consultant. This data could be anything for databases to written reports or even power point presentations.

However Under the constraints of the NDA, that all employees must sign, workers will be legally bound to keep all company data a trade secret.

What is the potential for data leakage when the participating devices leaves the office environment?

Once a device leaves the confines of the hyper fort offices, the potential for data leakage is rather low. This is because the only real risk of data being leaking is if the device is stolen, although the above framework does state that once a device is reported missing it would be remotely wiped. The above framework outlines that the use of a VPN is essential meaning that all wireless data transactions are encrypted to avoid any "man in the middle" attacks from someone attempting to steal confidential company data which substantial reduces the risk of data loss.

How to address the blending of personal and business usage when devices are in office.

As stated above Just as in any work environment, if, when on office time, employees were to use their devices in order to carry out personal objectives such as shopping, social media or even gaming, they would find the those manner of sites would be blocked would they would have to use some manner of internet connection not supplied by the company (E.G. 4G, or a public Wi-Fi).

What strategy to deploy to deal with different brands of devices.

Although different brands of devices may work differently, this should not be a problem for the framework as it does not specify a certain brand. Although the "accidental data sharing" point does note that users should be made to use separate profiles for business and pleasure, where applicable, when using BYOT devices.

What strategy to deploy to deal with different operating system platform.

Whereas operating system which have not been updated to their most recent versions could cause problems for the productivity of the system, as updates may not be available, different operating systems should hold no problems. The system in question has multiple versions which allow it to be run on as plethora of different devices and operating system (E.G. iOS and android).

What strategy to deploy to deal with different applications on user devices.

As discussed above: If hyper fort does not want employees to access a certain website or application then they can simply blacklist it on any company owned devices or the company network, meaning no employees could access it.

What mitigating strategy will be deployed when the owner of a participating device leave their employment or the device is lost, stolen, or fails.

As highlighted in the framework above, if a company owned BOYT device is ever reported missing then the company will remotely wipe it to avoid any data leakage. This process should not result in too much data being lost as all data on the device should have been backed up on to the hyper fort network.

Bibliography:

[1] Data concerning user responsibilities was taken from the following BYOT framework outline by the SANS institute titled "Acceptable use policy":

<https://uk.sans.org/security-resources/policies/general/pdf/acceptable-use-policy>

[2] Data concerning security policies was taken from the follow report from GOV.UK titled "BYOT guidance: device security consideration":

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf

[3] Information about security policies was derived from the follow report from docracy titled "Bring Your Own Device policy sample":

<https://www.docracy.com/0to97btX120/bring-your-own-device-policy-sample>

[4] Data from the following report by Miradore.com, showing their BYOT policies, was use in the mobile device management section of the document:

<https://www.miradore.com/product/>

[5] Data showing the advantages of BYOT was found from the following article by Tara Struyk on techopedia.com and is titled "BYOT what it means in I.T.":

<https://www.techopedia.com/6/28293/it-business/it-management/byot-what-it-means-for-it/4>

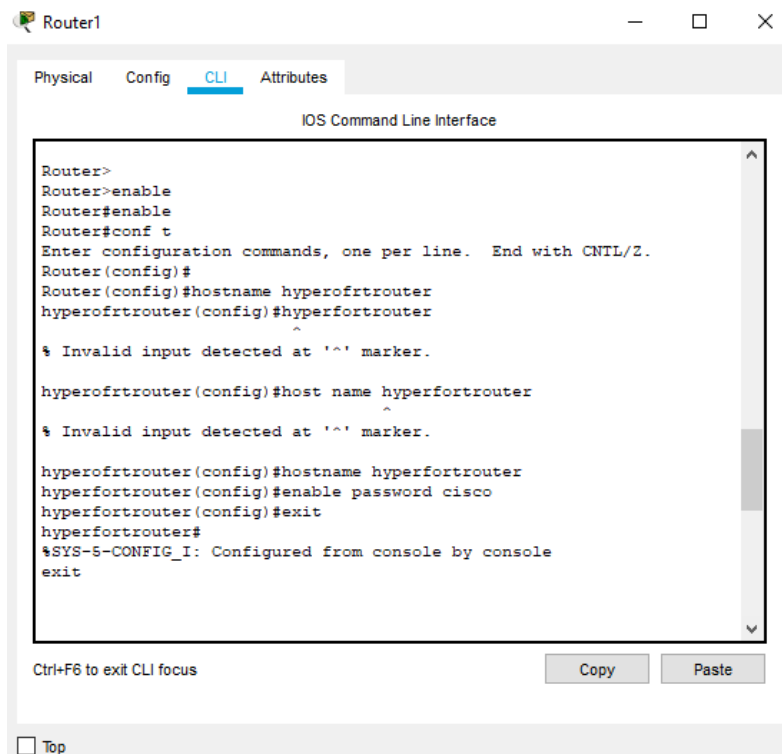
[6] Data showing the disadvantages of BYOT was taken from the following article by Arun Kumar on thewindowsclub.com and is titled "Bring Your Own Devices (BYOD) advantages and disadvantages - 1":

<https://www.thewindowsclub.com/bring-your-own-device-byod>

Appendix:

Appendix [A]:

The following plethora of screen shots depict a router and switch being set up step-by-step:



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router>
Router>enable
Router#enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#hostname hyperoftrouter
hyperoftrouter(config)#hyperfortrouter
^
% Invalid input detected at '^' marker.

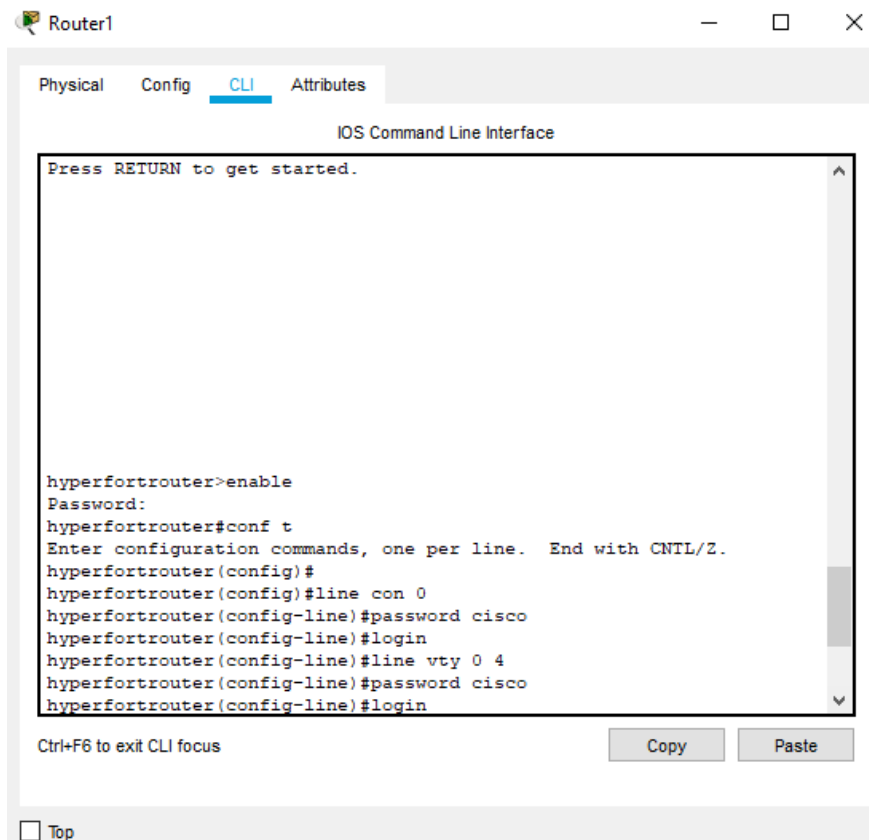
hyperoftrouter(config)#host name hyperfortrouter
^
% Invalid input detected at '^' marker.

hyperoftrouter(config)#hostname hyperfortrouter
hyperfortrouter(config)#enable password cisco
hyperfortrouter(config)#exit
hyperfortrouter#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

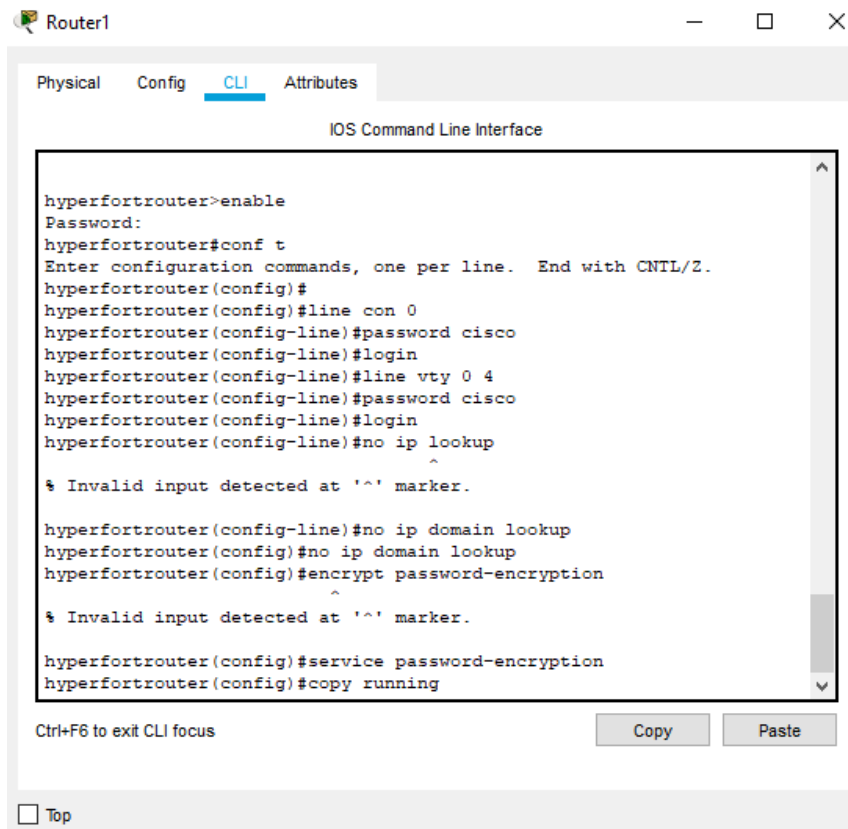
```
Press RETURN to get started.

hyperfortrouter>enable
Password:
hyperfortrouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
hyperfortrouter(config)#
hyperfortrouter(config)#line con 0
hyperfortrouter(config-line)#password cisco
hyperfortrouter(config-line)#login
hyperfortrouter(config-line)#line vty 0 4
hyperfortrouter(config-line)#password cisco
hyperfortrouter(config-line)#login
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



Router1

Physical Config **CLI** Attributes

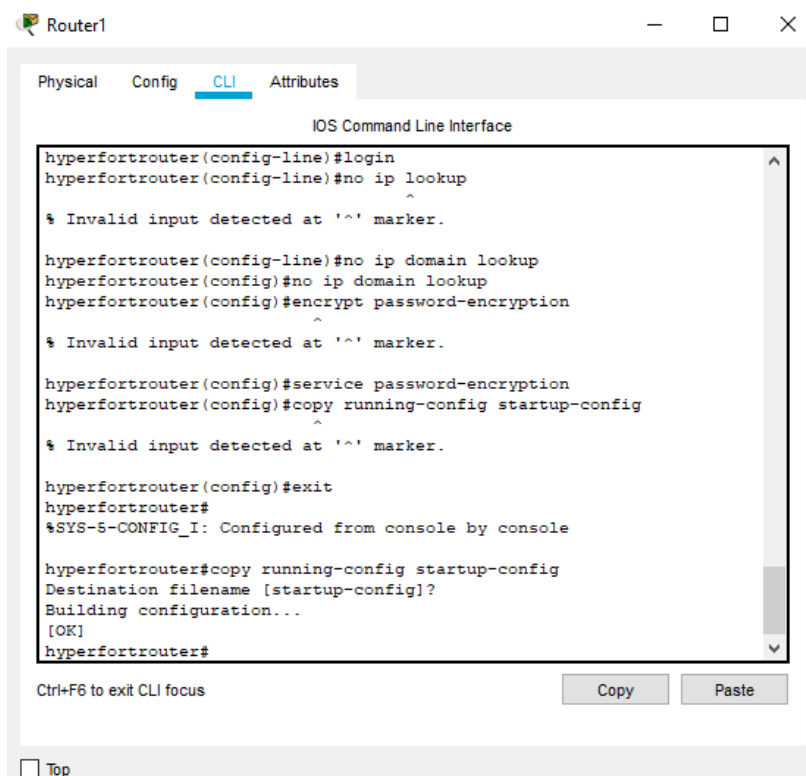
IOS Command Line Interface

```
hyperfortrouter>enable
Password:
hyperfortrouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
hyperfortrouter(config)#
hyperfortrouter(config)#line con 0
hyperfortrouter(config-line)#password cisco
hyperfortrouter(config-line)#login
hyperfortrouter(config-line)#line vty 0 4
hyperfortrouter(config-line)#password cisco
hyperfortrouter(config-line)#login
hyperfortrouter(config-line)#no ip lookup
^
% Invalid input detected at '^' marker.
hyperfortrouter(config-line)#no ip domain lookup
hyperfortrouter(config)#no ip domain lookup
hyperfortrouter(config)#encrypt password-encryption
^
% Invalid input detected at '^' marker.
hyperfortrouter(config)#service password-encryption
hyperfortrouter(config)#copy running
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



Router1

Physical Config **CLI** Attributes

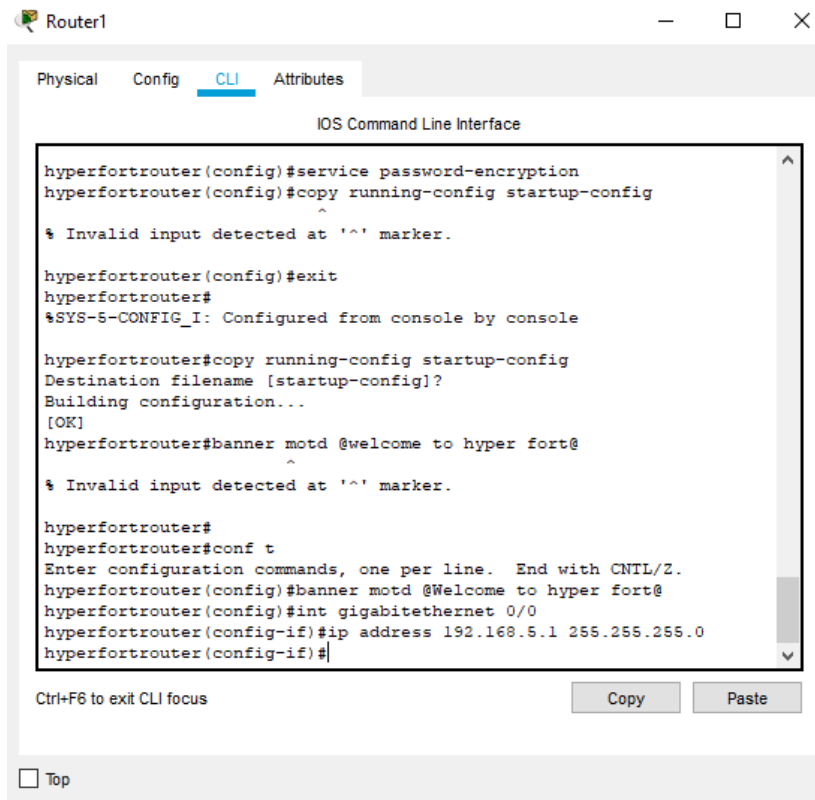
IOS Command Line Interface

```
hyperfortrouter(config-line)#login
hyperfortrouter(config-line)#no ip lookup
^
% Invalid input detected at '^' marker.
hyperfortrouter(config-line)#no ip domain lookup
hyperfortrouter(config)#no ip domain lookup
hyperfortrouter(config)#encrypt password-encryption
^
% Invalid input detected at '^' marker.
hyperfortrouter(config)#service password-encryption
hyperfortrouter(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.
hyperfortrouter(config)#exit
hyperfortrouter#
%SYS-5-CONFIG_I: Configured from console by console
hyperfortrouter#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
hyperfortrouter#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
hyperfortrouter(config)#service password-encryption
hyperfortrouter(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.

hyperfortrouter(config)#exit
hyperfortrouter#
%SYS-5-CONFIG_I: Configured from console by console

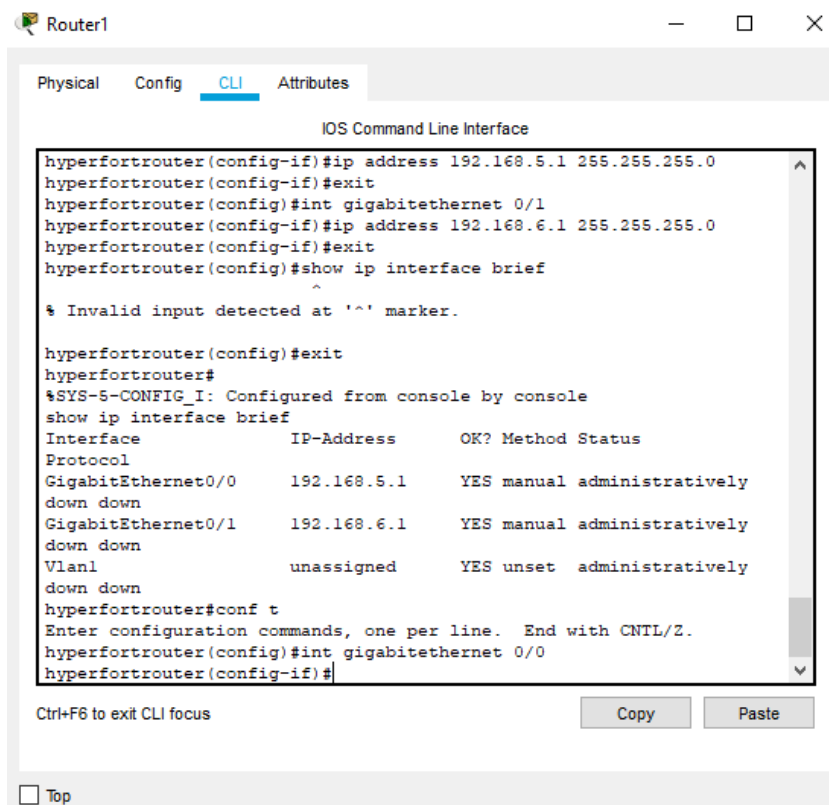
hyperfortrouter#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
hyperfortrouter#banner motd @welcome to hyper fort@
^
% Invalid input detected at '^' marker.

hyperfortrouter#
hyperfortrouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
hyperfortrouter(config)#banner motd @Welcome to hyper fort@
hyperfortrouter(config)#int gigabitethernet 0/0
hyperfortrouter(config-if)#ip address 192.168.5.1 255.255.255.0
hyperfortrouter(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

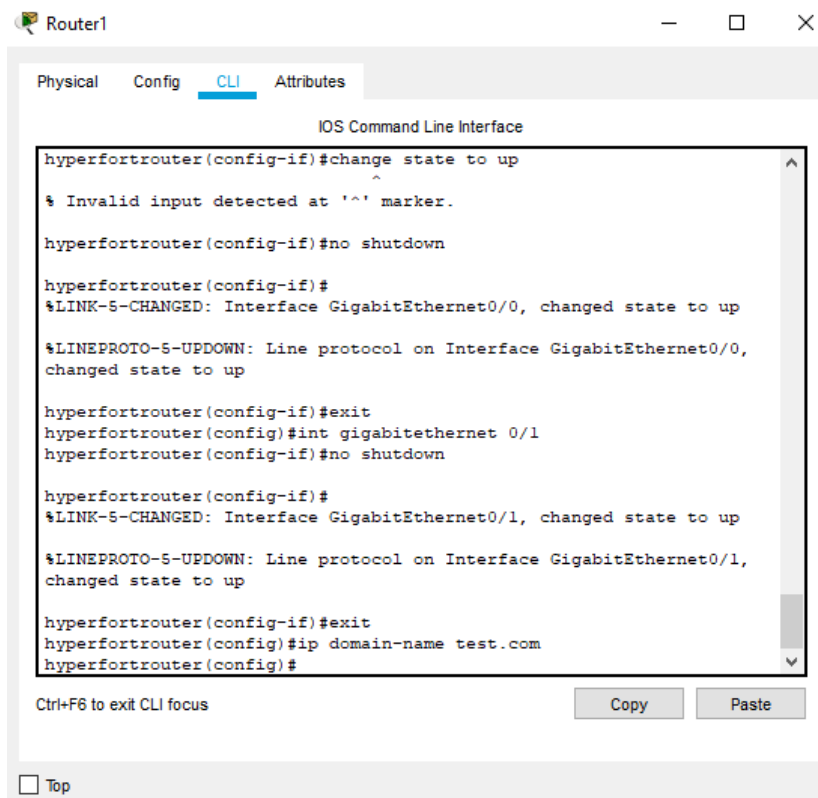
```
hyperfortrouter(config-if)#ip address 192.168.5.1 255.255.255.0
hyperfortrouter(config-if)#exit
hyperfortrouter(config)#int gigabitethernet 0/1
hyperfortrouter(config-if)#ip address 192.168.6.1 255.255.255.0
hyperfortrouter(config-if)#exit
hyperfortrouter(config)#show ip interface brief
^
% Invalid input detected at '^' marker.

hyperfortrouter(config)#exit
hyperfortrouter#
%SYS-5-CONFIG_I: Configured from console by console
show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0       192.168.5.1     YES manual administratively
down down
GigabitEthernet0/1       192.168.6.1     YES manual administratively
down down
Vlan1                    unassigned      YES unset  administratively
down down
hyperfortrouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
hyperfortrouter(config)#int gigabitethernet 0/0
hyperfortrouter(config-if)#
```

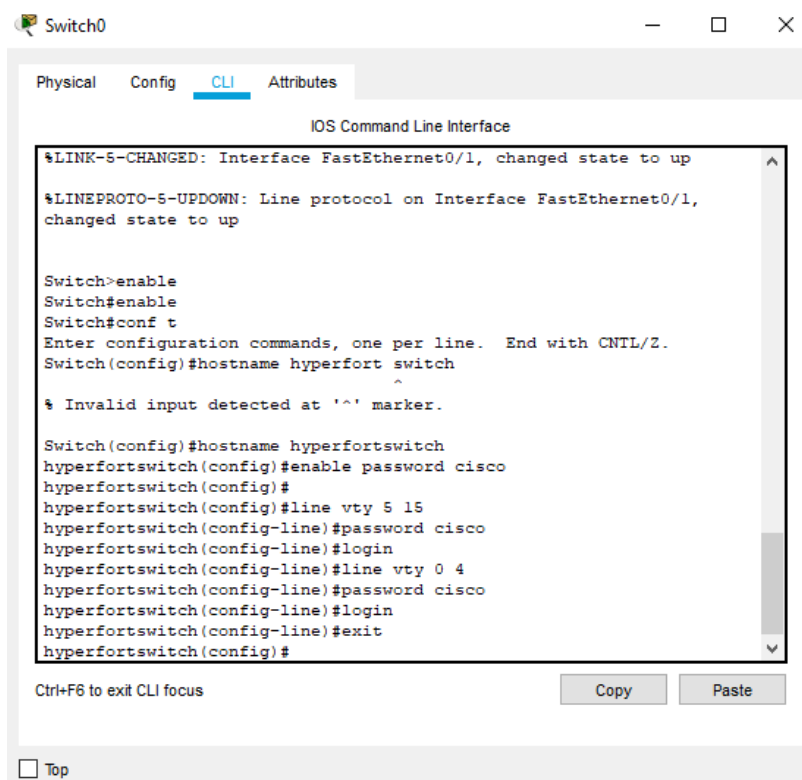
Ctrl+F6 to exit CLI focus

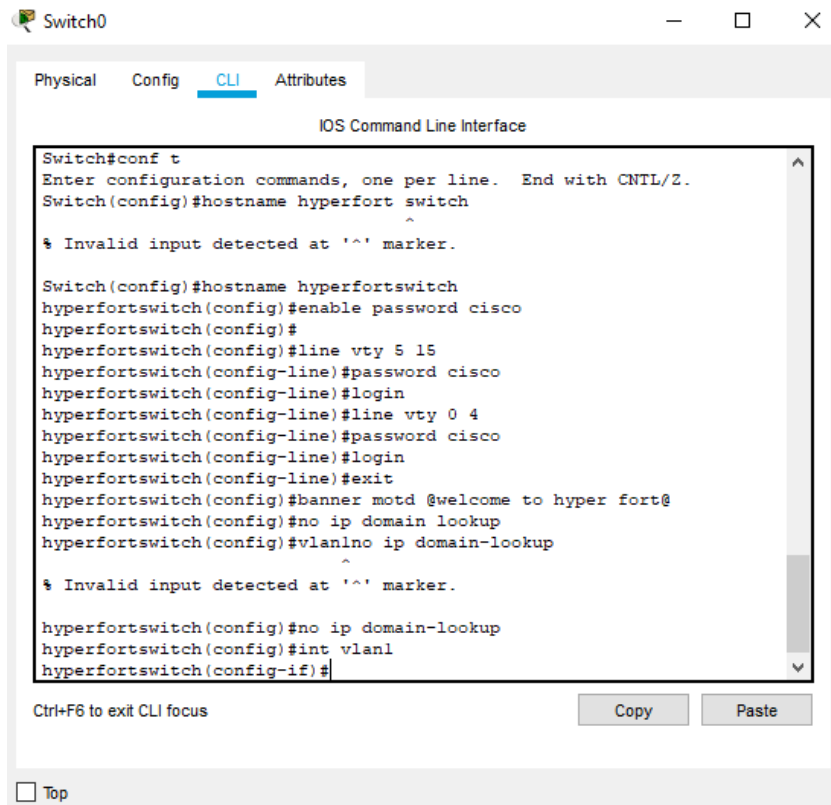
Copy Paste

☐ Top



Switch:





Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname hyperfort switch
^
% Invalid input detected at '^' marker.

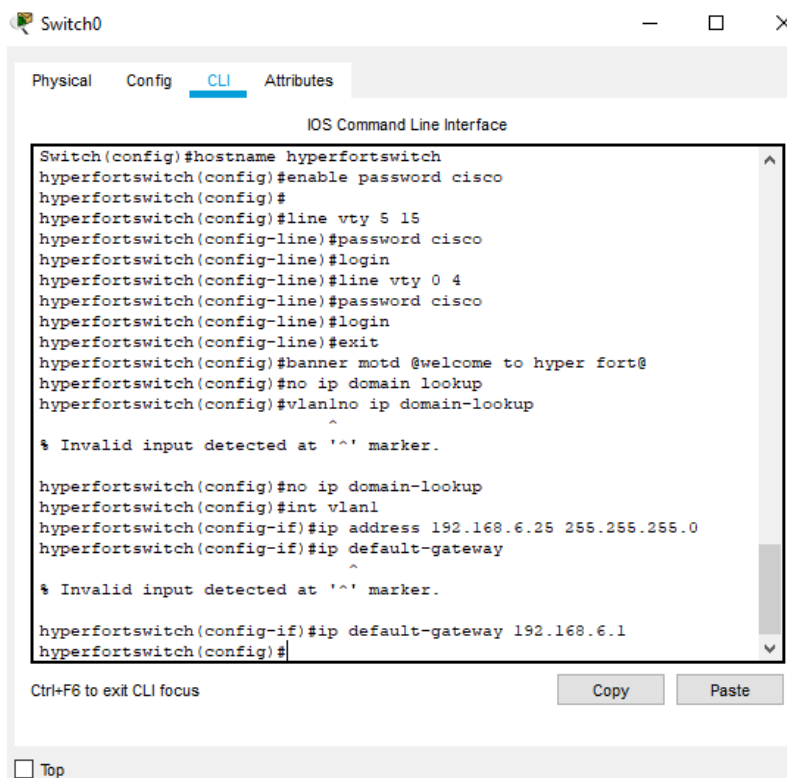
Switch(config)#hostname hyperfortswitch
hyperfortswitch(config)#enable password cisco
hyperfortswitch(config)#
hyperfortswitch(config)#line vty 5 15
hyperfortswitch(config-line)#password cisco
hyperfortswitch(config-line)#login
hyperfortswitch(config-line)#line vty 0 4
hyperfortswitch(config-line)#password cisco
hyperfortswitch(config-line)#login
hyperfortswitch(config-line)#exit
hyperfortswitch(config)#banner motd @welcome to hyper fort@
hyperfortswitch(config)#no ip domain lookup
hyperfortswitch(config)#vlan1no ip domain-lookup
^
% Invalid input detected at '^' marker.

hyperfortswitch(config)#no ip domain-lookup
hyperfortswitch(config)#int vlan1
hyperfortswitch(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config)#hostname hyperfortswitch
hyperfortswitch(config)#enable password cisco
hyperfortswitch(config)#
hyperfortswitch(config)#line vty 5 15
hyperfortswitch(config-line)#password cisco
hyperfortswitch(config-line)#login
hyperfortswitch(config-line)#line vty 0 4
hyperfortswitch(config-line)#password cisco
hyperfortswitch(config-line)#login
hyperfortswitch(config-line)#exit
hyperfortswitch(config)#banner motd @welcome to hyper fort@
hyperfortswitch(config)#no ip domain lookup
hyperfortswitch(config)#vlan1no ip domain-lookup
^
% Invalid input detected at '^' marker.

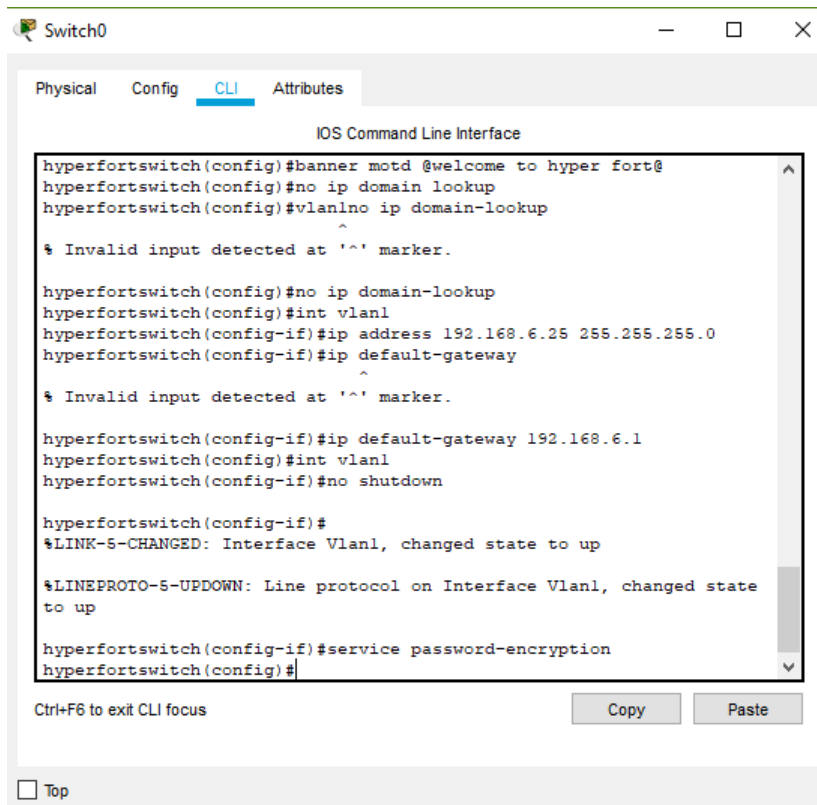
hyperfortswitch(config)#no ip domain-lookup
hyperfortswitch(config)#int vlan1
hyperfortswitch(config-if)#ip address 192.168.6.25 255.255.255.0
hyperfortswitch(config-if)#ip default-gateway
^
% Invalid input detected at '^' marker.

hyperfortswitch(config-if)#ip default-gateway 192.168.6.1
hyperfortswitch(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



The screenshot shows a network switch configuration window titled "Switch0". It has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area is titled "IOS Command Line Interface" and contains a text box with the following text:

```
hyperfortswitch(config)#banner motd @welcome to hyper fort@
hyperfortswitch(config)#no ip domain lookup
hyperfortswitch(config)#vlan1no ip domain-lookup
^
% Invalid input detected at '^' marker.

hyperfortswitch(config)#no ip domain-lookup
hyperfortswitch(config)#int vlan1
hyperfortswitch(config-if)#ip address 192.168.6.25 255.255.255.0
hyperfortswitch(config-if)#ip default-gateway
^
% Invalid input detected at '^' marker.

hyperfortswitch(config-if)#ip default-gateway 192.168.6.1
hyperfortswitch(config)#int vlan1
hyperfortswitch(config-if)#no shutdown

hyperfortswitch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

hyperfortswitch(config-if)#service password-encryption
hyperfortswitch(config)#
```

Below the text box, there is a status bar with the text "Ctrl+F6 to exit CLI focus" on the left, and "Copy" and "Paste" buttons on the right. At the bottom left of the window, there is a "Top" button.