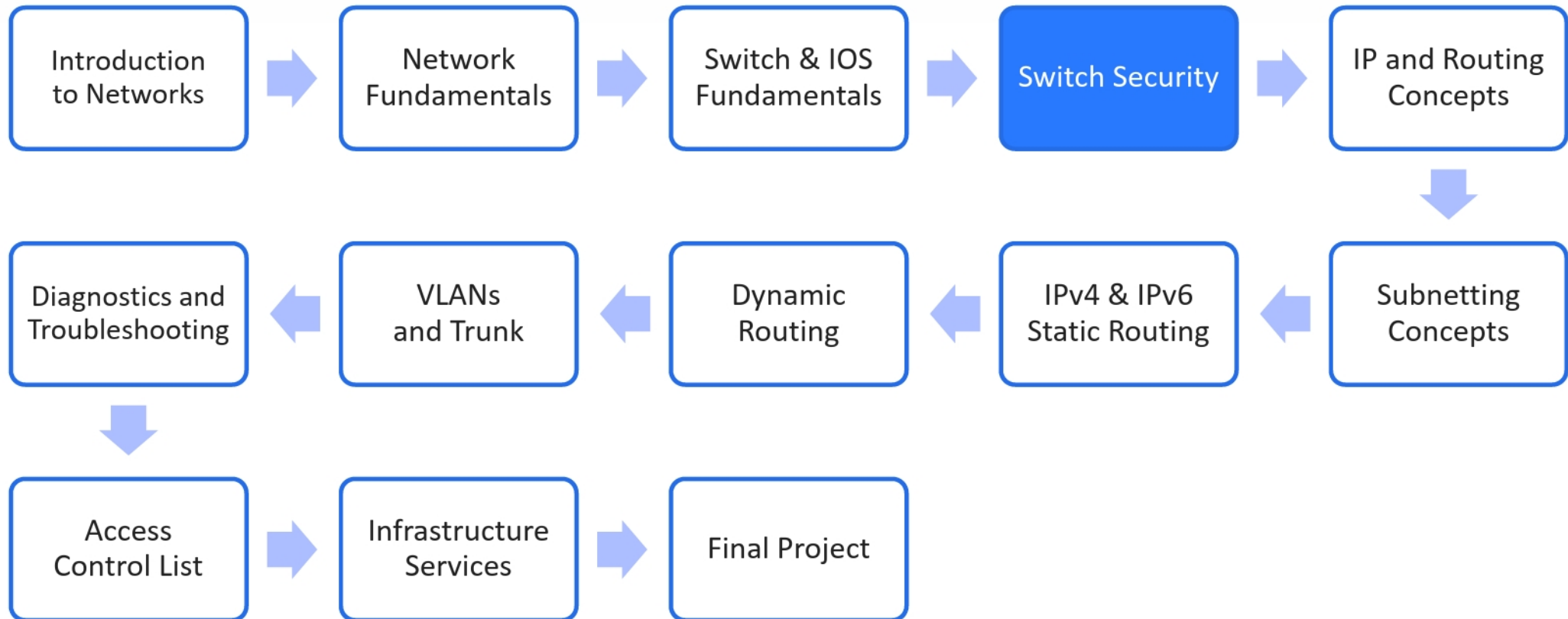


Cybersecurity Professional Program

SWITCH SECURITY

Computer Networking

Computer Networking Course Path



Overview

Lesson Objective

The objective of this lesson is to learn new ways to secure a switch from unwanted access. The lesson explains how the Port Security feature helps prevent access by unauthorized MAC addresses, and how to establish secure connections over the network.



Port Security

Remote Access

Switch Security

PORT SECURITY

Risks in a Switched Environment

MAC Spoofing



MAC spoofing is when attackers change their own physical PC address to conceal their true identity and pose as someone else. For example, an attacker may spoof a MAC address with a legitimate MAC address, to bypass an access control mechanism, such as port security.



CAM Table Overflow



CAM Table Overflow is an attack that targets a switch's MAC table. The idea is to flood the table with a large number of fake addresses. When the list of addresses exceeds the maximum size of the table, the switch will initiate its fallback mode and begin to act as a hub, meaning every frame will be forwarded to every host on the network.



Port Security

Overview



The Port Security feature is used to restrict input to an interface by limiting MAC addresses of workstations that are allowed to access a specific port.

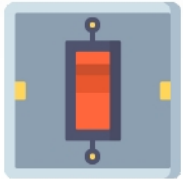
When secure MAC addresses are assigned to a port, the port will not forward packets with source addresses outside the defined group.



By default, port security is not defined on switches and requires configuration.

Violation Modes

Shutdown



This is the default violation mode. When a violation occurs, the port will be shut down and logged automatically. The port must then be reset manually to become operational again.

Restrict



In case of a violation, Ethernet frames with unauthorized source MAC addresses are dropped. The switch provides notification of security violations and keeps count of the number of violations.

Protect



In case of a violation, Ethernet frames with unauthorized source MAC addresses are dropped. In this violation mode, the switch does not provide notification regarding the event.

The port security feature includes three protection modes to handle incidents in which it receives an Ethernet frame with a restricted MAC address.

Manual Vs. Sticky

MAC address learning can be performed in one of two ways: Manual or Sticky.

Manual



The manual method requires static configuration of each allowed MAC address and its assignment to an interface. This is the most secure method, but it is very time consuming and open to faulty configuration.



Sticky



In the sticky method, allowed MAC addresses are learned dynamically and are limited to the maximum number configured for the interface. The switch learns the source address of the first few devices associated with the interface, providing a fast and scalable method of operation.



Max & Err-Disabled

Max Allowed MAC Addresses



Although the number of default MAC addresses allowed in Port Security is one, the number can be changed within the range of 1 to 3072.



Err-disabled



When a switch port is in Err-disabled mode, the port may have been disabled automatically by the switch operating system, due to port security shutdown mode violation.



Port Status

```
Switch# show interfaces  
fastEthernet 0/1 status
```

Port	Status
Fa0/1	err-disabled



To determine if Err-disabled was turned off for a port, run the **show interfaces [interface] status** command.

Common Triggers for Err-disabled

Duplex Mismatch



This state occurs when two parties, set for point-to-point communication, are configured to use different duplex modes.

Bad NIC



A faulty network interface card with software or hardware issues may trigger the Err-disabled state.

Broadcast Storms



When there is a broadcast volume too large for processing in the broadcast domain, the switches may be overwhelmed and trigger the err-disabled mode on their ports.



```
show interfaces fastEthernet 0/1
fEthernet0/1 is down, line protocol is down (err-disabled)
hardware is Lance, address is 0001.c7d0.a301 (bia 0001.c7d0.a301)
100000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
ncapsulation ARPA, loopback not set
keepalive set (10 sec)
full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
RP type: ARPA, ARP Timeout 04:00:00
last input 00:00:08, output 00:00:05, output hang never
last clearing of "show interface" counters never
input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
queueing strategy: fifo
output queue: 0/40 (size/max)
minute input rate 0 bits/sec, 0 packets/sec
minute output rate 0 bits/sec, 0 packets/sec
956 packets input, 193351 bytes, 0 no buffer
Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
```

Err-disabled may be triggered due to reasons other than Port Security.



Port Security Requirements

Access Mode



Access ports are responsible for traffic flow.

Access mode should only be defined on ports connected to endpoint devices, such as PCs.

You can configure port security on interfaces that you configured as access ports with access mode.



Enable Port Security

Commands

```
switchport mode access  
switchport port-security
```



Enabling port security is done in the interface configuration mode, which is set using **interface [interface-id]**.

Then, Access mode needs to be set with **switchport mode access**.

For port security to operate correctly, the interface must be configured as an Access port.

Finally, Port Security can be enabled on the interface using the command **switchport port-security**

Example

```
Switch(config)# interface fastEthernet 0/1  
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport port-security  
Switch(config-if)#
```



Port Security Configuration

Command

```
switchport port-security [configuration] [value]
```



Port Security is configured by setting up each component individually using the same structure.

Violation defines the type of violation rule to be applied to the port.

The commands **mac-address** and **maximum** define sticky learning, up to a maximum of five addresses.

Example

```
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

```
*****
```

```
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security maximum 5
```



Port Security Show Commands

Presenting the authorized MAC addresses associated with a port and the type (sticky or manually) is done with the command **show port-security address**

If only an overview is needed, **show port-security** can be run for a quick overview of the configuration.

To view a specific interface, the command **show port-security interface [interface]** should be used, since it provides more information.

Example

```
Switch# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
          Fa0/1           5           1           0           Restrict
          Fa0/2           1           0           0           Shutdown
-----

Switch# show port-security address
                        Secure Mac Address Table
-----
Vlan  Mac Address          Type                Ports                Remaining Age
      -----
1     0002.1798.DAC6        SecureSticky        FastEthernet0/1      -
1     0090.2172.8736        DynamicConfigured   FastEthernet0/2      -
-----

Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```



Lab NET-04-L1

Configure and Verify Port Security

30–60 Min.



Mission

The objective of this exercise is to implement Port Security on a switch, practice using Port Security options, and learn how to verify settings.

Steps

- Configure & Verify Port Security

Environment & Tools

- All platforms
- Cisco Packet tracer 7.2.2 and higher

Related Files

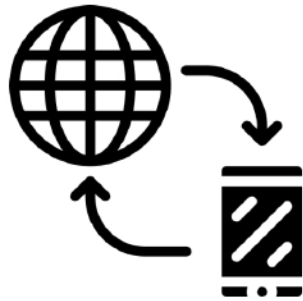
- Lab document
- NET-04-L1.pka

Switch Security

REMOTE ACCESS

Overview

Overview



Today, other than for initial configuration, most access to deployed switches is done remotely.

Remote access allows administrators to manage and monitor their network devices from anywhere in the network.

This is important, since some switches may be located in physically inaccessible areas.



Two common remote access protocols are used in switches today: SSH and Telnet.

Telnet Vs. SSH

Telnet and SSH are the two most widely used CLI-based remote access protocols.

Telnet



Telnet was developed many years ago to allow users to manage devices from anywhere, via a simple and minimal configuration. However, using Telnet involves a potential security risk because usernames and passwords are sent in plain text on TCP port 23.



SSH



SSH is similar to Telnet, but with a significant difference: SSH encrypts all data transferred between the user and end device. SSH uses RSA encryption, a robust and reliable encryption type. It operates on TCP port 22.



SSH Encryption

RSA Encryption



Modern encryption relies heavily on the RSA algorithm since most methods use public and private encryption keys.

The public and private encryption key method, also known as asymmetric cryptography, uses two different, but mathematically linked, keys.

The public key is shared with everyone, while the private key is only given to specific persons.

RSA ensures implementation of the CIA triangle, and avoids authentication rejection.



SSH Encryption

RSA Encryption



Protocols like SSH and SSL/TLS use RSA to encrypt communication and digital signatures.

Although RSA works through the computational difficulty of factoring large integers, computational complexity grows exponentially every day, and larger and larger numbers are required to maintain secure communication.

RSA is dependent on a powerful computational system. The more complicated the keys are, the more power is required.

Recently, ECC (Elliptic Curve Cryptography) is becoming more popular, since it can create faster, smaller, and more efficient cryptographic keys.

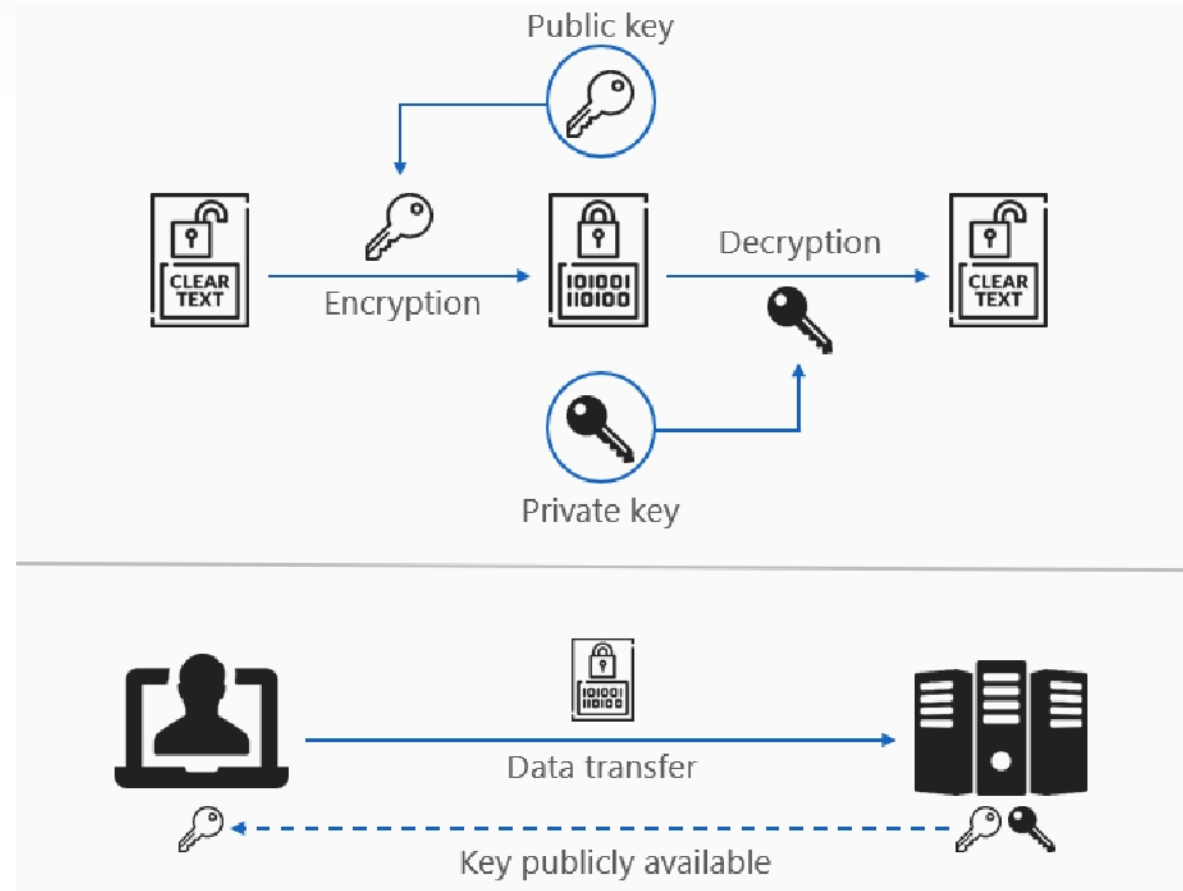


Asymmetric Encryption

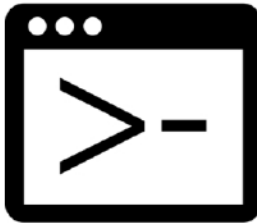
Asymmetric encryption is when two different keys are used to encrypt and decrypt messages. The keys are mathematically related in a way that messages encrypted with one key, typically the public key, cannot be decrypted by it.

The decryption can be done only using the corresponding private key in the key pair. This method is considered to be more complex and slower than symmetric encryption, which uses one key for both encryption and decryption.

Encryption/Decryption Process



Virtual Teletype



Virtual Teletype (VTY) is a command-line interface (CLI) in network devices used to create remote access connections. VTY is virtual and does not require any hardware.



Switches have 16 VTY lines (0-15), routers have 5 VTY lines (0-4).

Switched Virtual Interface



The primary purpose of creating a computer network is to share resources and enable communication within the network.

Layer 2 switches create VLANs (Virtual LANs) that form a single broadcast domain. If a broadcast message is sent within the same VLAN, all devices connected to that VLAN will receive the message.

Hosts can communicate on the same VLAN without a Layer 3 device (router). Devices on a different VLAN, on the other hand, cannot communicate with each other, without proper routing.



Switched Virtual Interface



A router or Layer 3 switch can handle network segmentation and inter-VLAN communication.

A router can segment a network and create separate broadcast domains, with each network segment using a different sub-interface of a physical interface on the router.

Layer 3 switches require the creation of multiple VLANs on the switch, which form multiple broadcast domains. Then, for each VLAN, a corresponding Layer 3 interface needs to be created on the switch, to handle the routing.

This Layer 3 interface is the SVI.

The difference is that the SVI Layer 3 interface is virtual.



SSH Configuration

Before establishing an SSH session, several items need to be configured.

01 Change the default hostname.

02 Create a user account.

03 Set the enable password.

04 Configure a domain name.

Set a security message.

Enable VTY lines and limit protocol access.

Enable Layer 3 connectivity.

Generate SSH keys.

05

06

07

08

SSH Prerequisites

Several initial settings must be configured before enabling SSH on the device.

1. Set the device name.
2. Create a local account.
3. Secure the privileged mode.
4. Set an appropriate security message (optional).
5. Set a domain name.

Initial Configuration

```
Switch(config)#hostname S1
S1(config)#username Admin password p@nd@
S1(config)#enable password c!sc0
S1(config)#service password-encryption
S1(config)#banner motd #Access to this device is for authorized
personnel only!#
S1(config)#ip domain-name CyberPro.com
```



Allow Remote Access

Command

```
line vty <id-range> & login local
```



Step 1 - Enter the VTY configuration mode. Select the number of maximum sessions.

Step 2 - Enable authentication using username and password.

Step 3 - Telnet is enabled by default; the transport command prevents using Telnet and only uses SSH for remote connections. The options are none, all, Telnet, or SSH.

Setting up the VTY Lines

```
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
```



IP Switch Settings

Commands

```
interface vlan 1  
ip address <ip-address> <subnet-mask>
```



Configuring IP on Interface VLAN 1 & Default Gateway

```
S1(config)#interface vlan 1  
S1(config-if)#ip address 10.0.0.150 255.255.255.0  
S1(config-if)#no shutdown  
S1(config-if)#exit  
...  
S1(config)#ip default-gateway 10.0.0.1
```



The default SVI is VLAN 1. Setting an address and enabling the interface is crucial if we want to communicate directly with the switch. If the switch needs to send data to other networks, the default gateway is also required.

Generate RSA Keys

Command

```
crypto key generate rsa
```



The crypto key command generates the Private and Public RSA keys on the network device. The switch or router needs those keys to secure the SSH session.

Set the key length. The default is 512, but it is recommended to set the number of bits to higher than 1024. The maximum value is 2048.

Generate the Private and Public Keys on the Device

```
S1(config)#crypto key generate rsa
The name for the keys will be: S1.CyberPro.com
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```



Verify SSH Configuration

The **show ssh** command presents the active SSH sessions on the network device.

Show ip ssh displays the version definition, authentication timeout, and retries.

Show ssh Command

```
S1#show ssh
Connection      Version Mode Encryption  Hmac      State
Username
2               1.99  IN   aes128-cbc   hmac-sha1 Session
Started Admin
2               1.99  OUT  aes128-cbc   hmac-sha1 Session
Started Admin
%No SSHv1 server connections running.
...

S1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```



SSH Connection

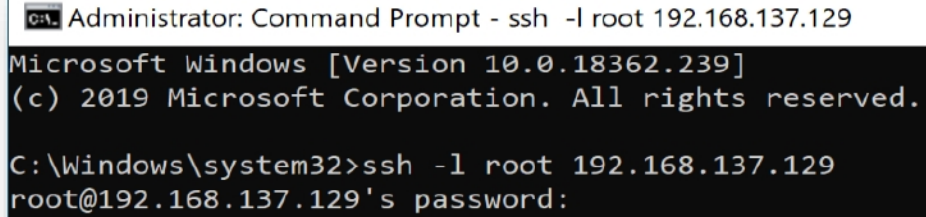
Accessing the device remotely using SSH can be done using a CLI, such as PuTTY or a device terminal.

The universal command for creating an SSH session is:

```
ssh -l <username> <target-ip>
```

In the example on the right, the command is executed in Windows CMD.

SSH in CMD

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt - ssh -l root 192.168.137.129". The window shows the Microsoft Windows version (10.0.18362.239) and copyright information (© 2019 Microsoft Corporation). The command prompt shows the command `C:\Windows\system32>ssh -l root 192.168.137.129` being entered, followed by the prompt `root@192.168.137.129's password:`. A mouse cursor is visible on the left side of the terminal area.

```
Administrator: Command Prompt - ssh -l root 192.168.137.129
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ssh -l root 192.168.137.129
root@192.168.137.129's password:
```



LAB NET-04-L2

Remote Access with SSH
30–60 Min.



Mission

The objective of this exercise is to set up the SSH service on network devices for remote management from anywhere on the network. In addition, this exercise practices configuring IP connectivity to a Layer 2 switch using the In-Band Management method.

Steps

- Configure SSH.
- Verify SSH configuration.

Environment & Tools

- All platforms
- Cisco Packet Tracer 7.2.2 or higher

Related Files

- Lab document
- NET-04-L2.pka

An overhead, top-down view of three people sitting around a rustic wooden table, likely in a collaborative workspace or meeting. The scene is bathed in a cool blue light. In the upper left, a person with long dark hair is partially visible, holding a blue pen over a laptop. In the center, a person with short blonde hair is looking at a laptop screen. In the lower right, a person with dark hair is typing on a laptop. The table is cluttered with various items: two laptops, a tablet, a smartphone, two disposable coffee cups, and several sheets of paper, including one with a colorful bar chart. A patterned rug is visible in the background. The word "QUESTIONS?" is superimposed in the center of the image.

QUESTIONS?



THANK YOU
