Ilian

- Commande_switch
  - Commande_switch_basique + Vlans
- commande_routeur
  - commande_routeur + Service DHCP
  - Filtrage (firewall)
- Serveur TFTP
  - Doc / config serveur TFTP
- Plan Réseau
  - Plan réseau/Infrastructure projet IRS
- Sécurisation Lan (Types D'attaques)
  - Sécurisation Lan
- Principe de sécurité Switch et routeur
  - Switch/Routeur
- Bonus
  - Problème / résolues
- Carte Arduino

Commande_switch

Commande_switch_basique + Vlans

1) sécurisation

Switch(config)# enable password <votre mot de passe> (stocké en clair dans la configuration : show running-config)
Switch(config)# enable secret <votre mot de passe> (hash visible dans la configuration : secret5)

// Mettre en place une authentification à la connexion

Switch(config)#line con 0
Switch(config-line)#password cisco
Switch(config-line)#login

Switch(config)#service password-encryption // Masquer les mots de passe de connexion dans la configuration
Switch(config)#banner motd # <message> #

2) commande de configuration plan réseau

switch(config)# hostname S3 // change le nom du switch
S3(config)# interface vlan 10 // ajout du vlan 10
Switch3(config-if)# ip address 192.168.10.0 255.255.255.192 // attribution de l'ip et du masque

3) Commande de visualisation / sauvegarde

show running-config // elle fournit la pluspart des informations sur le commutateur
do show run // examiner la configuration
do show vlan // consulter tout les vlans
do show ip interface brief
copy running-config startup-config //Elle sauvegarde la configuration actuelle pour qu’elle soit conservée même

après un redémarrage.

show interfaces status //affiche le statut des interfaces

show interface fastEthernet 0/X // affiche des informations sur l'interface spécifiée

show interfaces trunk // affiche les interfaces de type trunk et les VLAN transitant sur celles-ci

show spanning-tree (interface fa0/x // vlan x) // affiche les informations à propos du protocole spanning tree

show ip dhcp binding

4) exportation configuration en texte

//Exporter la configuration vers un fichier texte par tftp (running / startup config)

SW3#copy running-config tftp

Address or name of remote host []? 10.10.0.2

Destination filename [SW50-confg]?

Writing running-config....!!

[OK - 1120 bytes]

1120 bytes copied in 3.008 secs (372 bytes/sec)

//Importer la configuration depuis un fichier texte par tftp vers run ou startup config :

SW3#copy tftp running-config

Address or name of remote host []? 10.10.0.2

Source filename []? SW50-confg

Destination filename [running-config]? running-config

Accessing tftp://10.10.0.2/SW50-confg...

Loading SW50-confg from 10.10.0.2: !

[OK - 1120 bytes]

1120 bytes copied in 0.006 secs (186666 bytes/sec)

5) étapes configuration switch

1) Sécurisation accès au switch

hostname SW-XXX

no ip domain-lookup

enable secret <motdepasse>

service password-encryption

banner motd # Accès strictement réservé #

username admin secret <motdepasse>

2) Configuration vlan / lan

- Création de vlan
- paramétrages vlan
- gateway

3) Configuration des ports

- Switchport mode access
- Trunk
- Spanning-tree

4) sécurité avancée

- DHCP Snooping
- Protection STP

5) ACL

- Acl restriction ssh
- Acl bloquage

6) SYSLOG, NTP (raphael)

7) Vérification / Sauvegarde

6) script entier

```
switch(config)# hostname S1

cata-x(config)#line vty 0 15
cata-x(config-line)#password cataclysmique2
cata-x(config-line)#login
```

```
cata-x(config)#line console 0
cata-x(config-line)#password cataclysmique
cata-x(config-line)#login

cata-x(config)#enable secret cataclysmique3
cata-x(config)#service password-encryption

no ip domain-lookup
banner motd # Accès strictement réservé #

S1(config)# interface vlan 10
Switch3(config-if)# ip address 192.168.10.1 255.255.255.192
Switch3(config-if)# no shutdown

Switch3(config-if)#interface range FastEthernet0/1 - 5
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 10
Switch3(config-if)#spanning-tree portfast
Switch3(config-if)#spanning-tree bpduguard enable
```

7) configurer le port trunk:

```
// exemple

interface fastEthernet0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50,60
end
```

8) Nommage des vlans:

```
vlan 10
name Fabrication_Maintenance
exit

vlan 20
name Gestion_Admin_Direction_Stock
```

```
exit

vlan 30
name Commercial_Etudes
exit

vlan 40
name Visiteurs
exit

vlan 50
name cameras
exit

vlan 60
name arduino
exit
```

9) port Trunk :

```
// pour le switch principal

interface gigabitEthernet0/1
description TRUNK_TO_ROUTER
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50,60
switchport nonegotiate

interface g0/2
switchport mode trunk
switchport trunk allowed vlan 10,20,30,40,50,60
```

commande_routeur

commande_routeur + Service DHCP

1. configurer le routeur (routeur on a stick) :

```
VLAN 10 – 192.168.10.0/26

interface gigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.192

interface gigabitEthernet0/0
no shutdown
```

2. configurer le service DHCP :

```
// pour le vlan 10

ip dhcp pool VLAN10
network 192.168.10.0 255.255.255.192
default-router 192.168.10.1
dns-server 1.1.1.1

// pour le vlan 20

ip dhcp pool VLAN20
network 192.168.10.64 255.255.255.192
default-router 192.168.10.65
dns-server 1.1.1.1
```

```
write memory
```

Bloquer des adresses ip!!!

```
// pour vlan 10

ip dhcp excluded-address 192.168.10.1 192.168.10.20

// pour vlan 20

ip dhcp excluded-address 192.168.10.65 192.168.10.80
```

Filtrage (firewall)

Serveur TFTP

Doc / config serveur TFTP

1. Qu'est-ce que TFTP ?

TFTP (Trivial File Transfer Protocol) est un protocole de transfert de fichiers simplifié. Contrairement à FTP, il ne dispose d'aucune authentification ni chiffrement, ce qui le rend très léger et rapide. Il fonctionne sur le port UDP 69.

Caractéristique	Détail
Protocole	UDP port 69
Authentification	Aucune
Chiffrement	Aucun
Taille max fichier	~32 MB (selon implémentation)
Usage recommandé	Réseau de gestion isolé uniquement
Alternative sécurisée	SCP (ip scp server enable sur Cisco)

2. Qu'est-ce que tftpd-hpa ?

tftpd-hpa est l'implémentation la plus répandue et fiable d'un serveur TFTP sous Linux.

Installation:

```
apt update
apt install tftpd-hpa
```

Fichier de configuration : /etc/default/tftpd-hpa:

```
TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="0.0.0.0:69"       # Ecoute sur toutes les interfaces
TFTP_OPTIONS="--secure --create"
```

Préparer le dossier de stockage:

```
mkdir -p /srv/tftp
chown tftp:tftp /srv/tftp
chmod 777 /srv/tftp
```

Démarrer et activer le service:

```
systemctl restart tftpd-hpa
systemctl enable tftpd-hpa
systemctl status tftpd-hpa
```

3. Sauvegarde de la configuration courante (Switch/Routeur):

Sauvegarde de la configuration courante:

```
copy running-config tftp
! Address or name of remote host? 192.168.99.6
! Destination filename? "filename"
```

Sauvegarde de la configuration de démarrage:

```
copy startup-config tftp
! Address or name of remote host? 192.168.99.6
! Destination filename? "filename"
```

Restauration d'une configuration depuis tftp:

```
copy tftp running-config
! Address or name of remote host? 192.168.99.10
! Source filename? isr4321-running-config
```

4. Vérification / Supervision :

Vérifier les fichiers reçus sur le serveur TFTP (VM) :

```
ls -lh /srv/tftp/
```

Surveiller les transferts en temps réel (côté Cisco) :

```
debug ip tftp
! Pour désactiver :
no debug ip tftp
! Ou tout désactiver :
undebug all
```

Tester la connectivité TFTP depuis la vm:

```
tftp 192.168.99.6
> get isr4321-running-config
> quit
```

5. Résumer commandes clés:

Action	Commande / Emplacement
Installer tftpd-hpa	apt install tftpd-hpa
Fichier de config TFTP	/etc/default/tftpd-hpa
Dossier des backups	/srv/tftp/
Redémarrer le service	systemctl restart tftpd-hpa
Voir les fichiers reçus	ls -lh /srv/tftp/

Sauvegarder config routeur	copy running-config tftp
Sauvegarder config switch	copy running-config tftp
Vérifier port UDP 69	ss -ulnp | grep 69
Debug TFTP (Cisco)	debug ip tftp

Plan Réseau

Plan réseau/Infrastructure projet IRS

1. Présentation de l'infrastructure

1.1 Architecture générale :

L'infrastructure du Bâtiment B est composée des éléments suivants :

- Un routeur Cisco ISR4321 (Router_batB) assurant le routage inter-VLAN via des sous-interfaces 802.1Q
- Un switch Cisco Catalyst (Switch_b) assurant la commutation L2 avec segmentation VLAN
- Un serveur Proxmox connecté au switch via un lien trunk sur le port Fa0/23
- Des machines virtuelles hébergées sur Proxmox, accessibles sur le VLAN 999
- Un serveur TFTP (VM Debian) pour la sauvegarde des configurations réseau
- D'un téléphone Ip attribuer sur le VLAN 20

L'infrastructure du Bâtiment A est composée des éléments suivants :

- Un switch Cisco Catalyst (Switch_b) assurant la commutation L2 avec segmentation VLAN
- D'un téléphone Ip attribuer sur le VLAN 20
- A voir pour la suite...

1.2 Équipements Réseau :

Équipement	Modèle	IP de gestion	Rôle
Router_batB	Cisco ISR4321	192.168.99.1	Routage inter-VLAN, DHCP, NAT
Switch_b	Cisco Catalyst	192.168.99.14	Commutation L2, trunk 802.1Q
Serveur Proxmox	Serveur physique	192.168.99.2	Hyperviseur, hébergement VMs
VM TFTP	Debian Linux	192.168.99.6	Sauvegarde configs réseau

2. Segmentation VLAN

Le réseau est segmenté en 7 VLANs distincts permettant d'isoler les différents types de trafic et d'améliorer la sécurité ainsi que les performances.

2.1 Tableau Des Vlans :

VLAN	Nom	Réseau	Passerelle	Plage DHCP
10	Fab+Maintenance	192.168.10.0/26	192.168.10.1	.2 ? .62
20	Admin+Gestion +Direction	192.168.10.64/26	192.168.10.65	.66 ? .126
30	Com+Etudes	192.168.10.128/26	192.168.10.129	.130 ? .190
40	Wifi_Visiteurs	192.168.10.192/27	192.168.10.193	.194 ? .222
50	Nas / Caméras	192.168.10.224/27	192.168.10.225	.226 ? .254
60	Carte Arduino	172.24.255.248/29	172.24.255.254	.249 ? .253
999	Proxmox	192.168.99.0/28	192.168.99.1	.2 ? .14

2.2 Rôle Des Vlans :

Vlan 10 - Fabrication / Maintenance:
Le VLAN 10 est réservé à la fabrication ainsi que la maintenance il utilise le réseau 192.168.10.0 /27 .

VLAN 20 - téléphonie:
Le VLAN 20 est réservé à la gestion, administration, direction, stock, ainsi que pour la téléphonie ip Il utilise le réseau 192.168.10.64 /26 .

VLAN 30 - Commerce/études:
Le VLAN 20 est réservé pour le commerce et le service études, Il utilise le réseau 192.168.10.128 /26 .

VLAN 40 - Wifi/visiteurs:
Le VLAN 40 est réservé pour les visiteurs ainsi que pour la borne wifi Il utilise le réseau 192.168.10.192 /27 .

Vlan 50 - Caméras:
Le VLAN 50 est réservé pour les caméras ainsi que pour le NAS Il utilise le réseau 192.168.10.224 /27 .

VLAN 60 - Carte Arduino:
Le VLAN 60 est réservé aux Cartes Arduino. Il utilise le réseau 172.24.0.0/29 permettant d'accueillir un grand nombre d'équipements.

VLAN 999 - Management et VMs
Le VLAN 999 est le VLAN de management. Il est utilisé comme VLAN natif sur les liens trunk, et héberge le serveur Proxmox ainsi que toutes les machines virtuelles. Les VMs reçoivent une adresse IP automatiquement via le pool DHCP du routeur sur ce VLAN il utilise le réseau 192.168.99.0 /28 .

3. Configuration du routeur

3.1 Router-on-a-stick :

Le routeur utilise la technique router-on-a-stick : une seule interface physique (GigabitEthernet0/0/0) est connectée au switch en mode trunk. Des sous-interfaces logiques sont créées pour chaque VLAN avec encapsulation 802.1Q. En l'occurence on a des sous interfaces pour chaque vlan.

Exemple de configuration :

```
interface GigabitEthernet0/0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.192
interface GigabitEthernet0/0/0.999
 encapsulation dot1Q 999 native
 ip address 192.168.99.1 255.255.255.240
```

3.2 Service DHCP :

Le routeur héberge un pool DHCP pour chaque VLAN. Les adresses des équipements fixes (routeur, switch, Proxmox) sont exclues des plages DHCP afin d'éviter tout conflit d'adresse IP.

4. Configuration du switch

4.1 Ports trunk :

Les liens trunk permettent de transporter plusieurs VLANs simultanément entre les équipements. Le VLAN 999 est configuré comme VLAN natif sur tous les trunks, ce qui signifie que son trafic transite sans tag 802.1Q.

4.2 Tableau de Ports:

Port	Description	Mode	VLANs
Gi0/1	routeur_to_switch	Trunk	10,20,30,40,50,60,999 (native 999)
Fa0/23	proxmox_to_switch	Trunk	10,20,30,40,50,60,999 (native 999)
Fa0/1-5	Postes VLAN 10	Access	VLAN 10
Fa0/6-11	Postes VLAN 20	Access	VLAN 20
Fa0/12-15	Postes VLAN 30	Access	VLAN 30
Fa0/16-17	Postes VLAN 50	Access	VLAN 40
Fa0/18-20	NAS/Serveurs	Access	VLAN 50
Fa0/21-22	Cartes Arduino	Access	VLAN 60
Fa0/24-48	Vlan 2 Blackhole	Shutdown	VLAN 2

4.3 Sécurité des Ports :

Les ports d'accès sont sécurisés avec les mécanismes suivants :

- Port-security : maximum 2 adresses MAC par port
- Port-security violation restrict : restriction en cas de violation
- DHCP snooping : filtrage des réponses DHCP non autorisées
- ARP inspection : protection contre les attaques ARP spoofing
- Spanning-tree portfast : activation rapide des ports d'accès

5. Infrastructure Proxmox

5.1 Configuration Réseau :

Le serveur Proxmox est connecté au switch via le port Fa0/23 en mode trunk avec le VLAN 999 comme VLAN natif. Cela permet aux VMs de recevoir des adresses IP via le DHCP du routeur sans configuration de tag VLAN.

Configuration /etc/network/interfaces :

```
auto eno2
iface eno2 inet manual
auto vmbr1
iface vmbr1 inet static
        address 192.168.99.2/28
        gateway 192.168.99.1
        bridge-ports eno2
        bridge-vlan-aware yes
        bridge-vids 2-4094
```

5.2 Configuration Des Vms :

Pour qu'une VM reçoive une adresse IP via DHCP sur le VLAN 999, la configuration dans l'interface Proxmox est la suivante :

- Network Bridge : vmbr1
- VLAN Tag : vide (pas de tag = VLAN natif 999)
- La VM démarrera et recevra automatiquement une IP dans la plage 192.168.99.3 - 192.168.99.13
- La VM pourra communiquer avec tous les VLANs via le routeur

6. Points importants et rappels

7.1 Commandes de vérification utiles :

- show ip dhcp binding - voir les baux DHCP attribués
- show interface trunk - vérifier les VLANs sur les trunks
- show ip arp - vérifier la table ARP du routeur
- show vlan brief - vérifier l'état des VLANs sur le switch
- show ip dhcp conflict - vérifier les conflits d'adresses IP

Sécurisation Lan (Types D'attaques)

Sécurisation Lan

Résumer protection switch :

Stratégies de sécurité pour le switch:

// Port security

switchport port-security maximum 1 — switchport port-security violation shutdown — shutdown + switchport access vlan 999

//désactiver les ports inutiles

//vlan de management

//bannière et timeout

//désactiver CDP/LLDP sur les interface non trunk ou exposées

// DHCP Snooping

// désactiver dtp

//changer le vlan natif

interface vlan 99

//mots de passe chiffrés

//ssh

//dynamic arp inspection

//ip source guard

//802.1x

Résumer protection Routeur :

sécurité pour le routeur:

// Accès & authentification

//Désactivation des services inutiles
no service tcp-small-servers — no cdp enable — no ip http server — no ip proxy-arp — no ip directed-broadcast

//Sécurité des protocoles de routage
ip ospf authentication message-digest — ip authentication mode eigrp 1 md5 — passive-interface default — neighbor x.x.x.x password <clé>

//Hardening avancé

Lignes Routeur:

// Accès & authentification

! Mot de passe enable chiffré
enable secret <mdp>
service password-encryption
username admin privilege 15 secret <mdp>

! Génération clé RSA + SSH v2
crypto key generate rsa modulus 2048
ip ssh version 2

! Sécurisation lignes VTY (sécurisation connexion ssh)
line vty 0 4
 transport input ssh

```
 exec-timeout 5 0
 login local
 access-class ACL_ADMIN in

! Sécurisation console
line console 0
 exec-timeout 5 0
 login local

! Bannière légale
banner motd ^Acces autorise uniquement^

// Désactivation des services inutiles

no service tcp-small-servers
no service udp-small-servers
no service finger       (Désactive le protocole Finger (port 79), qui permettait de lister les utilisateurs connectés sur le routeur)

! Services IP dangereux
no ip bootp server     (Désactive le serveur BOOTP. Évite que le routeur réponde à des requêtes d'amorçage réseau non sollicitées)
no ip http server      (Désactive l'interface web d'administration en HTTP (non chiffré))
no ip http secure-server    (https)
no ip proxy-arp      (Empêche le routeur de répondre aux requêtes ARP à la place d'autres machines. Réduit les risques de ARP spoofing)
no ip directed-broadcast     (Bloque les broadcasts dirigés vers un sous-réseau)
no ip source-route     (Désactive la possibilité pour un paquet IP de dicter son propre chemin dans le réseau)

! Désactiver CDP globalement
no cdp run    (cache certaines configuration)

// acl

! Bloquer adresses RFC 1918 et bogons en entrée WAN
ip access-list extended ACL_ANTI_SPOOF
 deny ip 10.0.0.0 0.255.255.255      any
 deny ip 172.16.0.0 0.15.255.255   any
 deny ip 192.168.0.0 0.0.255.255   any
 deny ip 127.0.0.0 0.255.255.255   any
```

```
 permit ip any any

! Application sur interface WAN + uRPF
interface GigabitEthernet0/0
 ip access-group ACL_ANTI_SPOOF in
 ip verify unicast source reachable-via rx

 // Sécurité des protocoles de routage

! Authentification OSPF MD5
router ospf 1
 area 0 authentication message-digest

interface GigabitEthernet0/1
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 <clé>

! Interfaces passives par défaut
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet0/1

! Authentification EIGRP MD5
router eigrp 1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 <keychain>
```

Lignes switch:

```
// Sécurité des VLANs

! Déclaration des VLANs
vlan 10
 name USERS
vlan 20
 name FINANCE
vlan 99
```

```
 name MANAGEMENT
vlan 999
 name BLACKHOLE

! Interface de management
interface vlan 99
 ip address 192.168.99.1 255.255.255.0
 no shutdown

! Sécurisation des trunks
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,99

// Sécurité des ports access

! Ports utilisateurs (Fa0/1 - 20)
interface range FastEthernet 0/1 - 20
 switchport mode access
 switchport access vlan 10
 switchport nonegotiate
 switchport port-security maximum 1        (Limite à une seule adresse MAC autorisée sur ce port. Si un deuxième équipement est branché)
 switchport port-security violation shutdown     (Définit l'action en cas de violation : le port passe en mode err-disabled (shutdown automatique). Il faudra alors faire un shutdown puis no shutdown)

 switchport port-security     (Active la sécurité de port sur l'interface. Sans cette ligne, les deux précédentes n'ont aucun effet)
 spanning-tree portfast
 spanning-tree bpduguard enable
 no cdp enable
 no shutdown

! Ports inutilisés → VLAN blackhole + shutdown
interface range FastEthernet 0/21 - 24
 switchport mode access
 switchport access vlan 999
 shutdown

//Protection L2 (DHCP / ARP / IP)
```

```
! DHCP Snooping
//plus pour les ports
ip dhcp snooping ou ip dhcp snooping trust
ip dhcp snooping limit rate 6
//plus pour les vlans
ip dhcp snooping vlan 10,20
no ip dhcp snooping information option

interface GigabitEthernet 0/1
 ip dhcp snooping trust

! Dynamic ARP Inspection (DAI)
ip arp inspection vlan 10,20

interface GigabitEthernet 0/1
 ip arp inspection trust

! IP Source Guard sur ports access
interface range FastEthernet 0/1 - 20
 ip verify source (port untrusted tel que pc ou visiteur etc..)
 //ou pour filtrage ip + mac (ip verify soyrce port-security)

// spanning-tree

! PortFast + BPDU Guard globaux
spanning-tree portfast default    (Active PortFast sur tous les ports d'accès du switch globalement.)
spanning-tree portfast bpduguard default
```

Principe de sécurité Switch et routeur

Principe de sécurité Switch et routeur

Switch/Routeur

1) Switch

1.1. **Sécurisation des accès**

Désactiver les ports inutilisés

Mettre en place des VLANs d’administration séparés.

Utiliser SSH au lieu de telnet

Imposer des mots de passe forts + bannière légale.

Désactiver les ports inutilisés

Mettre en place des VLANs d’administration séparés.

Utiliser SSH au lieu de telnet

Imposer des mots de passe forts + bannière légale.

1.2. **Sécurité des ports**

Port Security :

Limiter le nombre d’adresses MAC autorisées par port.

Bloquer le port en cas de violation.

1.3. **Sécurité des VLAN et du plan de contrôle**

Séparer les VLAN

Interdire VLAN 1 pour la production.

Sécuriser le protocole STP

DHCP snooping

1.4.**Filtrage et surveillance**

Journalisation et envoi des logs vers un serveur.

2) Routeur

1. **Sécurisation des accès administratifs**

Utiliser SSH, pas Telnet.

Se connecter via un ACL d’administration (limiter par IP).

2. **ACL et filtrage avancé**

ACL pour :

filtrer le trafic entrant/sortant,

limiter le management au routeur,

bloquer les IP spoofing (anti-usurpation).

3. **Sécurité du routage**

Authentifier les protocoles de routage (MD5, SHA selon protocole) :

OSPF,

EIGRP,

BGP.

4. **VPN et chiffrement**

Mettre en place :

IPsec pour les liaisons intersites,

SSL VPN pour utilisateurs.

Bonus

Problème / résolues

Problèmes résolus :

• Conflit d'adresses IP VLANs 20 et 50 : supprimer les IPs des interfaces VLAN du switch car le routeur assure déjà le routage inter-VLAN

• DHCP non fonctionnel VLAN 999 : le switch avait sa propre IP sur Vlan999 - supprimée

• VLAN 999 natif : le mot-clé 'native' sur l'encapsulation dot1Q du routeur est indispensable car le switch envoie le trafic VLAN 999 sans tag

• TFTP timeout : utiliser 'ip tftp source-interface' pour forcer la bonne interface source

Carte Arduino

Explication du code IRS-SI

---

1. Les bibliothèques

```
#include <SPI.h>
#include <Ethernet.h>
#include <Wire.h>
#include <rgb_lcd.h>
#include <AM2302-Sensor.h>
```

On charge les outils nécessaires : SPI et Ethernet pour la connexion réseau, Wire pour le bus I2C, rgb_lcd pour l'écran, AM2302 pour le capteur température/humidité.

---

2. La configuration

```
#define PIN_DHT        A0
#define PIN_BOUTON     2
#define PIN_LUMINOSITE A3
```

On déclare les broches utilisées. Si tu changes un câble de place, tu modifies juste ici sans toucher au reste du code.

---

3. Les objets

```
rgb_lcd lcd;
EthernetServer serveur(PORT_HTTP);
AM2302::AM2302_Sensor capteurDHT(PIN_DHT);
```

On crée les 3 composants principaux : l'écran, le serveur web sur le port 80, et le capteur DHT.

---

4. Le setup — initialisation

```
lcd.begin(16, 2);
lcd.setRGB(0, 0, 255);
lcd.print("Initialisation");
```

L'écran démarre en bleu et affiche "Initialisation".

```
if (Ethernet.begin(mac)) {
    lcd.setRGB(0, 255, 0);
    lcd.print(Ethernet.localIP());
    serveur.begin();
} else {
    lcd.setRGB(255, 0, 0);
    lcd.print("ERREUR reseau");
    while (true) { }
}
```

On demande une adresse IP au routeur (DHCP). Si ça marche → écran vert + affichage de l'IP. Si ça échoue → écran rouge + blocage total.

---

5. La boucle principale

```
if (digitalRead(PIN_BOUTON) == LOW) {
    lireCapteurs();
    afficherSurLCD();
}
```

En permanence : si le bouton est pressé, on lit les capteurs et on affiche sur l'écran.

```
EthernetClient client = serveur.available();
if (client) {
    traiterRequeteHTTP(client);
}
```

En permanence aussi : si quelqu'un se connecte via un navigateur, on lui répond.

---

6. La lecture des capteurs

```
void lireCapteurs() {
    capteurDHT.read();
    temperature = capteurDHT.get_Temperature();
    humidite    = capteurDHT.get_Humidity();
    luminosite  = analogRead(PIN_LUMINOSITE);
}
```

On interroge le capteur DHT pour la temp/humidité, et on lit la valeur analogique du capteur de luminosité (0 = sombre, 1023 = pleine lumière).

---

7. La page web

```
client.println("HTTP/1.1 200 OK");
...
client.print("<p>Temperature : <b>"); client.print(temperature, 1);
client.print("<p>Humidite    : <b>"); client.print(humidite, 0);
client.print("<p>Luminosite  : <b>"); client.print(luminosite);
```

On envoie une page HTML simple au navigateur avec les 3 valeurs des capteurs en temps réel.