Networking Academy: Standalone Access Point Configuration

Hunter Zhuang

Contents

Purpose

The purpose of this lab is to set up a standalone access point (AP) that broadcasts a 2.4GHz network using a pre-shared key (PSK) to authenticate users; 5GHz network also using a pre-shared key to authenticate users; and a 5GHz network with enterprise authentication using RADIUS. All these Wi-Fi networks will be secured using WPA2. Additionally, in order configure the AP to provide internet connectivity for any devices that connect to the it, various protocols need to be configured like DHCP.

Background Information

Wireless APs are devices that allow other Wi-Fi devices to connect to it through radio waves, so that those devices can access resources on the network or the internet. There are multiple ranges for these radio waves, but the 2.4GHz and the 5GHz ranges are the most common. Wireless APs are useful for devices that want access to the internet, but also need to be mobile, like phones, tablets, and laptops. But the transmission of data wirelessly may seem like a breach of security because anyone can detect and read the transmissions, there are various ways to encrypt that data. One such way is with AES, an encryption algorithm, making it so that no one can read the data that is sent wirelessly, other than the AP.

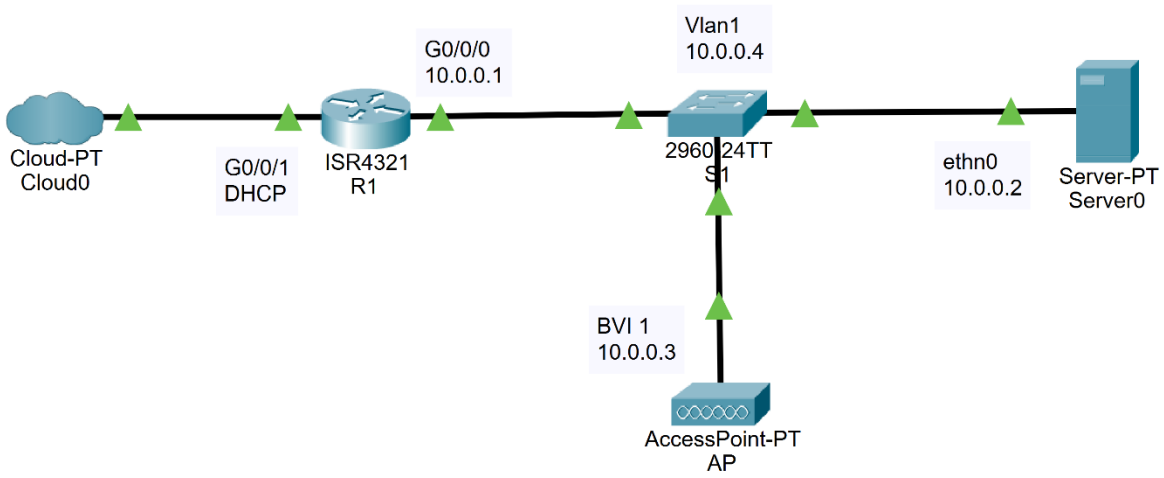
A service set identifier (SSID) refers to a particular wireless network's name transmitted by an AP. SSIDs are what appear when a user attempts to connect to a Wi-Fi network in the settings menu on their device. Basic service set identifiers (BSSIDs) are different from SSIDs and are almost never seen by users. BSSIDs are unique identifier labels that are given to each transmission of an SSID. For example, an SSID of "Floor 1" would have a different BSSID than an SSID of "Floor 2". BSSIDs are used for devices to be able to uniquely identify different Wi-Fi networks, especially when an area has a multitude of APs.

Security is important for wireless networks, especially since it is easy to connect to one. There are multiple forms of security to prevent unwanted devices from joining the network. One such method is to use a password for the Wi-Fi network, only allowing those who put in the correct password to get Wi-Fi. This method is effective but may not be effective enough for a company that wants to protect confidential documents. This is where another method of authentication is used: RADIUS (Remote Authentication Dial-In User Service), a centralized way to authenticate, authorize, and keep track of what users do on the network (accounting). A RADIUS server can be configured to have a separate user for each person who should have access to a network and can bestow different privileges to each user, since both a username and password is required to be authenticated. A bonus of RADIUS is that it can also do accounting for users. Since each user is signed into their account for the network, and administrator can check on any users' recent actions on the network.

Lab Summary

A standalone access point was configured with a 2.4GHz network and 5GHz network using WPA2 and a pre-shared key to authenticate users; Additionally, the access point was also configured to broadcast a 5GHz network with enterprise authentication using RADIUS. As a result, there is a RADIUS server. Lastly there is a router that provides connectivity to the internet through DHCP and NAT for the AP and other connected wireless devices. Further information on setup for this lab is available here: https://github.com/101zh/StandaloneAccessPointLab.

Network Diagram with IP



Lab Commands

AP Commands

- **`aaa new-model`**
  - Enables authentication, authorization, and accounting control commands.
- **`aaa group server radius`** [*`server-group-name`*]
  - Defines a radius server-group.
  - **`server`** [*`ip-address`*] **`auth-port`** [*`port-number`*] **`acct-port`** [*`port-number`*]
    - Specifies a radius server with the authentication and accounting ports for it.
- **`aaa authentication login`** [*`named-authentication-list`*] **`group radius`**
  - Sets an authentication list for radius.
- **`dot11 ssid`** [*`service-set-ID`*]
  - Enters the configuration mode for a service set ID.
  - **`vlan`** [*`vlan-number`*]
    - assigns the SSID to a VLAN.
  - **`authentication open`**
    - Configures the SSID to allow any device to authenticate and try and communicate with the access point.
  - **`authentication key-management wpa version 2`**
    - Configures the SSID to use WPA2 when a device attempts to authenticate with the access point.
  - **`mbssid guest-mode`**
    - Configures the SSID to allow for multiple SSIDs and to broadcast the SSID name.
  - **`wpa-psk ascii 0`** [*`unencrypted-password`*]
    - Specifies a clear-text password for the SSID.

    - **authentication open eap** [*eap-list-name*]
        - Configures the SSID to use EAP, allowing other authentication methods to be used.
    - **authentication network-eap** [*eap-list-name*]
        - Configures the SSID to use radius for authentication.
- **bridge irb**
    - Configures the access point to use integrated routing and bridging.
- **interface Dot11Radio0**
    - Enters the interface configuration mode for the access point's 2.4GHz radio.
    - **encryption mode ciphers aes-ccm**
        - Sets the 2.4 GHz radio to use AES-CCM for encryption
    - **encryption vlan** [vlan-number] **mode ciphers aes-ccm**
        - Configures AES-CCM encryption to be used for the specified vlan with the interface.
    - **ssid** [service-set-ID]
        - Specifies an SSID to be transmit on this radio.
    - **antenna gain** [resultant-antenna-gain-dB]
        - Sets a value for the antenna gain of the access point's radio; the value determines how focused the signal is for the radio.
    - **mbssid**
        - Enables multiple BSSIDs on the 2.4GHz radio.
    - **station-role root**
        - Configures the access point to be a root, which is the starting point for the transmitting of a network.
- **interface** [*interface-name*] **.** [*subinterface-number*]
    - Enters interface configuration mode for a subinterface
    - **encapsulation dot1Q** [vlan-ID] {**native**}
        - Configures the interface to encapsulate packets using 802.1Q
    - **bridge-group** [bridge-group-number]
        - Assigns the interface to a bridge group
- **interface Dot11Radio1**
    - Enters the interface configuration mode for the access point's 2.4GHz radio.
    - **peakdetect**
        - Tells the radio to avoid interfering with other wireless signals
    - **dfs band** [frequency-band-number] **block**
        - blocks a particular band of radio waves that the access point won't use. (typically used because of laws that restrict which bands can be used in which areas)
    - **channel dfs**
        - Tells the AP to dynamically select what frequency to be on
- **interface** [*interface-name*]
    - Enters interface configuration mode for any particular interface
    - **mac-address** [*MAC-address*]
        - Sets the mac-address of the interface
    - **ip helper-address** [*ip-address*]

        - Indicates a location for UDP broadcast packets. It is often used for DHCP, but there are other uses.
- **radius-server host** [*ip-address*] **auth-port** [*port-number*] **acct-port** [*port-number*] **key 0** [*unencrypted-password*]
    - Specifies a radius server IP, the authentication and accounting ports for it, and the clear-text password for communicating with the radius server.
- **bridge** [*bridge-group-number*] **route ip**
    - Tells a particular bridge group to use IP to route in the group

Switch Commands

- **interface** [*interface-name*]
    - Enters interface configuration mode for any particular interface
    - **switchport trunk encapsulation dot1q**
        - Tells the interface to use 802.1q trunking encapsulation when trunking
    - **switchport mode trunk**
        - Puts the interface in trunking mode, which allows multiple VLANs to go through one port.
    - **spanning-tree portfast**
        - Tells the interface to start forwarding packets the moment it is up

Router Commands

- **ip dhcp excluded-address** [*low-address*] [*high-address*]
    - Excludes addresses from low address to the high address from being distributed to hosts.
- **ip dhcp pool** [*pool-name*]
    - Defines a DHCP pool
    - **network** [*network-number*] [*subnet-mask*]
        - Sets the network for this DHCP pool
    - **default-router** [*ip-address*] [*ip-address2 … ip-address8*]
        - Defines the default gateway for host devices
    - **dns-server** [*ip-address*] [*ip-address2 … ip-address8*]
        - Defines the DNS server for host devices
- **interface** [*interface-name*]
    - Enters interface configuration mode for any particular interface
    - **ip nat** {**inside | outside**}
        - Defines the interface for either “inside” or “outside” network address translation
- **ip nat inside source list** [*access-list-number*] **interface** [*interface-name*] **overload**
    - Indicates a list of addresses to be translated on the inside to one interface with PAT (port address translation)
- **access-list** [*access-list-number*] {*deny|permit*} [*network-number*] [*wildcard-mask*]
    - Denies or permits a range of IP addresses

Problems

There were a multitude of problems in this lab. The first problem encountered was inter-VLAN routing: after setting VLAN interfaces on the switch, the AP couldn't ping any IP except for the IPs on VLAN 1. Then I realized that I had forgotten to make a way for packets to be routed between VLANs. So, I configured a router on a stick to allow packets to be routed between VLANs. Even after that, the access point still couldn't communicate with the internet. After much testing and debugging, I found out that I had conflicting routes of last resort, since a DHCP server already gave it to the router's outward facing interface. Once I removed the conflicting default route, I was able to receive internet connectivity. For the rest of the lab there weren't many other problems, that is until RADIUS configuration. Every time I tried to authenticate a user, the server wouldn't authenticate the user, even though I had connectivity with the RADIUS server. By looking through RADIUS documentation, I found out (the hard way) that users needed to be configured with a reply message for the authentication process for a user to work. I learned a valuable lesson of reading documentation in full without quickly skimming.

Conclusion

This lab was successfully completed, despite the many complex problems faced. During this lab, I had to revisit how to configure inter-VLAN routing. Although I had never configured a standalone access point from console, I was able to configure multiple secure Wi-Fi networks on different radio frequencies.

Configurations

R1 Configuration

```
hostname R1
!
!
!
ip dhcp excluded-address 10.0.0.1 10.0.0.4
ip dhcp excluded-address 10.0.24.1 10.0.24.4
ip dhcp excluded-address 10.0.5.1 10.0.5.4
!
ip dhcp pool vlan1
 network 10.0.0.0 255.255.255.0
 default-router 10.0.0.1
 dns-server 9.9.9.9 1.1.1.1
!
ip dhcp pool vlan24
 network 10.0.24.0 255.255.255.0
 default-router 10.0.24.1
 dns-server 9.9.9.9 1.1.1.1
!
ip dhcp pool vlan5
 network 10.0.5.0 255.255.255.0
```

```
 default-router 10.0.5.1
 dns-server 9.9.9.9 1.1.1.1
!
ip dhcp pool vlan50
 network 10.0.50.0 255.255.255.0
 default-router 10.0.50.1
 dns-server 9.9.9.9 1.1.1.1
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 ip nat inside
 negotiation auto
!
interface GigabitEthernet0/0/0.1
 encapsulation dot1Q 1 native
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/0.5
 encapsulation dot1Q 5
 ip address 10.0.5.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/0.24
 encapsulation dot1Q 24
 ip address 10.0.24.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/0.50
 encapsulation dot1Q 50
 ip address 10.0.50.1 255.255.255.0
 ip nat inside
!
interface GigabitEthernet0/0/1
 ip address dhcp
 ip nat outside
 negotiation auto
!
!
!
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
ip nat inside source list 5 interface GigabitEthernet0/0/1 overload
ip nat inside source list 24 interface GigabitEthernet0/0/1 overload
ip nat inside source list 50 interface GigabitEthernet0/0/1 overload
```

```
!
!
!
access-list 1 permit 10.0.0.0 0.0.0.255
access-list 5 permit 10.0.5.0 0.0.0.255
access-list 24 permit 10.0.24.0 0.0.0.255
access-list 50 permit 10.0.50.0 0.0.0.255
!
!
!
end
```

S1 Configuration

```
hostname S1
!
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
interface FastEthernet0/3
 spanning-tree portfast
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
!
!
interface Vlan1
 ip address 10.0.0.4 255.255.255.0
!
interface Vlan5
 ip address 10.0.5.4 255.255.255.0
!
interface Vlan24
 ip address 10.0.24.4 255.255.255.0
!
```

```
interface Vlan50
 ip address 10.0.50.4 255.255.255.0
!
!
!
end
```

AP Configuration

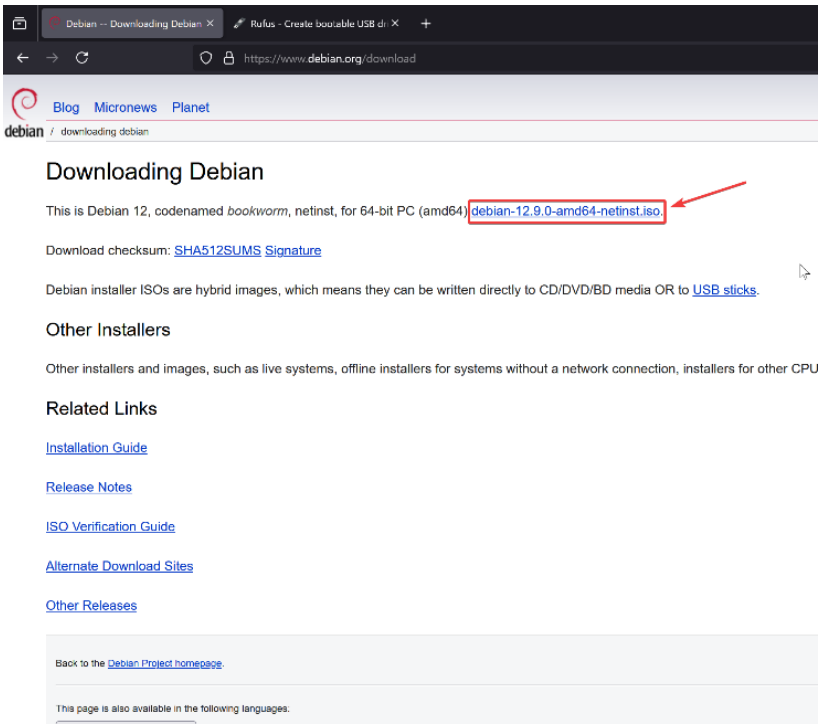
```
service password-encryption
!
hostname AP
!
!
!
aaa new-model
!
aaa group server radius RAD
 server 10.0.0.2 auth-port 1812 acct-port 1813
!
aaa authentication login EAP group radius
!
!
!
dot11 ssid 2.4FH
   vlan 24
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode
   wpa-psk ascii 7 071F205F5D1E161713
   ! ^^ Sets the password
!
dot11 ssid 5GSpaceLasers
   vlan 5
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode
   wpa-psk ascii 7 044B0A151C36435C0D
!
dot11 ssid 5GSpaceLasersEnterprise
   vlan 50
   authentication open eap EAP
   authentication network-eap EAP
   authentication key-management wpa version 2
   mbssid guest-mode
!
!
```

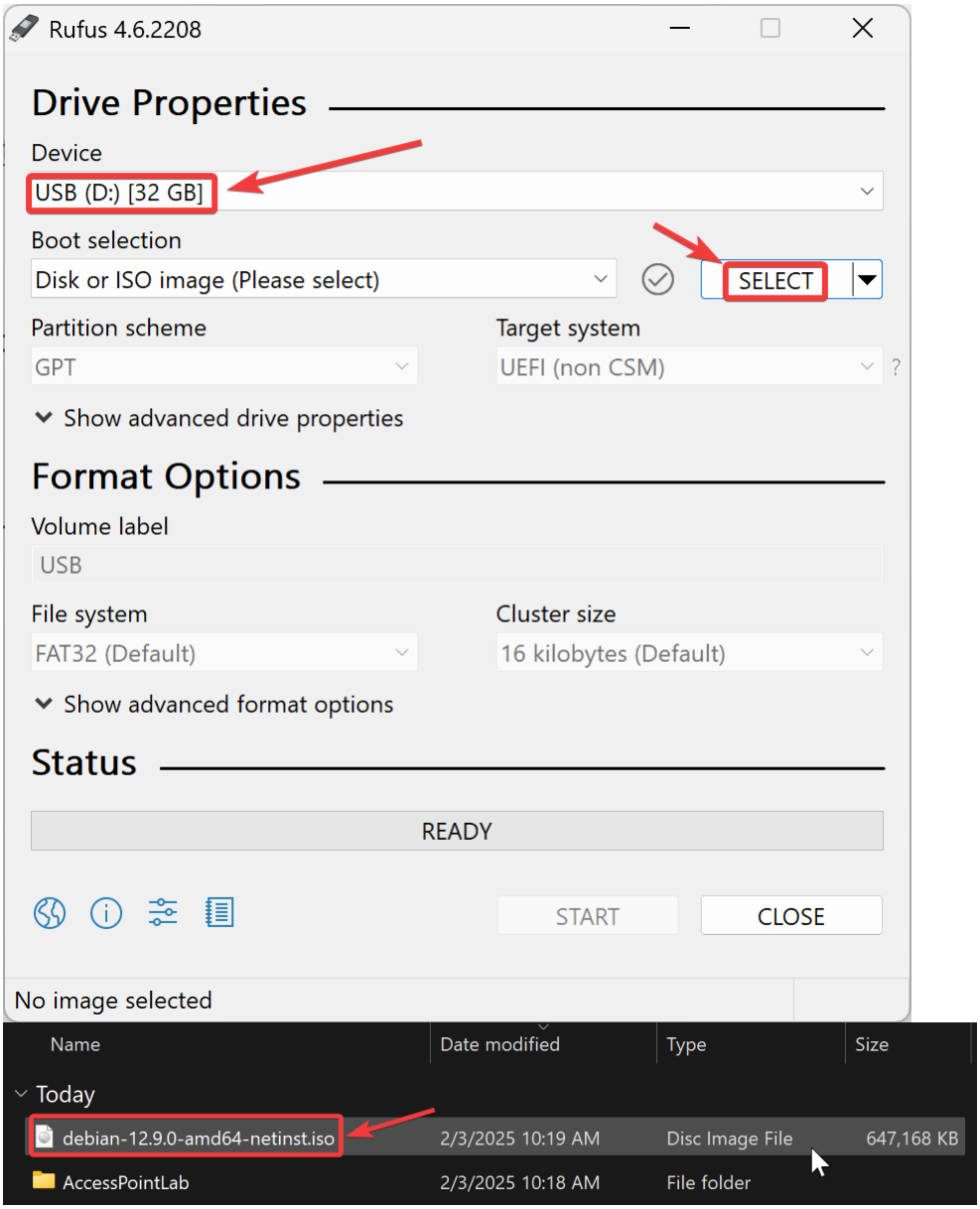
```
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 ip helper-address 10.0.0.1
 ip helper-address 10.0.24.1
 ip helper-address 10.0.5.1
 !
 encryption mode ciphers aes-ccm
 !
 encryption vlan 1 mode ciphers aes-ccm
 !
 encryption vlan 24 mode ciphers aes-ccm
 !
 encryption vlan 5 mode ciphers aes-ccm
 !
 encryption vlan 50 mode ciphers aes-ccm
 !
 ssid 2.4FH
 !
 antenna gain 0
 mbssid
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface Dot11Radio0.24
 encapsulation dot1Q 24
 bridge-group 24
!
!
!
interface Dot11Radio1
 no ip address
 ip helper-address 10.0.0.1
 ip helper-address 10.0.24.1
 ip helper-address 10.0.5.1
 !
 encryption vlan 5 mode ciphers aes-ccm
 !
 encryption vlan 1 mode ciphers aes-ccm
```

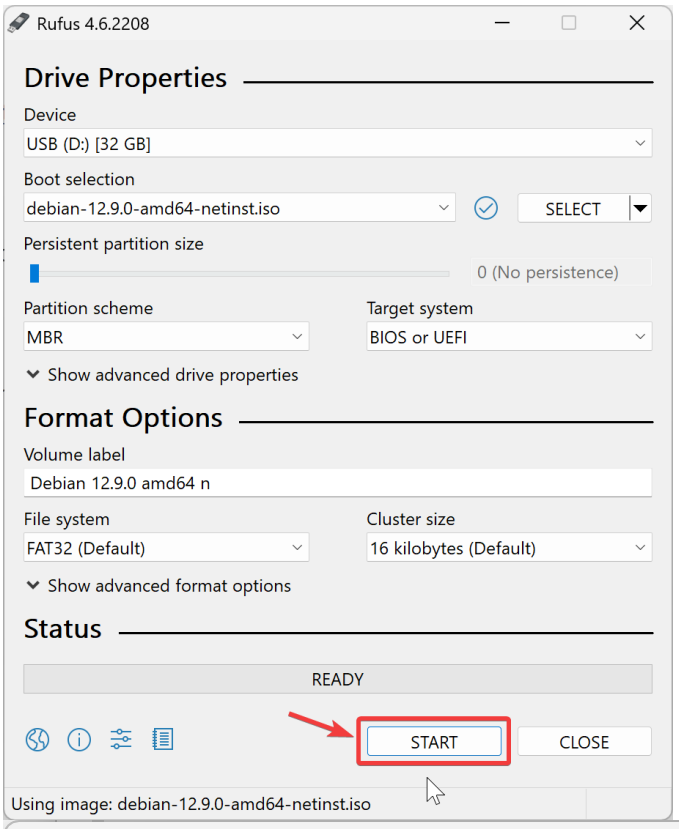
```
 !
 encryption vlan 24 mode ciphers aes-ccm
 !
 encryption vlan 50 mode ciphers aes-ccm
 !
 ssid 5GSpaceLasers
 !
 ssid 5GSpaceLasersEnterprise
 !
 antenna gain 0
 peakdetect
 dfs band 3 block
 mbssid
 channel dfs
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface Dot11Radio1.5
 encapsulation dot1Q 5
 bridge-group 5
!
interface Dot11Radio1.50
 encapsulation dot1Q 50
 bridge-group 50
!
!
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface GigabitEthernet0.5
 encapsulation dot1Q 5
 bridge-group 5
!
interface GigabitEthernet0.24
 encapsulation dot1Q 24
 bridge-group 24
```

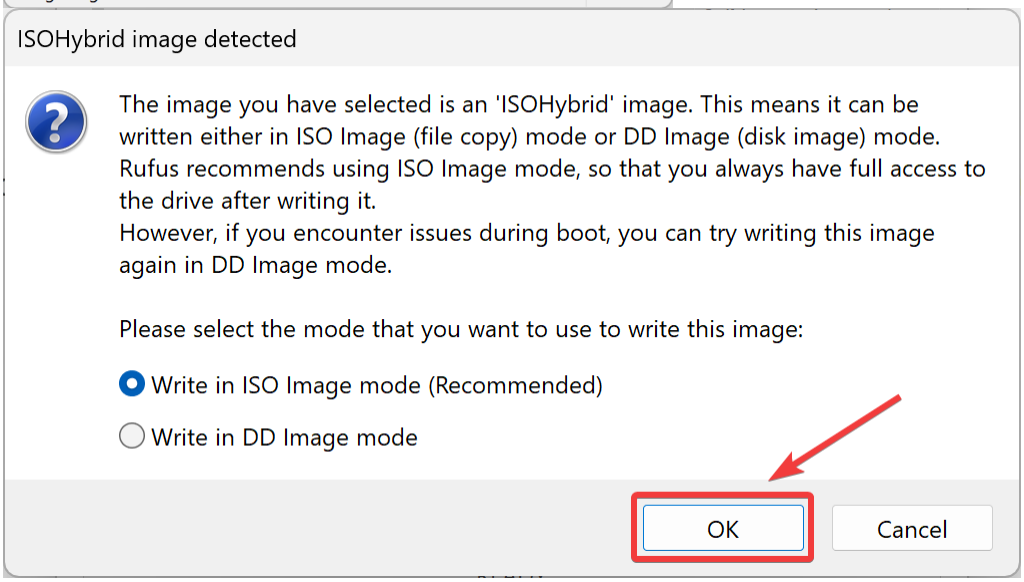
```
!
interface GigabitEthernet0.50
 encapsulation dot1Q 50
 bridge-group 50
!
!
!
interface BVI1
 mac-address 44d3.ca5a.86ac
 ip address 10.0.0.3 255.255.255.0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
!
!
radius-server host 10.0.0.2 auth-port 1812 acct-port 1813 key 7
111918160405041E00
!
bridge 1 route ip
!
!
end
```

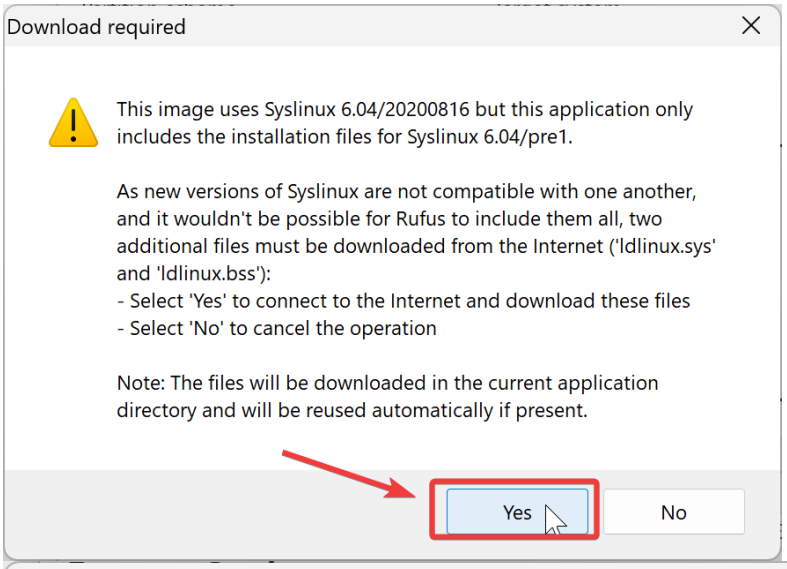
Server Configuration

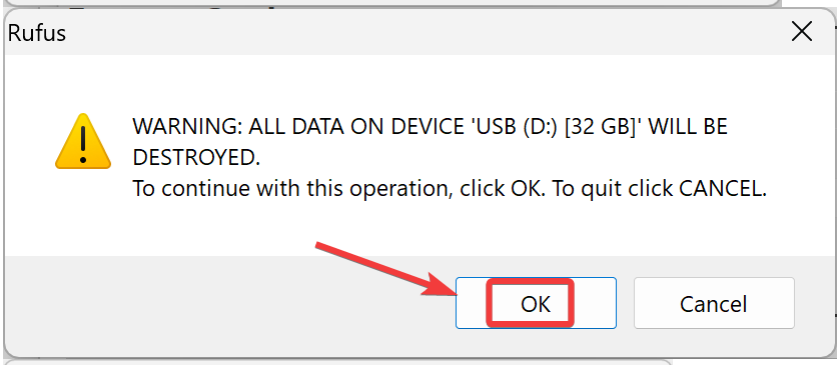


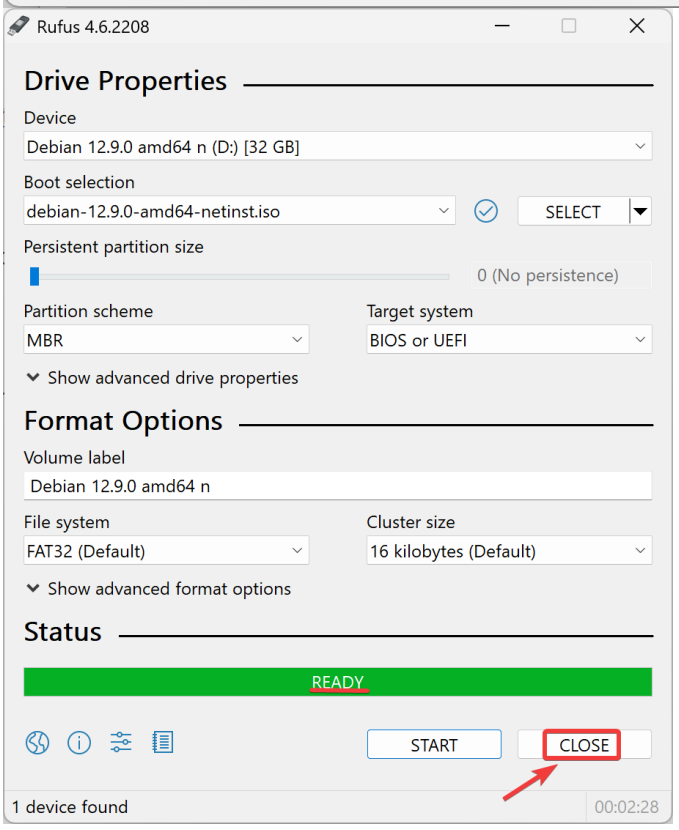

Rufus 4.6.2208
Drive Properties
Device
USB (D:) [32 GB]
Boot selection
Disk or ISO image (Please select)
SELECT
Partition scheme
GPT
Target system
UEFI (non CSM)
Show advanced drive properties
Format Options
Volume label
USB
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Show advanced format options
Status
READY
START
CLOSE
No image selected
Name
Date modified
Type
Size
Today
debian-12.9.0-amd64-netinst.iso
2/3/2025 10:19 AM
Disc Image File
647,168 KB
AccessPointLab
2/3/2025 10:18 AM
File folder

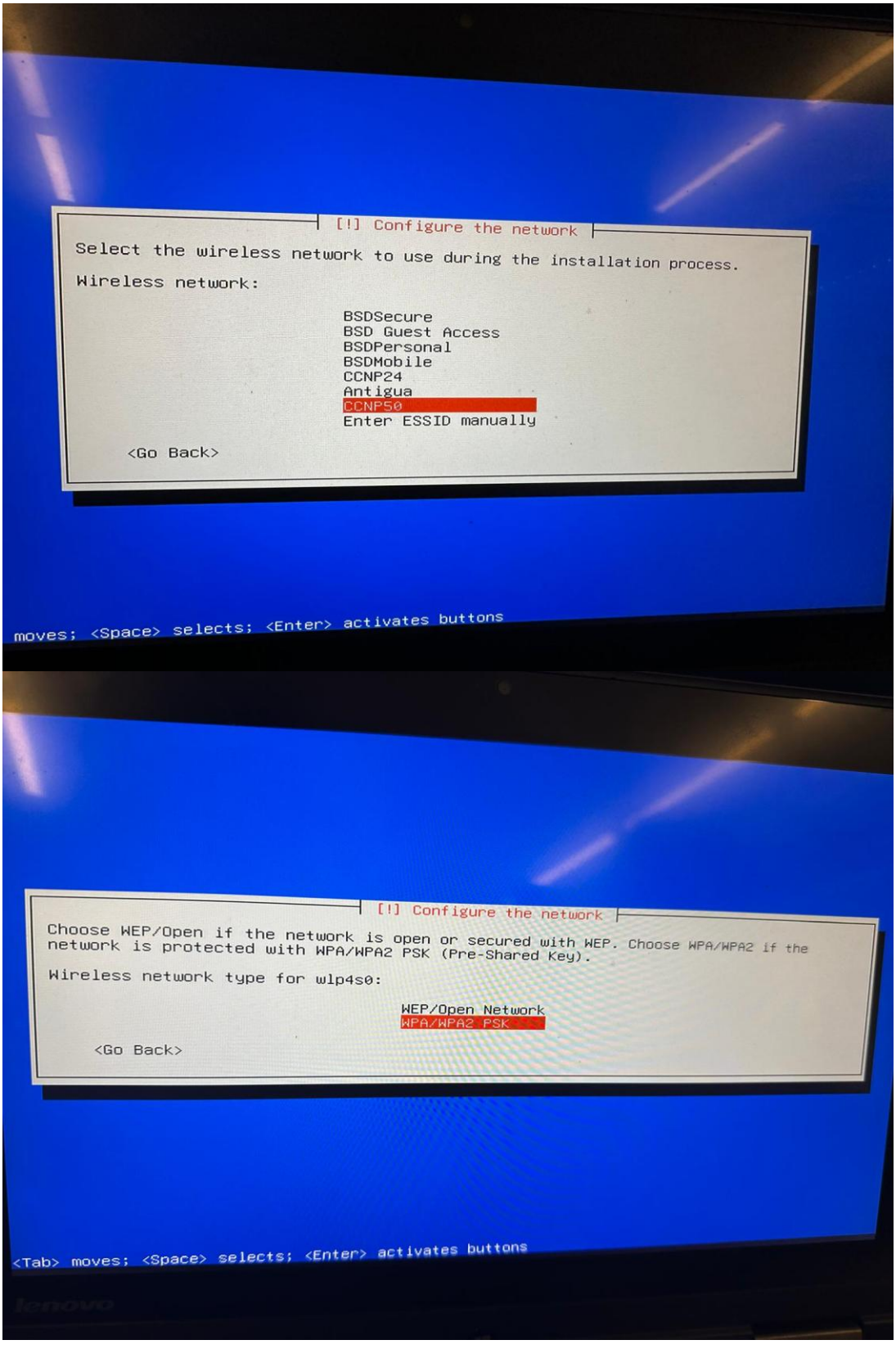

Rufus 4.6.2208
Drive Properties
Device
USB (D:) [32 GB]
Boot selection
debian-12.9.0-amd64-netinst.iso
SELECT
Persistent partition size
0 (No persistence)
Partition scheme
MBR
Target system
BIOS or UEFI
Show advanced drive properties
Format Options
Volume label
Debian 12.9.0 amd64 n
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Show advanced format options
Status
READY
START
CLOSE
Using image: debian-12.9.0-amd64-netinst.iso

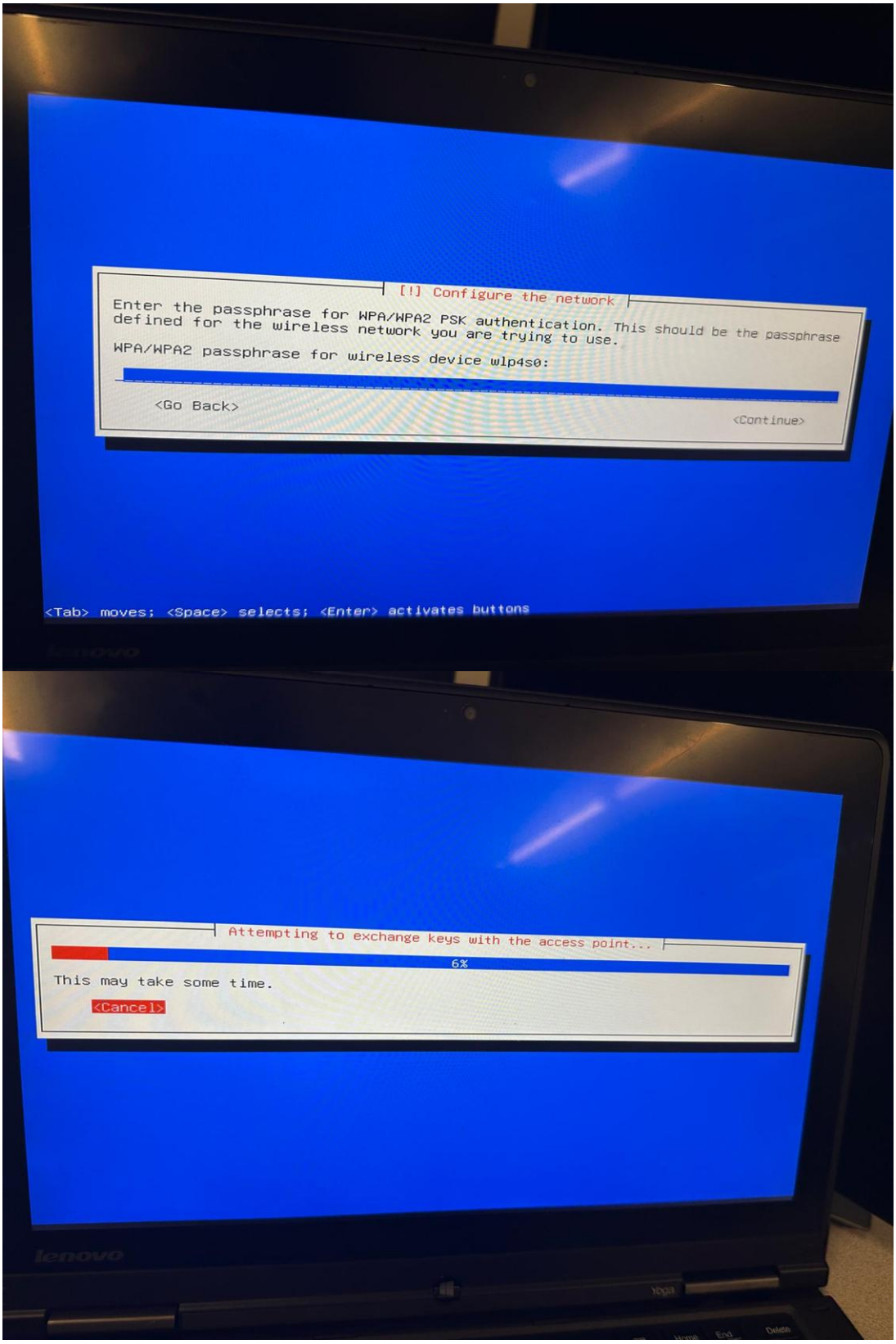

ISOHybrid image detected
The image you have selected is an 'ISOHybrid' image. This means it can be written either in ISO Image (file copy) mode or DD Image (disk image) mode. Rufus recommends using ISO Image mode, so that you always have full access to the drive after writing it.
However, if you encounter issues during boot, you can try writing this image again in DD Image mode.
Please select the mode that you want to use to write this image:
Write in ISO Image mode (Recommended)
Write in DD Image mode
OK
Cancel

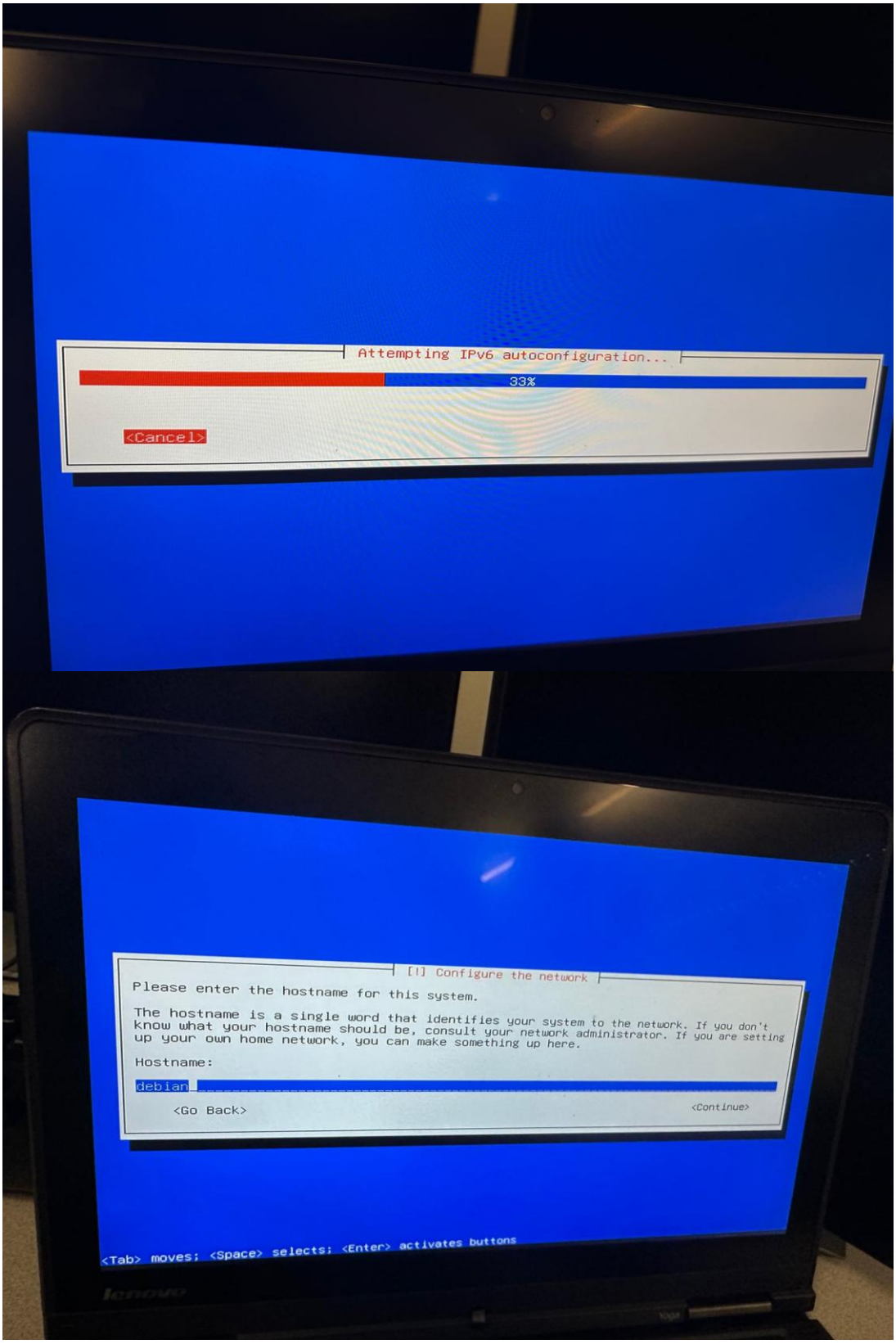

Download required
This image uses Syslinux 6.04/20200816 but this application only includes the installation files for Syslinux 6.04/pre1.
As new versions of Syslinux are not compatible with one another, and it wouldn't be possible for Rufus to include them all, two additional files must be downloaded from the Internet ('ldlinux.sys' and 'ldlinux.bss'):
- Select 'Yes' to connect to the Internet and download these files
- Select 'No' to cancel the operation
Note: The files will be downloaded in the current application directory and will be reused automatically if present.
Yes
No

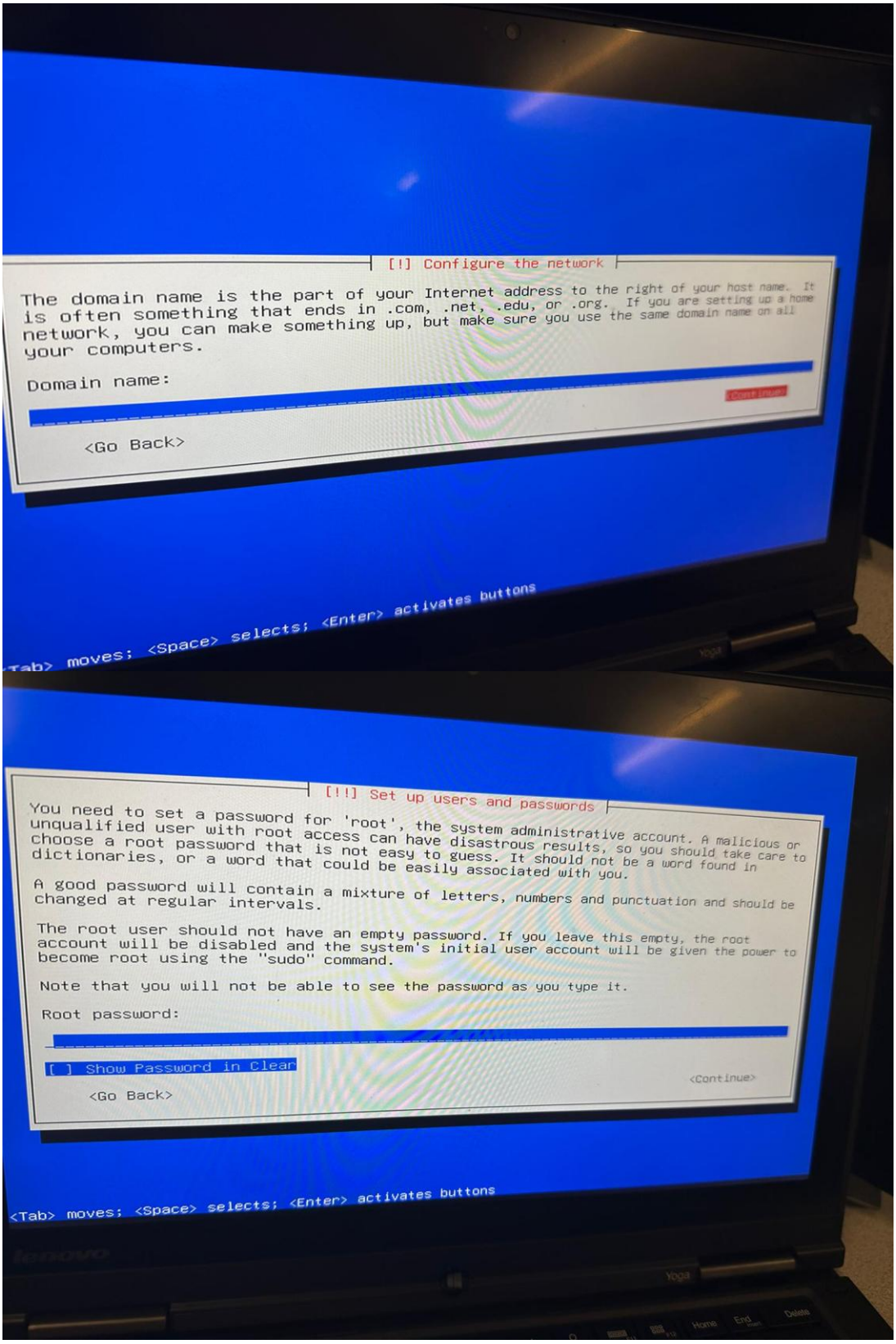

Rufus
WARNING: ALL DATA ON DEVICE 'USB (D:) [32 GB]' WILL BE DESTROYED.
To continue with this operation, click OK. To quit click CANCEL.
OK
Cancel

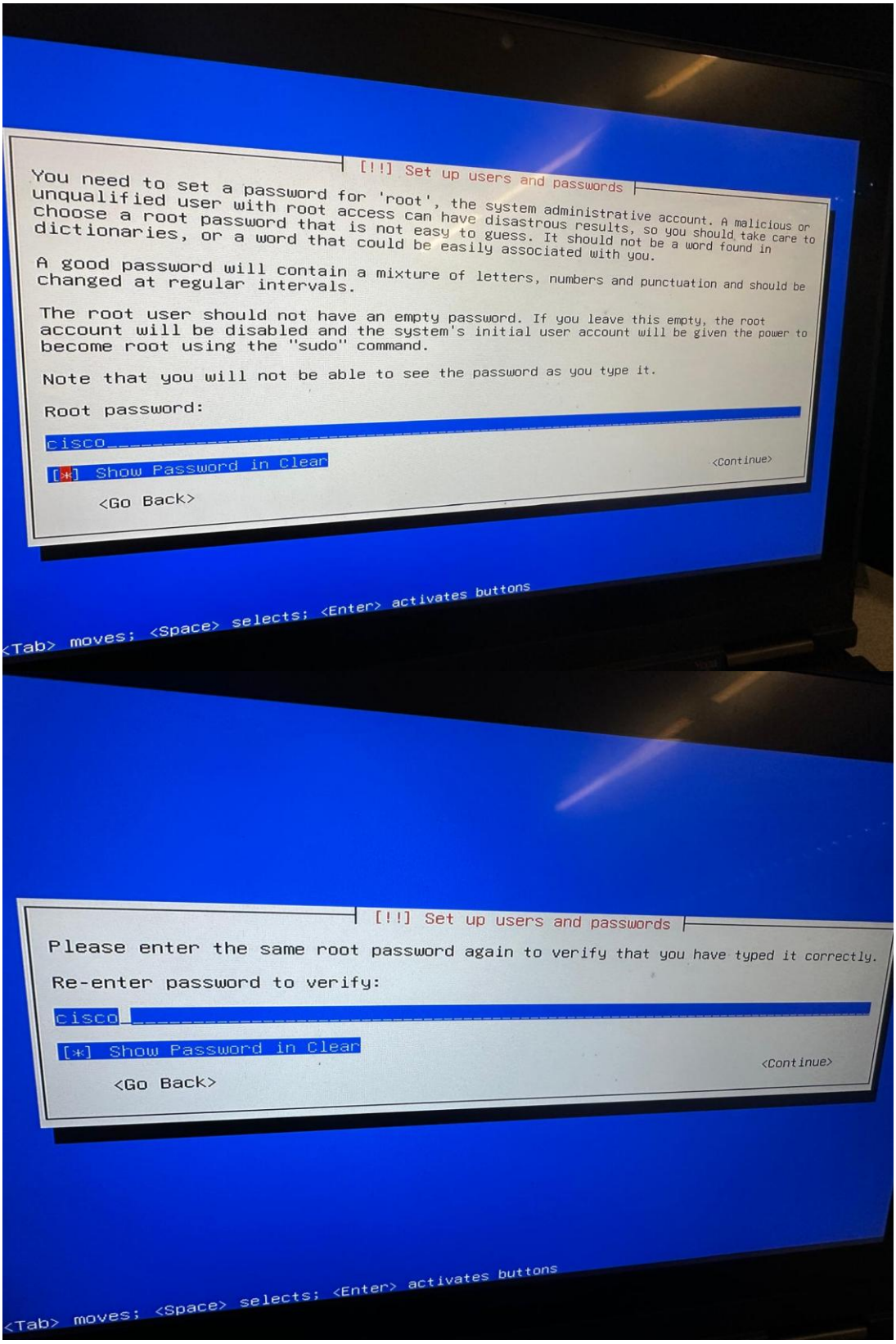

Rufus 4.6.2208
Drive Properties
Device
Debian 12.9.0 amd64 n (D:) [32 GB]
Boot selection
debian-12.9.0-amd64-netinst.iso
SELECT
Persistent partition size
0 (No persistence)
Partition scheme
MBR
Target system
BIOS or UEFI
Show advanced drive properties
Format Options
Volume label
Debian 12.9.0 amd64 n
File system
FAT32 (Default)
Cluster size
16 kilobytes (Default)
Show advanced format options
Status
READY
START
CLOSE
1 device found
00:02:28

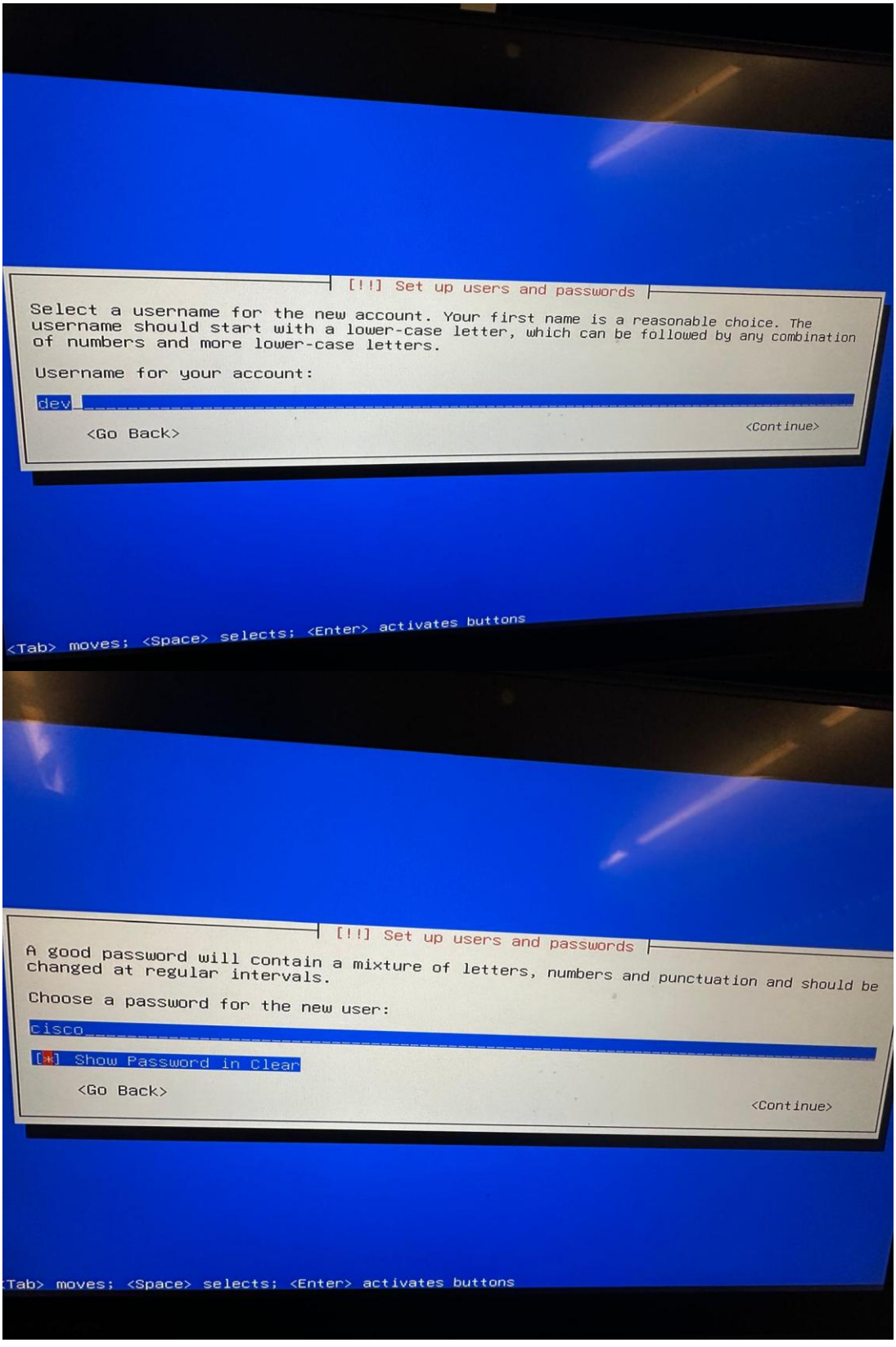

[!] Configure the network
Select the wireless network to use during the installation process.
Wireless network:
BSDSecure
BSD Guest Access
BSDPersonal
BSDMobile
CCNP24
Antigua
CCNP50
Enter ESSID manually
<Go Back>
moves; <Space> selects; <Enter> activates buttons
[!] Configure the network
Choose WEP/Open if the network is open or secured with WEP. Choose WPA/WPA2 if the network is protected with WPA/WPA2 PSK (Pre-Shared Key).
Wireless network type for wlp4s0:
WEP/Open Network
WPA/WPA2 PSK
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

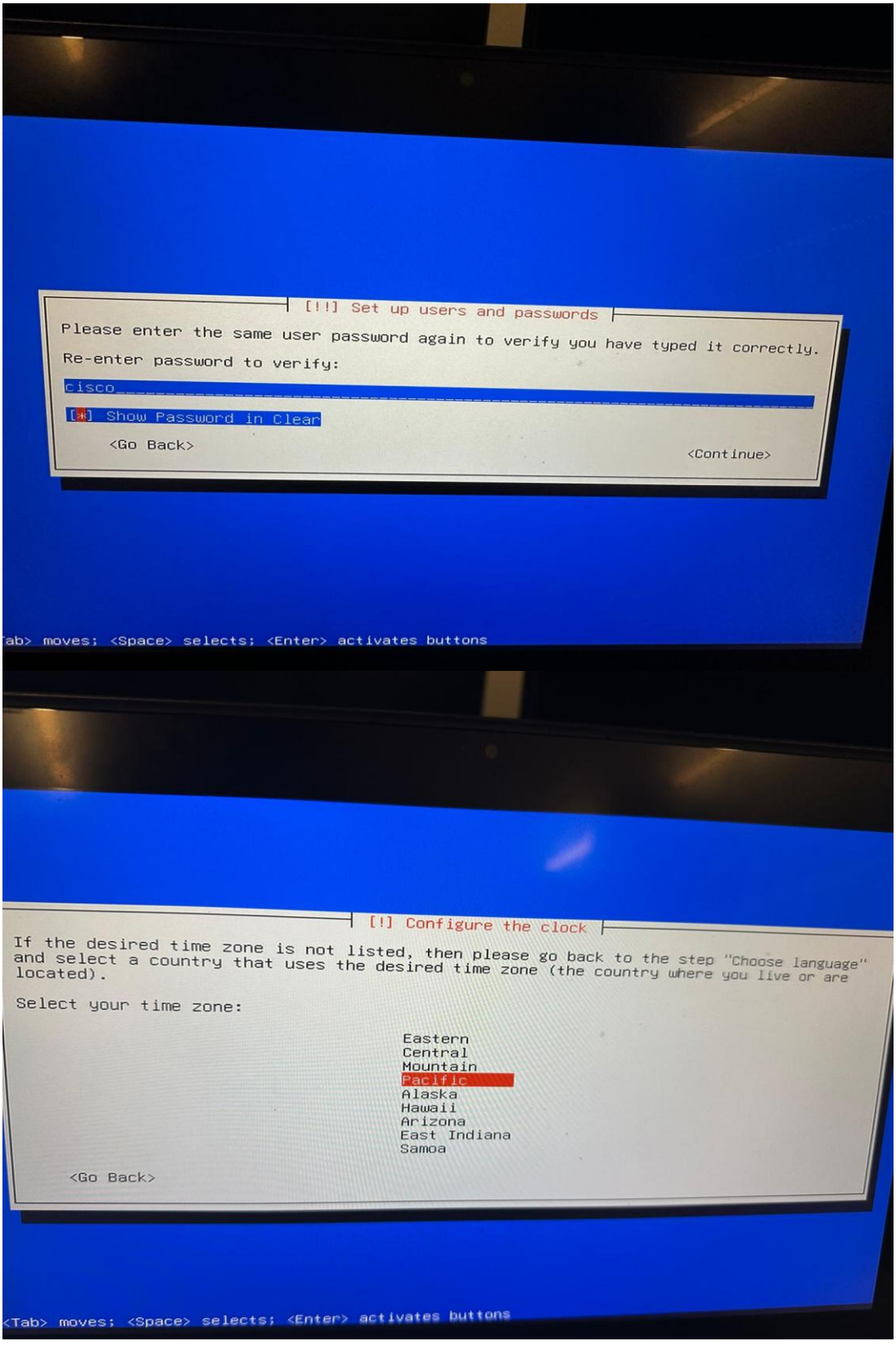

[!] Configure the network
Enter the passphrase for WPA/WPA2 PSK authentication. This should be the passphrase defined for the wireless network you are trying to use.
WPA/WPA2 passphrase for wireless device wlp4s0:
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons
Attempting to exchange keys with the access point...
6%
This may take some time.
<Cancel>

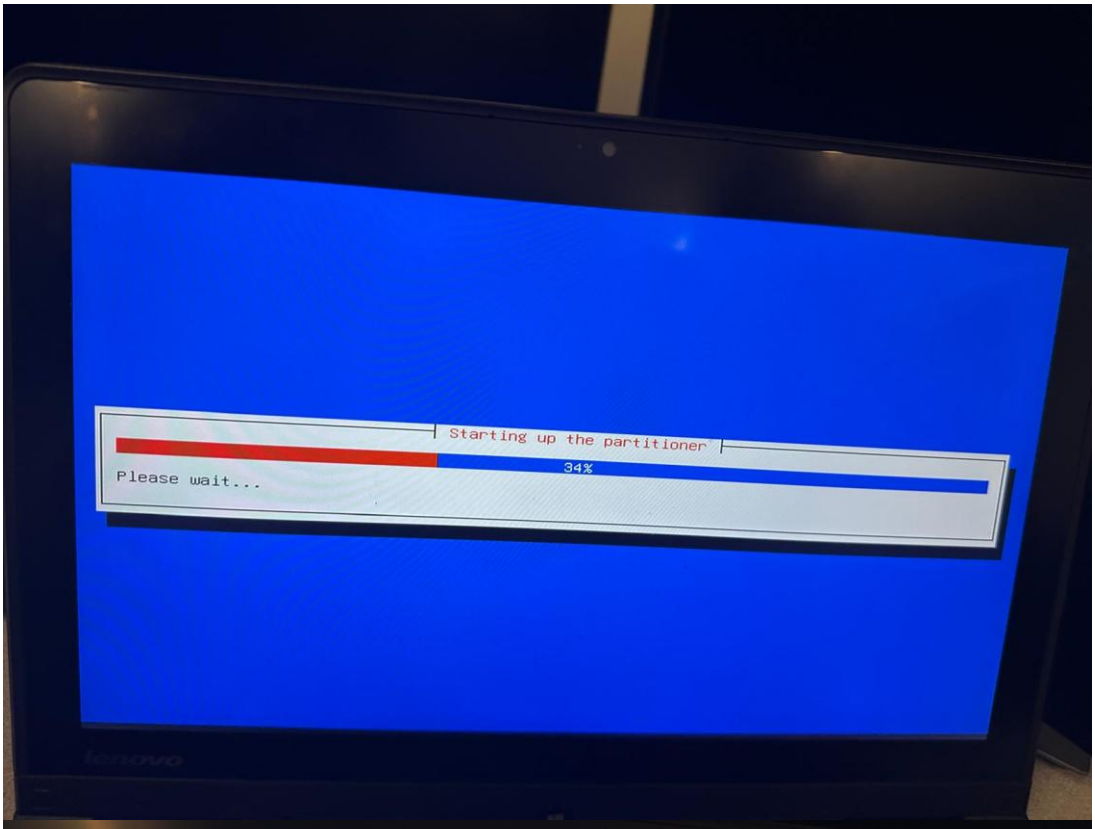

Attempting IPv6 autoconfiguration...
33%
<Cancel>
[!] Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
debian
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

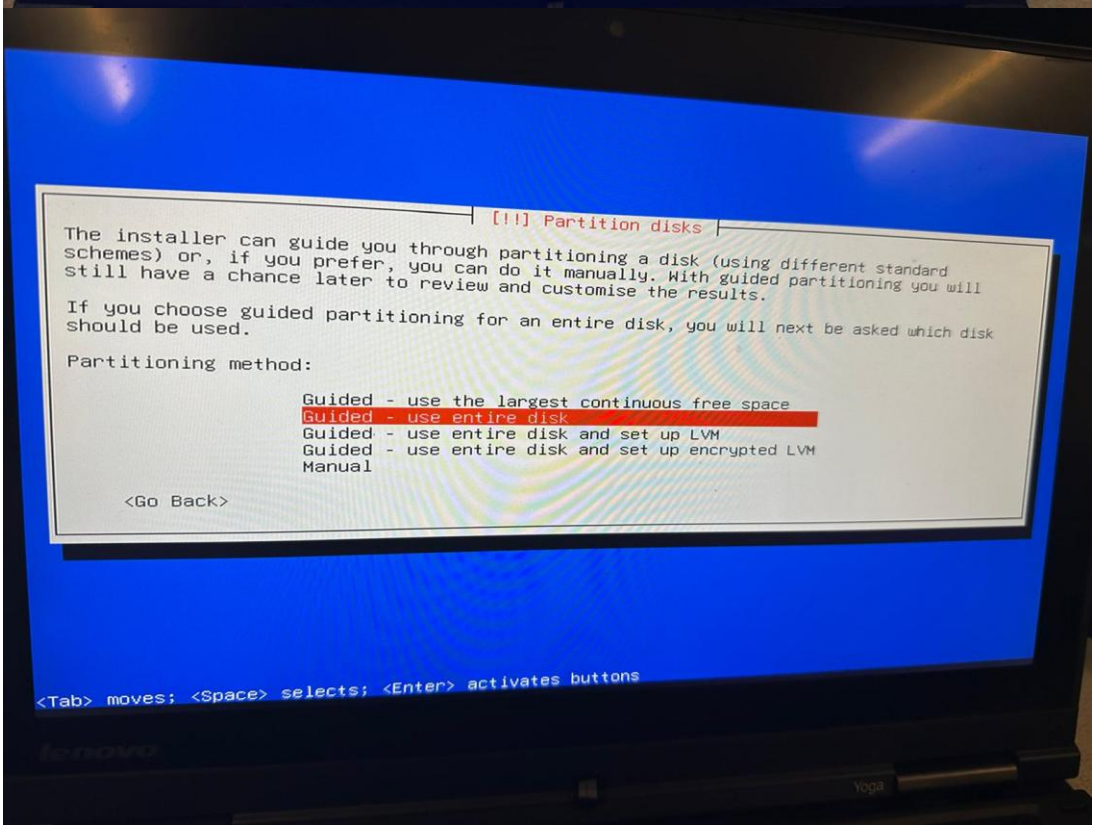

[!] Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.
Domain name:
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
[!!] Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
[ ] Show Password in Clear
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

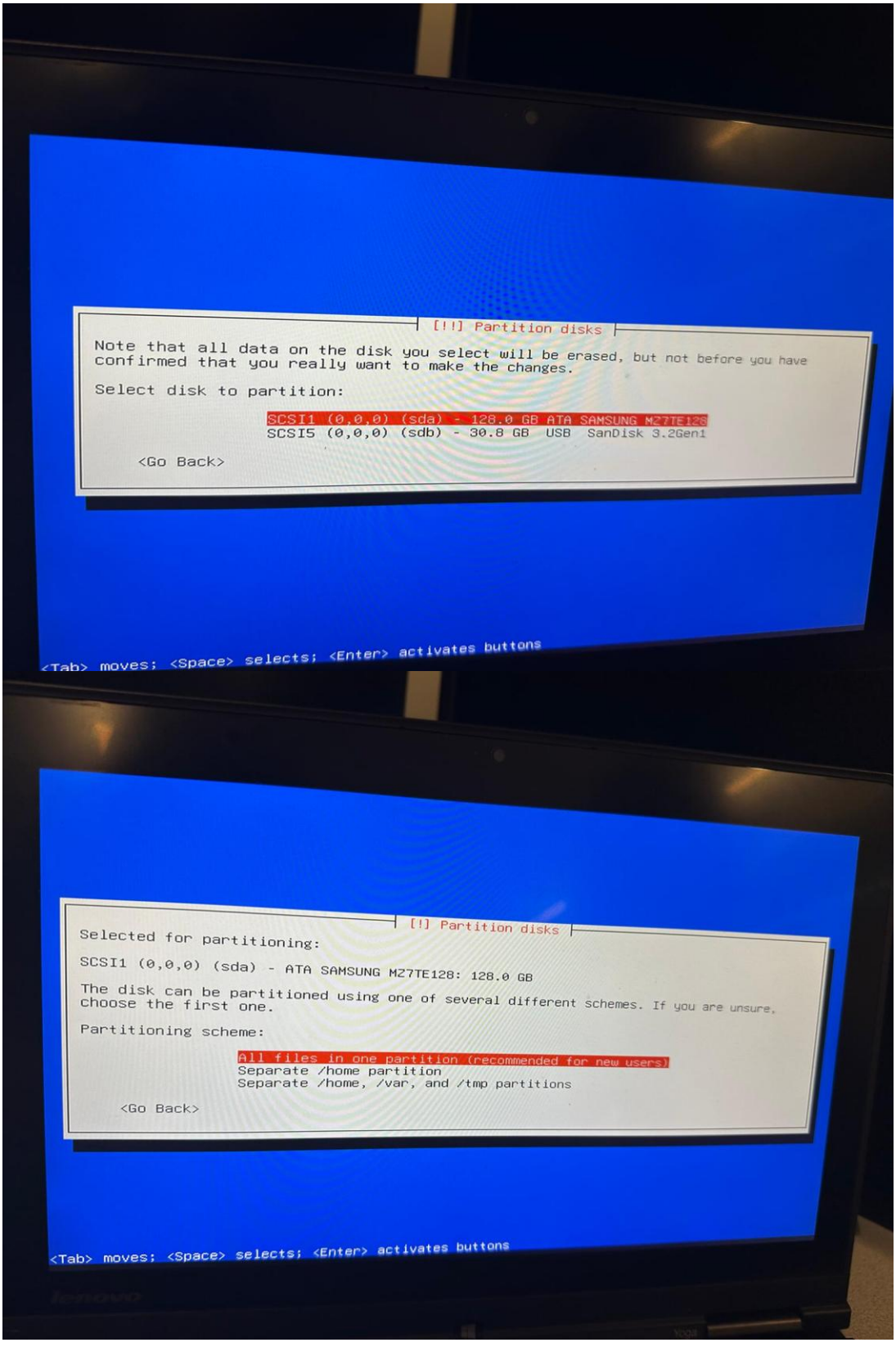

[!!] Set up users and passwords
You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.
Note that you will not be able to see the password as you type it.
Root password:
cisco
[*] Show Password in Clear
<Continue>
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
[!!] Set up users and passwords
Please enter the same root password again to verify that you have typed it correctly.
Re-enter password to verify:
cisco
[*] Show Password in Clear
<Continue>
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

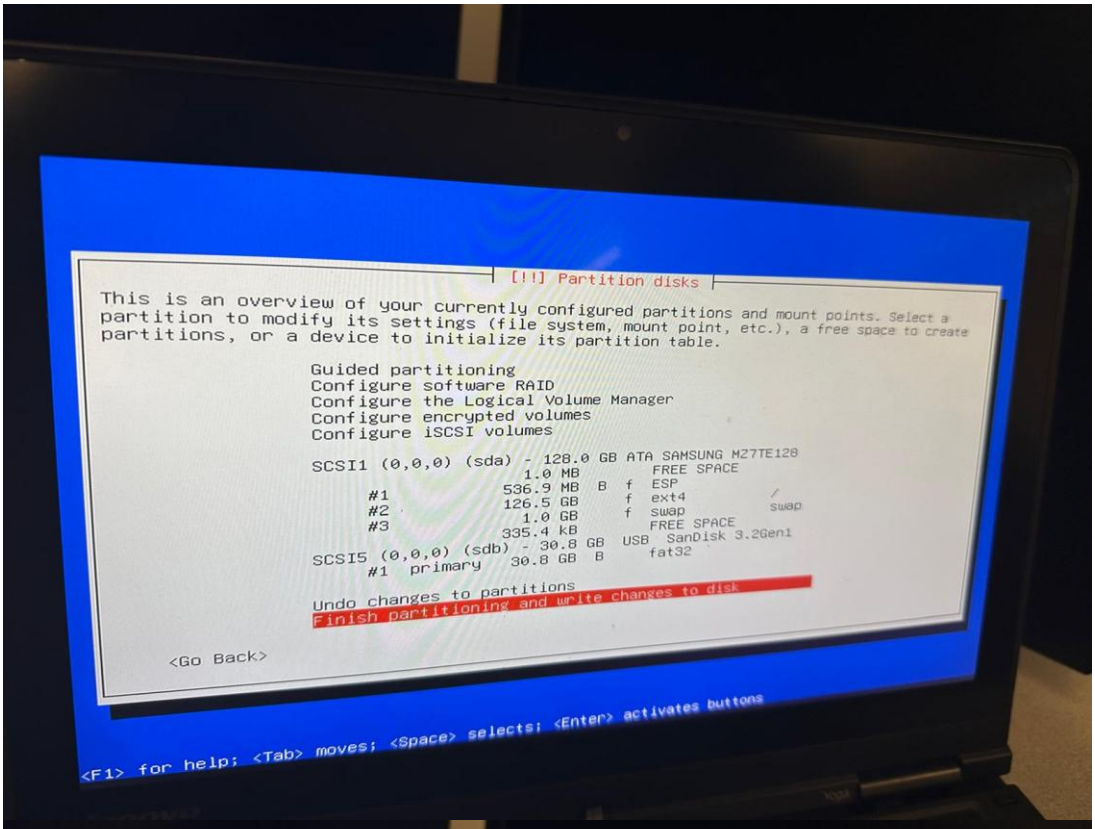

[!!] Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
dev
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons
[!!] Set up users and passwords
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
Choose a password for the new user:
cisco
[ ] Show Password in Clear
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

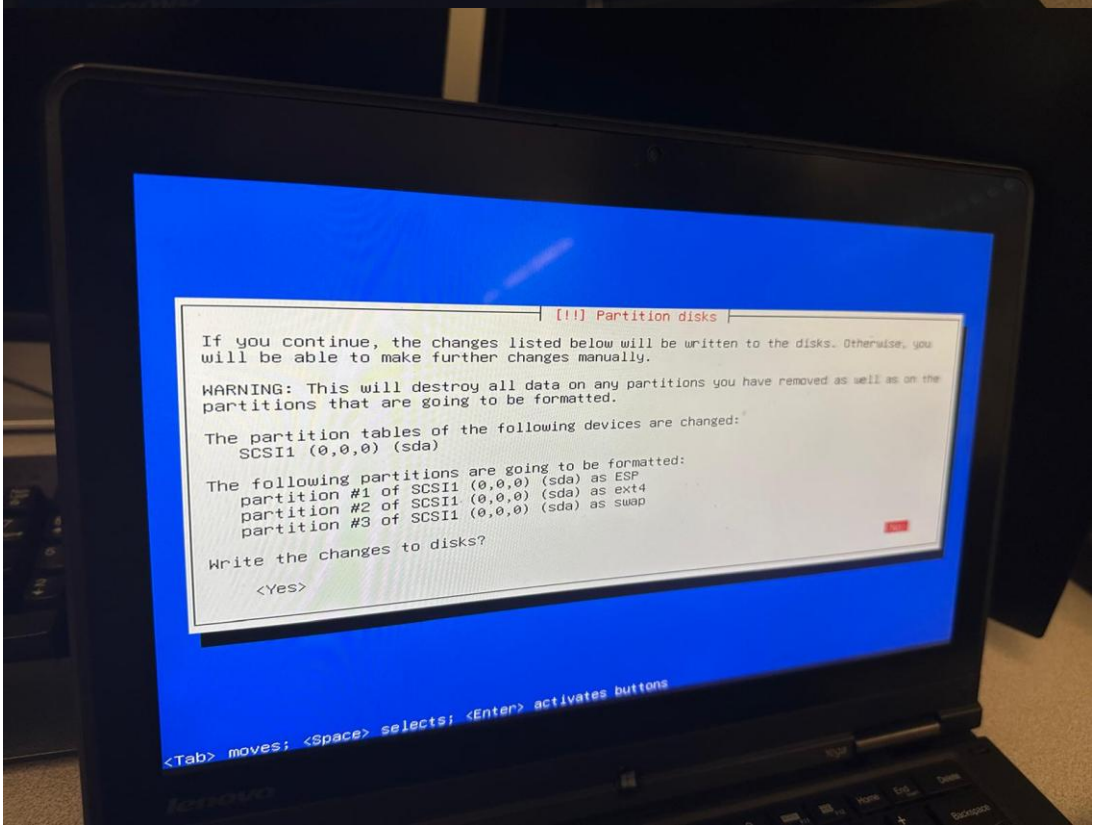

[!!] Set up users and passwords
Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:
cisco
[*] Show Password in Clear
<Go Back>
<Continue>
ab> moves; <Space> selects; <Enter> activates buttons
[!] Configure the clock
If the desired time zone is not listed, then please go back to the step "Choose language"
and select a country that uses the desired time zone (the country where you live or are
located).
Select your time zone:
Eastern
Central
Mountain
Pacific
Alaska
Hawaii
Arizona
East Indiana
Samoa
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

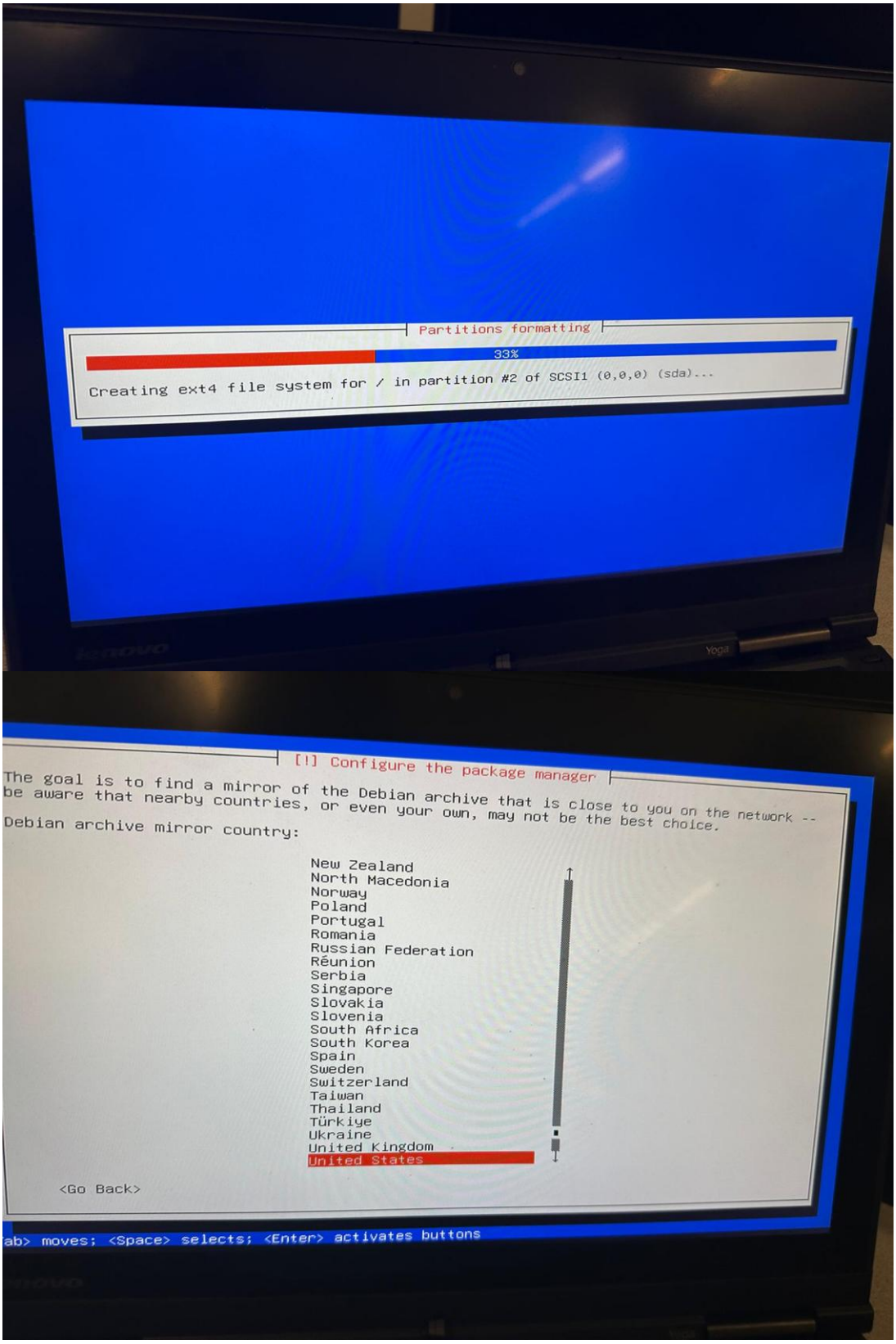

Starting up the partitioner
34%
Please wait...

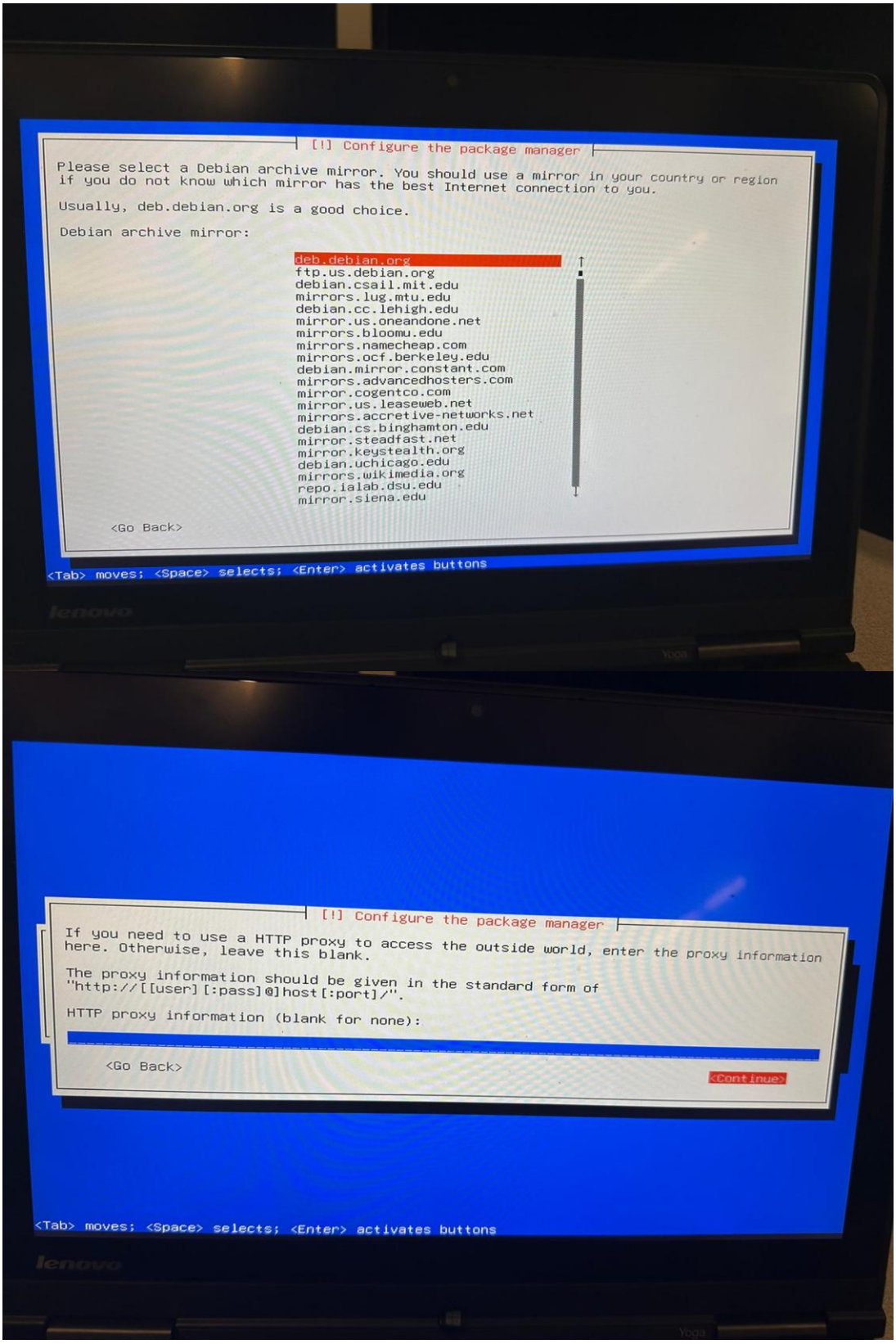

[!!] Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use the largest continuous free space
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI1 (0,0,0) (sda) - 128.0 GB ATA SAMSUNG MZ7TE128
SCSI5 (0,0,0) (sdb) - 30.8 GB USB SanDisk 3.2Gen1
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
[!] Partition disks
Selected for partitioning:
SCSI1 (0,0,0) (sda) - ATA SAMSUNG MZ7TE128: 128.0 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons

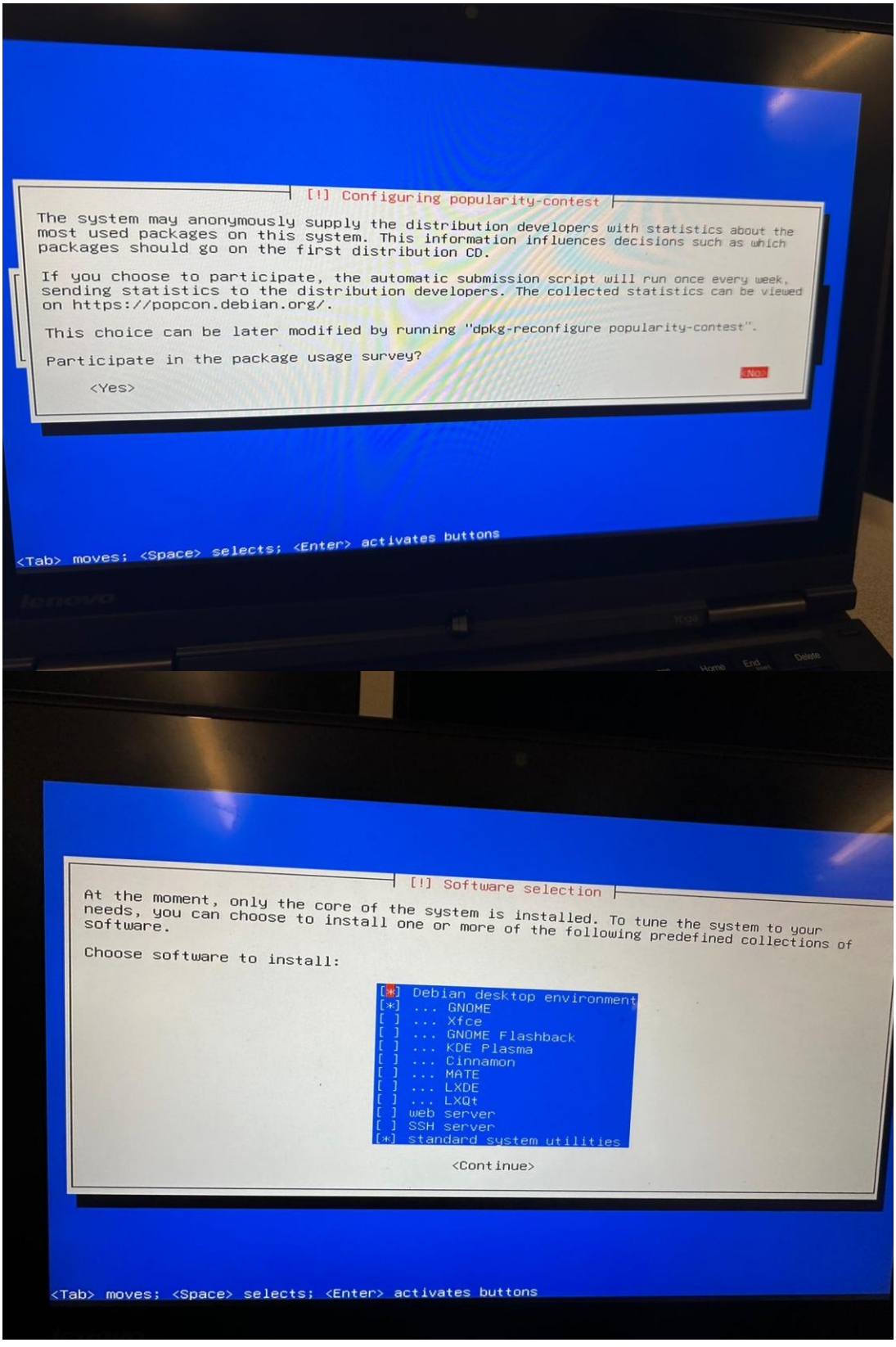

[!!] Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI1 (0,0,0) (sda) - 128.0 GB ATA SAMSUNG M27TE128
1.0 MB FREE SPACE
#1 536.9 MB B f ESP
#2 126.5 GB f ext4 /
#3 1.0 GB f swap swap
335.4 kB FREE SPACE
SCSI5 (0,0,0) (sdb) - 30.8 GB USB SanDisk 3.2Gen1
#1 primary 30.8 GB B fat32
Undo changes to partitions
Finish partitioning and write changes to disk
<Go Back>
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

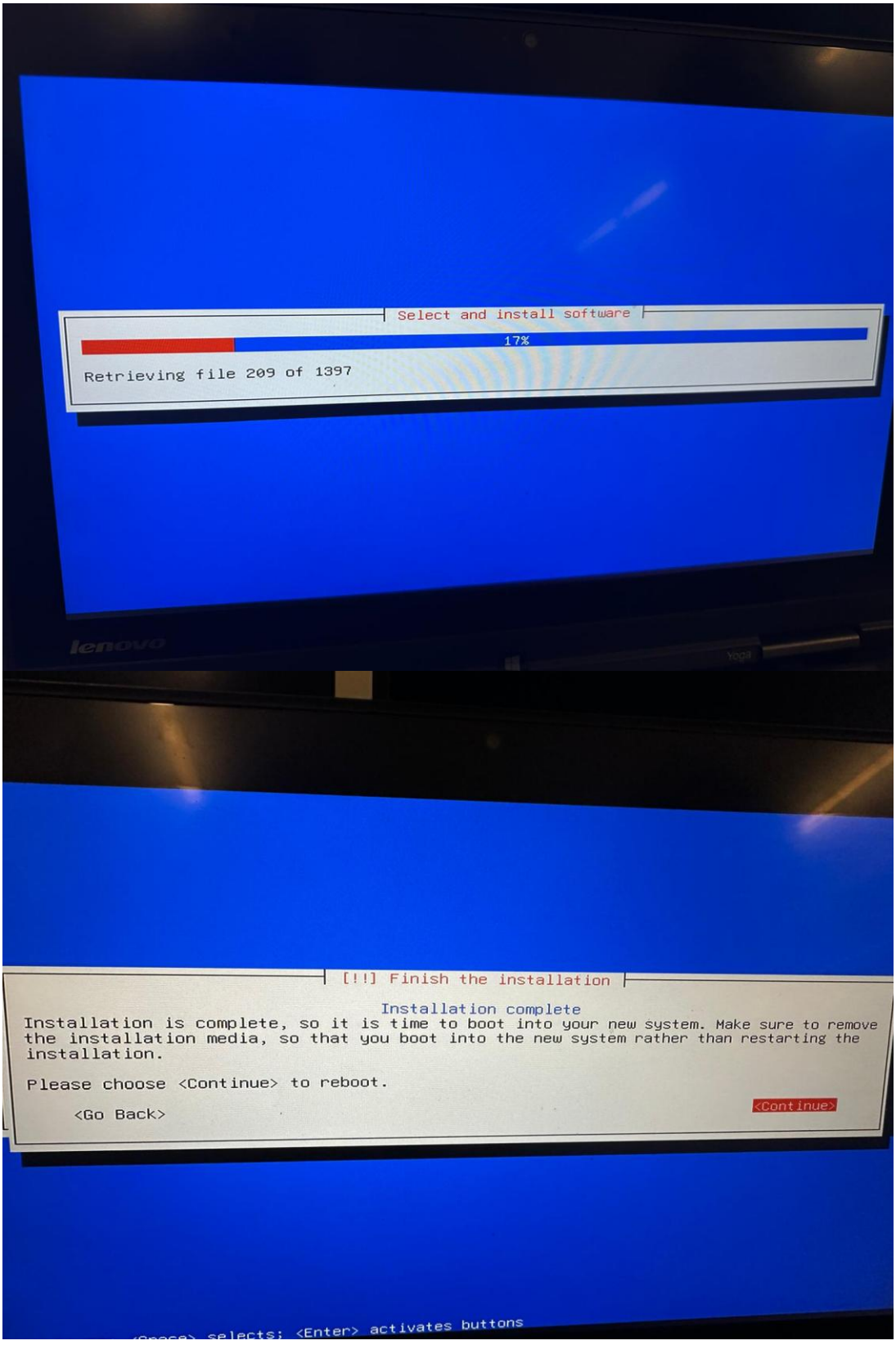

[!!] Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
WARNING: This will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted.
The partition tables of the following devices are changed:
SCSI1 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI1 (0,0,0) (sda) as ESP
partition #2 of SCSI1 (0,0,0) (sda) as ext4
partition #3 of SCSI1 (0,0,0) (sda) as swap
Write the changes to disks?
<Yes>
<Tab> moves; <Space> selects; <Enter> activates buttons

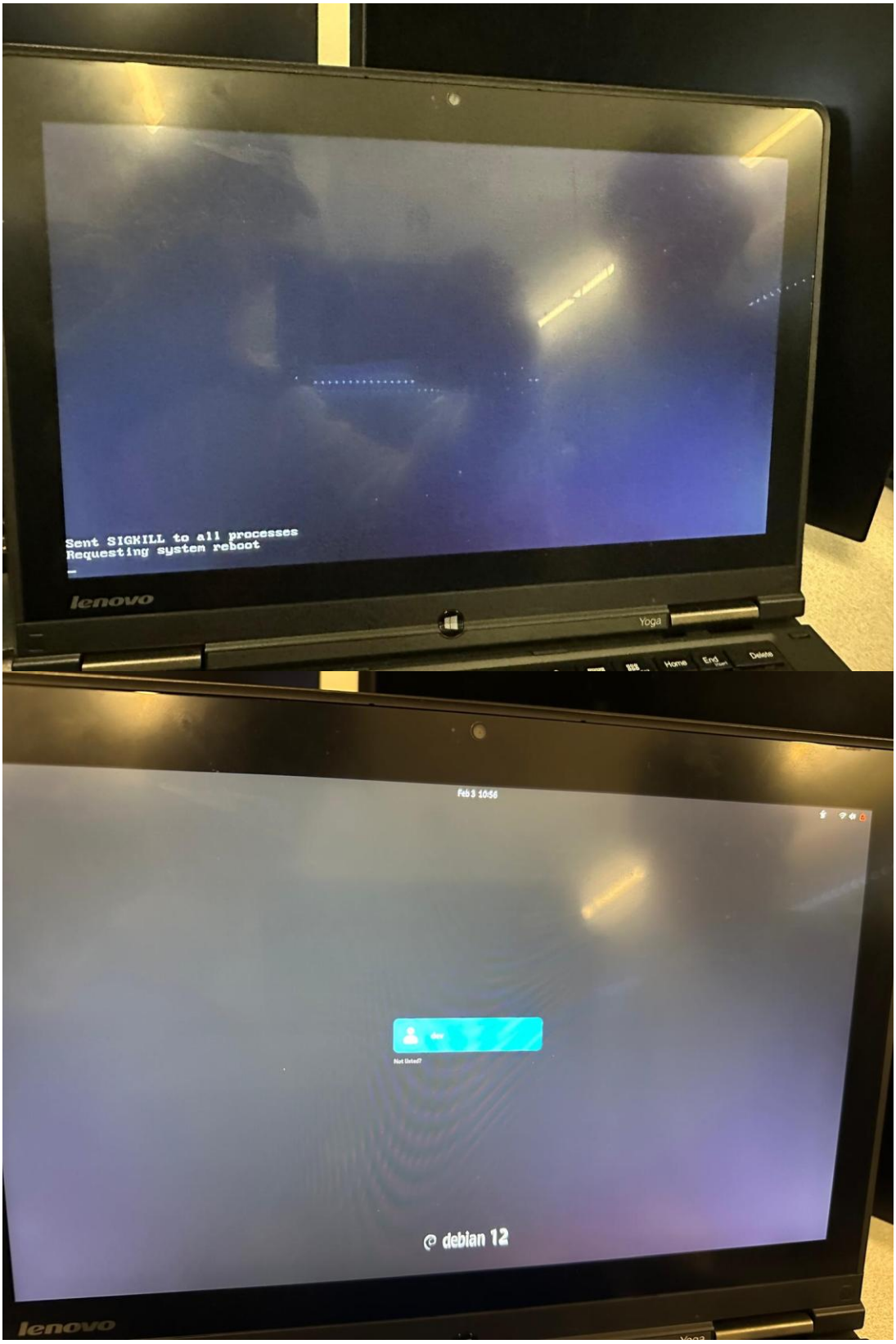

Partitions formatting
33%
Creating ext4 file system for / in partition #2 of SCSI1 (0,0,0) (sda)...
[!] Configure the package manager
The goal is to find a mirror of the Debian archive that is close to you on the network --
be aware that nearby countries, or even your own, may not be the best choice.
Debian archive mirror country:
New Zealand
North Macedonia
Norway
Poland
Portugal
Romania
Russian Federation
Réunion
Serbia
Singapore
Slovakia
Slovenia
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Türkiye
Ukraine
United Kingdom
United States
<Go Back>
ab> moves; <Space> selects; <Enter> activates buttons

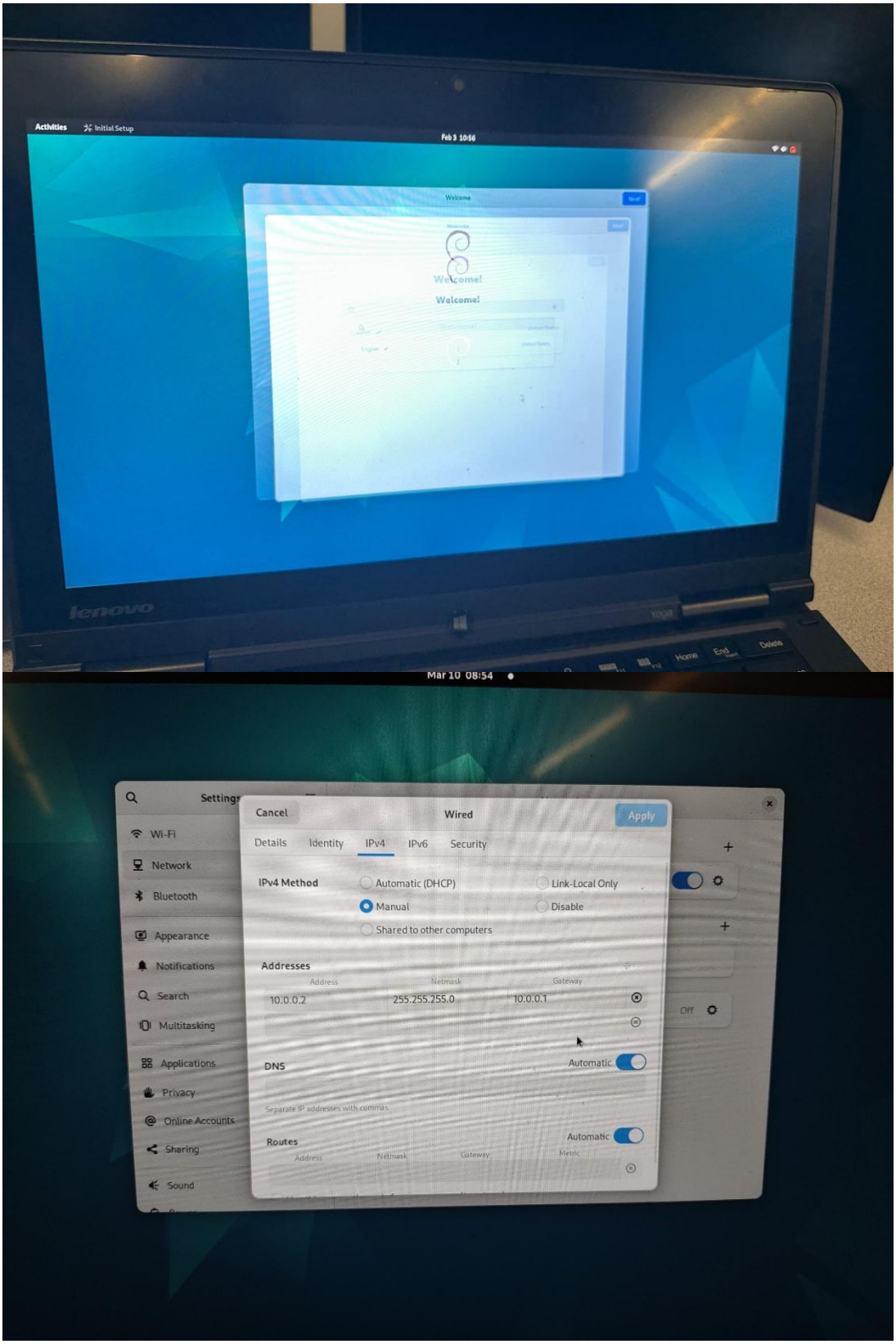

[!] Configure the package manager
Please select a Debian archive mirror. You should use a mirror in your country or region if you do not know which mirror has the best Internet connection to you.
Usually, deb.debian.org is a good choice.
Debian archive mirror:
deb.debian.org
ftp.us.debian.org
debian.csail.mit.edu
mirrors.lug.mtu.edu
debian.cc.lehigh.edu
mirror.us.oneandone.net
mirrors.bloomu.edu
mirrors.namecheap.com
mirrors.ocf.berkeley.edu
debian.mirror.constant.com
mirrors.advancedhosters.com
mirror.cogentco.com
mirror.us.leaseweb.net
mirrors.accretive-networks.net
debian.cs.binghamton.edu
mirror.steadfast.net
mirror.keystealth.org
debian.uchicago.edu
mirrors.wikimedia.org
repo.ialab.dsu.edu
mirror.siena.edu
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
lenovo

[!] Configure the package manager
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
HTTP proxy information (blank for none):
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons
lenovo


[!] Configuring popularity-contest
The system may anonymously supply the distribution developers with statistics about the most used packages on this system. This information influences decisions such as which packages should go on the first distribution CD.
If you choose to participate, the automatic submission script will run once every week, sending statistics to the distribution developers. The collected statistics can be viewed on https://popcon.debian.org/.
This choice can be later modified by running "dpkg-reconfigure popularity-contest".
Participate in the package usage survey?
<Yes>
<No>
<Tab> moves; <Space> selects; <Enter> activates buttons
[!] Software selection
At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.
Choose software to install:
[*] Debian desktop environment
[*] ... GNOME
[ ] ... Xfce
[ ] ... GNOME Flashback
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[ ] web server
[ ] SSH server
[*] standard system utilities
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons


Select and install software
17%
Retrieving file 209 of 1397
lenovo
[!!] Finish the installation
Installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.
Please choose <Continue> to reboot.
<Go Back>
<Continue>
<Enter> activates buttons


Sent SIGKILL to all processes
Requesting system reboot
lenovo
Yoga
Home
End
Delete
Feb 3 10:56
debian 12
lenovo


Activities
Initial Setup
Feb 3 10:56
Welcome
Next
Welcome!
Welcome!
lenovo
Home
End
Delete
Mar 10 08:54
Settings
Wi-Fi
Network
Bluetooth
Appearance
Notifications
Search
Multitasking
Applications
Privacy
Online Accounts
Sharing
Sound
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
IPv4 Method
Automatic (DHCP)
Link-Local Only
Manual
Disable
Shared to other computers
Addresses
Address
Netmask
Gateway
10.0.0.2
255.255.255.0
10.0.0.1
DNS
Automatic
Separate IP addresses with commas
Routes
Automatic
Address
Netmask
Gateway
Metric
Off

FreeRADIUS Configuration

```
# lines with "#" are comments
# some comments will explain how to do something or
# tell you to do something

su -l
adduser <user> sudo
sudo apt install freeradius

# Confirm installation of freeRADIUS

cd /etc/systemd
sudo nano logind.conf

# Set HandleLidSwitch to ignore and uncomment the line
# Purpose: make a laptop running freeRADIUS doesn't sleep when the lid
is closed.

# Note: depending on the version of freeRADIUS or the distro of linux,
# freeradius configuration files could be stored in other locations.
cd /etc/system/freeradius/3.0
sudo nano clients.conf

# Add a client. For example:
# client apFH {
#          ipaddr = 10.0.0.3
#          require_message_authenticator = no
#          secret = password
#          nas_type = "other"
#          proto = "*"
# }

cd /etc/system/freeradius/3.0/mods-config/files
sudo nano authorize

# Add some users. For example:
# admin    Cleartext-Password := "password"
#               Reply-Message := "Hello, %{User-Name}"
#
# username Cleartext-Password := "password"
#               Reply-Message := "Hello, %{User-Name}"


sudo systemctl start freeradius
```