

# Projecte Xarxa Corporativa Segura

---

Complex Esportiu Municipal

---

Alumnes: Hamza El Haddad Sabri

Data: 28/05/2025-05/06/2025

---

# ÍNDEX

Introducció i Objectius del Projecte	3
Anàlisi dels Requisits del Cas d'Estudi Escollit	3
Descripció de l'organització	4
Necessitats de comunicació i segmentació	4
Requisits de seguretat i accessibilitat	4
Serveis essencials a suportar	5
Disseny de la Xarxa	6
Topologia Proposada	6
Adreçament IP i Segmentació	7
Taula d'adreçament IP i assignació de ports :	8
Configuració Bàsica de la Xarxa	9
Mesures de Seguretat Bàsiques Implementades	14
Validació de la Xarxa i Resultats de les Proves	15
Conclusions i Millores Futures	19

# Introducció i Objectius del Projecte

El present projecte té com a objectiu dissenyar, simular i documentar una xarxa corporativa segura adaptada a les necessitats d'un **Complex Esportiu Municipal** fictici. Es tracta de demostrar competències en planificació d'adreçament IP, segmentació mitjançant VLANs, configuració bàsica de dispositius de xarxa (routers i commutadors) i aplicació de mesures fonamentals de seguretat.

**Objectius generals:** Crear una infraestructura de xarxa senzilla però funcional que **separi el trànsit per departaments** (Administració, Vigilància i Públic) i garanteixi la **connectivitat adequada** per als serveis necessaris, tot **minimitzant els riscos de seguretat**.

**Objectius específics:**

- **Segmentació per VLANs:** Dividir la xarxa en almenys tres VLANs (Administració, Vigilància, Públic) per aïllar els recursos de cada àrea i reduir dominis de difusió.
- **Encaminament inter-VLAN segur:** Implementar *routing* entre subxarxes de manera que dispositius de diferents VLAN puguin comunicar-se **només quan sigui permès** (per exemple, els administradors poden accedir a càmeres de vigilància, però els usuaris públics no poden accedir a recursos interns).
- **Adreçament IP planificat:** Assignar esquemes d'adreces IP adequats a cada VLAN, tenint en compte un possible creixement de dispositius i facilitant la identificació de cada xarxa.
- **Mesures bàsiques de seguretat:** Configurar **ACLs** (l·listes de control d'accés) per restringir el trànsit entre VLANs segons polítiques definides, establir **contrasenyes segures** als dispositius de xarxa, i **desactivar ports** no utilitzats per prevenir accessos no autoritzats.
- **Validació i proves:** Verificar el funcionament de la xarxa simulada amb **Packet Tracer**, comprovant que les VLANs estan correctament configurades, que l'encaminament funciona i que les restriccions de seguretat s'apliquen (mitjançant comandes *ping* i *traceroute* entre dispositius).

Amb aquests objectius, es pretén obtenir una xarxa senzilla però robusta, capaç de donar servei a un complex esportiu municipal, assegurant la separació del trànsit per usos i la protecció dels recursos interns davant accessos indeguts.

## Anàlisi dels Requisits del Cas d'Estudi Escollit

**Cas d'estudi seleccionat:** *Cas 9 – Complex Esportiu Municipal*. S'ha triat aquest escenari ja que presenta una situació realista on conviuen diferents tipus d'usuaris i dispositius (administració, sistemes de vigilància i públic en general), exigint una clara segmentació de la xarxa i mesures de seguretat per protegir dades i serveis. A continuació, s'analitzen els requisits concrets:

## Descripció de l'organització

Ens trobem davant unes instal·lacions esportives municipals que inclouen un estadi principal, pavellons esportius annexos, piscines i diverses zones de servei al públic. L'organització gestiona tant les operacions internes (administració, control d'accés, etc.) com serveis orientats als usuaris o espectadors (connexió Wi-Fi, pantalles informatives, etc.).

## Necessitats de comunicació i segmentació

Donada la diversitat de serveis, es requereix **separar les comunicacions en diferents xarxes lògiques**. En concret, es contemplen tres segments principals: **xarxa de gestió interna, xarxa de seguretat i xarxa de serveis digitals al públic**. Cada segment ha de funcionar com una LAN independent en termes de broadcast i trànsit intern. Aquesta segmentació s'implementa amb VLANs, de manera que els dispositius de cada àmbit es comuniquin com si estiguessin en xarxes físiques separades. Per exemple, els ordinadors de l'administració han d'estar en una VLAN separada de la dels sistemes de vigilància (càmeres IP) i dels dispositius dels usuaris. D'aquesta forma s'aconsegueix aïllar el trànsit de cada departament i **evitar que dispositius de zones diferents es comuniquin directament sense autorització**.

A nivell de maquinari, el complex necessitarà connectivitat cablejada per a les oficines administratives i els equips de seguretat (servidors de vídeo vigilància, controls d'accés), així com accessos Wi-Fi per al públic. Es preveu la instal·lació de commutadors (switches) en les àrees principals (edifici d'administració i instal·lacions esportives) i la interconnexió dels mateixos amb un encaminador central.

## Requisits de seguretat i accessibilitat

La xarxa ha de garantir que cada segment estigui **adequadament protegit contra accessos indeguts**. En particular:

- **Aïllament de la xarxa interna:** La VLAN d'Administració ha de quedar restringida només al personal autoritzat. Els usuaris de la xarxa pública no han de poder accedir a dades internes (per exemple, bases de dades de socis o sistemes de gestió).
- **Protecció de la xarxa de vigilància:** Les càmeres IP i sistemes de control d'accés (tornells, alarmes) residiran en la VLAN de Vigilància. Per seguretat, aquesta VLAN ha d'estar aïllada de la pública; només personal d'administració o tècnics autoritzats haurien de poder accedir a aquests dispositius. Cal implementar controls d'accés per

garantir-ho (per exemple ACLs al router).

- **Xarxes independents per IoT:** Atès que hi pot haver dispositius IoT (com sensors ambientals, marcadors electrònics, etc.), es recomana tenir-los en segments separats o dins de la VLAN de Vigilància, on es puguin controlar els accessos. En qualsevol cas, aquests dispositius no han de poder comunicar-se amb els equips de confiança sense passar per un encaminador amb filtres de seguretat. Això minimitza els riscos que un dispositiu IoT comprometès afecti la resta de la xarxa.
- **Accessibilitat controlada:** Si es permet accés remot a la xarxa (per exemple, administració remota dels sistemes o monitoratge de les càmeres des de fora del recinte), s'haurà de fer mitjançant canals segurs (VPN, connexions xifrades) i polítiques d'autenticació robustes. *(Nota: L'accés remot no es desplega en la simulació bàsica, però es té present com a requeriment futur.)*

## Serveis essencials a suportar

La infraestructura ha de suportar diversos serveis clau:

- **Publicitat digital i informació a usuaris:** Pantalles i sistemes d'informació dins del recinte que probablement es connecten a servidors interns o a Internet per mostrar contingut (aquests dispositius es connectarien a la VLAN Pública o IoT segons el cas).
- **Connexió Wi-Fi per a usuaris/espectadors:** Una xarxa sense fils pública perquè els visitants es puguin connectar durant els esdeveniments. Aquesta ha d'estar totalment **aïllada de les xarxes internes** i possiblement amb un ample de banda controlat. En la nostra implementació, la VLAN *Públic* simularà aquest entorn Wi-Fi d'usuaris.
- **Aplicacions de reserves i ticketing:** Sistemes que permeten reservar instal·lacions o comprar entrades en línia. Probablement aquests serveis resideixin a l'àrea d'Administració (servidors interns que connecten amb l'exterior). La xarxa ha de permetre que els usuaris públics hi accedeixin només a través de la infraestructura adequada (per exemple, el servidor de tickets podria estar en una zona desmilitaritzada o DMZ, fora de l'abast directe de la VLAN pública; però això excedeix l'abast del nostre disseny bàsic).

En resum, els requisits del **Complex Esportiu Municipal** exigeixen una segmentació de xarxa estricta per **separar administració, seguretat i públic**, alhora que es manté la **connectivitat necessària** perquè els serveis funcionin (per exemple, els administradors han de poder veure les càmeres, i els usuaris han de poder accedir a internet o a portals públics). Tot això s'ha d'aconseguir assegurant **polítiques de seguretat** adequades en el router i els commutadors.

# Disseny de la Xarxa

## Topologia Proposada

Per complir els requeriments, es proposa una topologia amb un **encaminador central (router)** i dos **commutadors (switches)** principals, seguint l'estructura típica d'una xarxa LAN empresarial petita. La configuració essencial és un **model *router-on-a-stick***: un únic encaminador connectat a la xarxa de commutadors mitjançant un enllaç troncal (*trunk*) 802.1Q que transporta el trànsit de totes les VLAN. Els switches gestionen localment les VLANs i es connecten entre sí i amb el router via ports troncal.

Cada **VLAN** correspon a un segment:

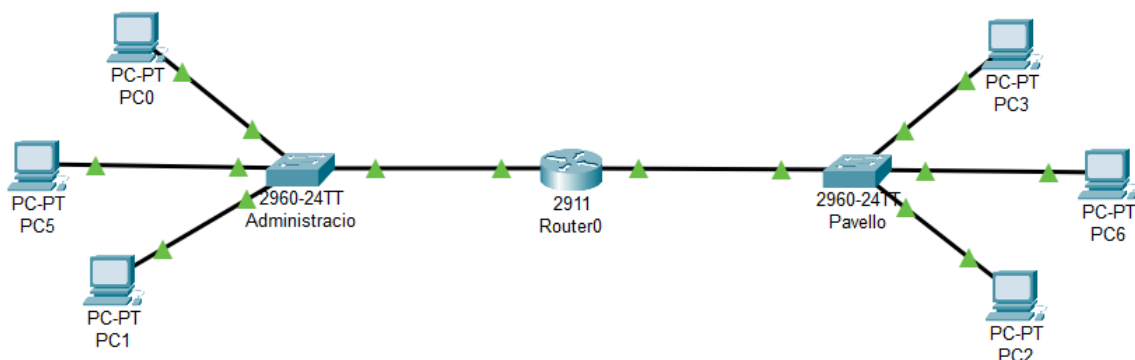
- **VLAN Administració:** per a ordinadors de gestió i altres recursos interns del personal.
- **VLAN Vigilància:** per a dispositius de seguretat (càmeres IP, controls d'accés, etc.).
- **VLAN Públic:** per a punts d'accés Wi-Fi, dispositius mòbils dels espectadors i altres serveis orientats al públic.

S'han utilitzat **2 commutadors (S1 i S2)** per representar dues zones físiques del complex (per exemple, S1 al edifici d'administració i S2 a l'estadi/pavellons). Ambdós switches estan interconnectats amb un enllaç troncal, de manera que les VLAN estan **presentes a ambdós costats**. Això permet, per exemple, tenir tant a S1 com a S2 ports assignats a la VLAN Pública (punts d'accés Wi-Fi repartits) o a la VLAN de Vigilància (càmeres tant a l'edifici com a l'estadi).

Els dispositius mínims connectats per fer proves i simulacions són: **un PC d'Administració** (connectat a un port d'accés de S1 en VLAN Administració), **una càmera IP de vigilància** (simulada per un PC o IoT device a S2 en VLAN Vigilància), i **un host públic (PC/portàtil)** connectat a la VLAN Pública (per exemple, a S2, representant un usuari a l'estadi). Addicionalment, es podria incloure un altre host a la VLAN Pública a S1 per simular un usuari a les oficines (o un punt Wi-Fi al vestíbul), però no és estrictament necessari.

En aquesta topologia, el router actua com a **porta d'enllaç per defecte** de totes les VLANs: es configuren subinterfícies (encapsulació dot1q) per a cadascuna, amb una IP corresponent a cada subxarxa. Així, el router pot *rotejar* el trànsit entre VLANs diferents. Els switches es configuren amb els ports d'accés assignats a la VLAN correcta i amb un **port troncal** en cada switch (el port cap al router, i el port d'enllaç entre S1 i S2). D'aquesta manera, es garanteix que el trànsit etiquetat de cada VLAN pot arribar fins al router i viceversa.

La figura següent mostra esquemàticament la topologia descrita:



En la **Figura 1** s'observa com R1 (encaminador) està connectat a S1 amb una interfície física (p. ex., G0/0/1) configurada com a trunk 802.1Q que transporta diverses VLAN. S1 i S2 estan connectats igualment per un enllaç troncal (p. ex., entre ports F0/1). Cada VLAN té associada una subinterfície al router (p. ex. G0/0/1.10 per VLAN Administració, G0/0/1.20 per Vigilància, etc.) i una adreça IP de gateway. Els hosts dins d'una mateixa VLAN només es comuniquen entre ells a nivell de switch, mentre que per comunicar-se amb altres VLAN necessiten passar per R1 (que aplica les polítiques de routing i seguretat).

Aquesta topologia és **viable a implementar en Packet Tracer en menys de 6 hores**, ja que inclou pocs dispositius i configuracions relativament senzilles. A més, reflecteix una situació real on una organització petita utilitza un sol router per interconnectar diverses xarxes locals virtuals. La senzillesa del disseny facilita també fer proves i detectar problemes de configuració amb rapidesa.

## Adreçament IP i Segmentació

Per a cada VLAN s'ha planificat una **subxarxa IP separada**. S'ha optat per adreces privades RFC1918 de rang *classe C* (mask /24) per simplicitat, ja que proporcionen fins a 254 adreces útils per segment, més que suficient per a les necessitats actuals del complex. L'esquema d'adreçament bàsic és:

- **VLAN Administració:** xarxa 192.168.10.0/24 (mask 255.255.255.0). Aquesta subxarxa està destinada als equips de gestió i personal. La **porta d'enllaç** (gateway) assignada al router és 192.168.10.1/24 (interfície subif R1.10), i els PCs d'administració utilitzaran adreces dins d'aquest rang (p. ex. 192.168.10.50 per a un PC de secretaria).
- **VLAN Vigilància:** xarxa 192.168.20.0/24 (255.255.255.0). Assignada a càmeres IP, DVRs de seguretat i sistemes de control. El router té 192.168.20.1/24 com a gateway (subif R1.20). Les càmeres i altres dispositius obtindrien IPs en aquest segment (per exemple, 192.168.20.100 per a una càmera).

- **VLAN Públic:** xarxa 192.168.30.0/24 (255.255.255.0). Per als access points Wi-Fi i usuaris convidats. El gateway del router és 192.168.30.1/24 (subif R1.30). Els clients sense fils rebran IPs en aquest rang (ja sigui per DHCP o estàticament, a Packet Tracer es pot simular via DHCP).

**Taula d'adreçament IP i assignació de ports :**

PC	VLAN	IP	Gateway	Switch / Port
PC0	10	192.168.10.10	192.168.10.1	Switch-Admin / Fa0/2
PC5	20	192.168.20.10	192.168.20.1	Switch-Admin / Fa0/4
PC1	30	192.168.30.10	192.168.30.1	Switch-Admin / Fa0/3
PC3	20	192.168.20.11	192.168.20.254	Switch-Pavello / Fa0/3
PC6	30	192.168.30.11	192.168.30.254	Switch-Pavello / Fa0/4
PC2	30	192.168.30.12	192.168.30.254	Switch-Pavello / Fa0/2

*Justificació de les màscares:* s'ha triat /24 per coherència i perquè cobreix àmpliament el nombre de dispositius actual. En un escenari real, es podria ajustar la màscara per cada VLAN en funció de necessitats: per exemple, VLAN Administració potser només requereix unes poques desenes d'adreces (es podria usar /26 per ~62 hosts), mentre que la VLAN Pública podria requerir moltes (en un estadi gran, milers d'usuaris podrien connectar-se al Wi-Fi). En cas necessari, es podria ampliar la VLAN Pública a una subxarxa /23 o /22 per disposar de més adreces, o repartir els APs en múltiples VLANs per distribució de càrrega. En aquesta proposta inicial, però, un /24 per cada segment proporciona simplicitat i encara així permet escalabilitat moderada.



Cada VLAN té **una xarxa IP única** de manera que el router pot fer l'encaminament correctament. La separació en subxarxes també és clau per aplicar ACLs efectives (per exemple, denegar trànsit de 192.168.30.0/24 cap a 192.168.10.0/24 bloquejarà qualsevol accés de VLAN Pública a Administració). Aquest esquema d'adreces facilita la lectura i identificació: els equips d'Administració sempre tindran adreces 192.168.10.x, Vigilància 192.168.20.x i Públic 192.168.30.x, coherent amb els IDs de VLAN (10,20,30).

## Configuració Bàsica de la Xarxa

Un cop definida la topologia i l'adreçament, es procedeix a la **configuració dels dispositius** en Packet Tracer:

- **Configuració de VLANs als switches:** En ambdós switches S1 i S2 es creen les tres VLAN necessàries, assignant-los identificadors i noms descriptius. Per exemple:
  - VLAN 10 → *Administració*
  - VLAN 20 → *Vigilància*
  - VLAN 30 → *Public*

A continuació es mostra la configuració VLAN del commutador ubicat a l'edifici d'administració, on es poden veure els ports assignats a cada VLAN.

VLANs	al	Switch	Administració	(Switch-Admin)
Switch-Admin#show vlan brief				
VLAN Name		Status	Ports	
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2	
10	Administracio	active	Fa0/2	
20	Vigilancia	active	Fa0/4	
30	Public	active	Fa0/3	
1002	fddi-default	active		
1003	token-ring-default	active		
1004	fddinet-default	active		
1005	trnet-default	active		

De manera similar, el switch Pavelló mostra la configuració VLAN següent:

### VLANs al Switch Pavello (Switch-Pavello)

```
Switch-Pavello#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	Administracio	active	
20	Vigilancia	active	Fa0/3
30	Public	active	Fa0/2, Fa0/4
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch-Pavello#
```

```
ACCS RESTRINGIT A PERSONAL AUTORITZAT
```

```
User Access Verification
```

```
Password:
```

```
Router-CEM>show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.10	192.168.10.1	YES	manual	up	up
GigabitEthernet0/0.20	192.168.20.1	YES	manual	up	up
GigabitEthernet0/0.30	192.168.30.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/1.10	unassigned	YES	unset	up	up
GigabitEthernet0/1.20	unassigned	YES	unset	up	up
GigabitEthernet0/1.30	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-CEM>
```

- Als ports on connecten els dispositius finals se'ls configura mode *access* i s'assignen a la VLAN corresponent. Per exemple, el port de S1 on està el PC d'administració es posa en VLAN 10: S1(config-if)# switchport mode access seguit de S1(config-if)# switchport access vlan 10. De forma similar, el port de S2 connectat a la càmera IP s'assigna a VLAN 20, i el port de S2 pel host públic a VLAN 30.
- **Configuració d'enllaços troncal:** El port de S1 que connecta cap a R1 (p. ex. F0/5) es configura com a *trunk* 802.1Q, ja que haurà de portar múltiples VLAN fins al router.

Igualment, el port d'S2 cap a S1 (p. ex. **F0/1** a S2 i **F0/1** a S1) es configuren com trunk. S'utilitza encapsulation dot1Q (en switches Packet Tracer, les comandes serien switchport mode trunk i, si cal, switchport trunk encapsulation dot1q). Aquest pas assegura que el trànsit etiquetat de VLAN pugui circular entre switches i arribar al router.

**Configuració de subinterfícies al router (R1):** A R1, la interfície física connectada a S1 (per ex. G0/0/1) es divideix lògicament en subinterfícies per a cada VLAN.

### Subinterfícies configurades al router Router-CEM

La següent comanda mostra l'estat de les interfícies actives i les subinterfícies configurades al router, amb les IPs assignades com a gateways per a cada VLAN.

ACCS RESTRINGIT A PERSONAL AUTORITZAT

User Access Verification

Password:

Router-CEM>show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.10	192.168.10.1	YES	manual	up	up
GigabitEthernet0/0.20	192.168.20.1	YES	manual	up	up
GigabitEthernet0/0.30	192.168.30.1	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/1.10	unassigned	YES	unset	up	up
GigabitEthernet0/1.20	unassigned	YES	unset	up	up
GigabitEthernet0/1.30	unassigned	YES	unset	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

Router-CEM>

- Es repeteix per a VLAN 30. D'aquesta manera R1 té una interfície virtual a cadascuna de les VLAN, actuant de gateway. *Nota:* No s'ha configurat cap VLAN nativa específica, s'empra la per defecte (VLAN 1) pel trànsit no etiquetat si n'hi hagués, tot i que en aquesta xarxa tot el trànsit de dades va etiquetat en VLAN 10,20,30.
- **Taules d'encaminament:** En aquest escenari amb un sol router, no es requereix configuració addicional de routing dinàmic ni rutes estàtiques, ja que R1 aprèn directament les tres subxarxes connectades. Cada host té com a default gateway l'adreça IP del router a la seva VLAN (p. ex., el PC Admin té gateway 192.168.10.1). Un cop configurades les IPs, els hosts de diferents VLANs **podran comunicar-se a través del router**, ja que aquest fa la funció d'intermediari entre xarxes.
- **Configuració bàsica de commutadors i router:** A més de VLANs i IPs, es realitzen configuracions bàsiques com ara assignar noms als dispositius (**hostname**), configurar contrasenyes d'accés (consola, VTY i *enable secret*, detallat a la secció de seguretat) i desactivar DNS lookup als routers per evitar retards (comandes estàndard de

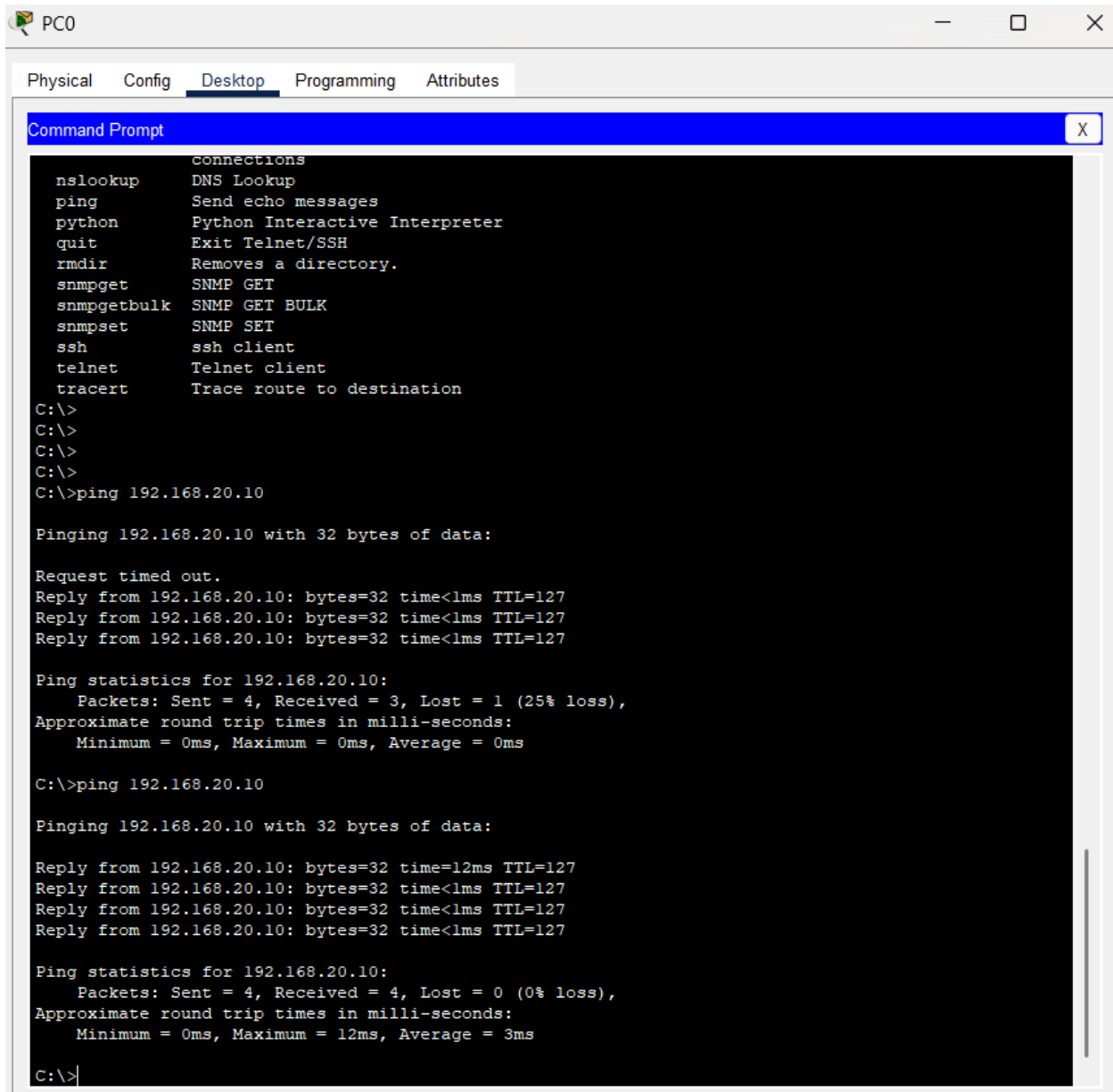
*housekeeping*). No s'entra en detalls en aquest informe, però són passos de "configuració inicial" recomanats.

Un cop realitzada la configuració base, es procedeix a **verificar la connectivitat** entre dispositius de diverses VLAN (abans d'aplicar les restriccions de seguretat). En la simulació, s'han executat comandes *ping* i *traceroute*:

- **Tests de ping sense ACL:** El PC d'Administració (VLAN 10) fa *ping* a la càmera de Vigilància (VLAN 20) i rep resposta satisfactòriament, mostrant que l'encaminament inter-VLAN funciona. De la mateixa manera, un ping des de l'host Públic (VLAN 30) cap al PC d'Administració obté resposta **abans** d'afegir filtres (això després es bloquejarà amb ACL). Aquestes proves indiquen que les subinterfícies del router estan operatives i que els switches etiqueten/descapsulen VLANs correctament.

## Ping amb èxit entre VLAN 10 i VLAN 20

El PC de la VLAN d'Administració (PC0) pot comunicar-se correctament amb un dispositiu de la VLAN de Vigilància, com es mostra a continuació:



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
nslookup      Connections
ping          DNS Lookup
python        Send echo messages
quit          Python Interactive Interpreter
rmdir         Exit Telnet/SSH
snmpget       Removes a directory.
snmpgetbulk   SNMP GET
snmpset       SNMP GET BULK
ssh           SNMP SET
telnet        ssh client
tracert       Telnet client
              Trace route to destination
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time=12ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>
```

- **Traceroute:** Un traceroute des del PC d'Administració cap a l'host Públic mostra dos salts: primer el paquet va al gateway 192.168.10.1 (R1) i després a la IP de destí 192.168.30.X. El router, per tant, és efectivament el node intermedi (salt 1) en la comunicació entre VLANs. Aquesta prova valida el *routing* i alhora permet veure que no hi ha cap camí alternatiu no desitjat (només es passa pel router, com és d'esperar).

En conjunt, la configuració bàsica deixa la xarxa plenament funcional quant a connectivitat: **tots els dispositius poden veure's entre sí a nivell IP** gràcies a l'encaminador. El pas següent consisteix a **aplicar les mesures de seguretat** per restringir aquelles comunicacions que no han d'estar permeses segons la política definida (per exemple, impedir que la VLAN pública accedeixi a les privades).

## Mesures de Seguretat Bàsiques Implementades

Una part fonamental del projecte és incorporar seguretat des del disseny. Un cop la xarxa està operativa, s'han aplicat les següents mesures bàsiques:

**Llistes de Control d'Accés (ACLs) al router:** S'han configurat ACLs esteses sobre les interfícies del router per **filtrar el trànsit entre VLANs**. Concretament, es vol **bloquejar l'accés des de la VLAN Pública cap a les VLAN internes**. La política adoptada és: "Els usuaris de la xarxa pública no poden iniciar connexions cap a recursos d'Administració o Vigilància". En canvi, el trànsit originat des de VLAN Administració o Vigilància sí que podria arribar a VLAN Pública si cal (per exemple, un administrador pot fer ping a un host públic per diagnòstic).

Implementació: es crea una ACL estesa, per exemple anomenada "PUBLIC-OUT" aplicada **entrant** sobre la subinterfície del router de VLAN 30 (Públic). Aquesta ACL conté línies que *deneguen* qualsevol paquet amb origen 192.168.30.0/24 i destinació 192.168.10.0/24 (Administració) o 192.168.20.0/24 (Vigilància). A continuació, una línia *permet* any assegura que la resta de trànsit està permès (per exemple, accés a internet o a un servidor públic si n'hi hagués). D'aquesta manera, quan un host de VLAN 30 intenta accedir a un equip de VLAN 10 o 20, el router descarta el trànsit.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#ip access-list extended PUBLIC-OUT
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/0.30
Router(config-subif)#ip access-group PUBLIC-OUT in
Router(config-subif)#exit
Router(config)#
Router(config)#end
```

- Aquesta ACL atura els accessos *no desitjats* entre VLANs mantenint, però, la possibilitat de comunicació en sentit contrari o cap a fora. Aplicar l'ACL en ingress de la VLAN font (la pública) és eficient perquè centralitza el filtratge només on cal. Si es volgués una segmentació encara més estricta, es podrien afegir ACLs a les altres VLANs també (per exemple bloquejant accés de Vigilància cap a Administració excepte certs protocols, etc.), però per simplicitat s'ha implementat només la restricció més

crítica (Públic).

- **Contrasenyes i seguretat d'accés als dispositius:** Tots els dispositius de xarxa han estat configurats amb contrasenyes per evitar accés no autoritzat a la configuració. En el router R1, s'ha establert una *enable secret* encriptada, contrasenya per a la línia de consola i per a les línies vty (accessos Telnet/SSH). Igualment als switches S1 i S2 se'ls ha posat contrasenya de consola, vty i enable. A més, s'ha configurat el *login* local o per password segons el cas, i banners legals d'avís (*message of the day*) per dissuadir accessos indeguts. Aquestes mesures garanteixen que només personal autoritzat pugui modificar la configuració de la xarxa. (En un entorn real, es recomanaria emprar SSH en lloc de Telnet per xifrar les sessions d'administració; en Packet Tracer això també es pot simular generant claus RSA i activant *ip ssh*).
- **Desactivació de ports no utilitzats:** Als commutadors, tots els ports d'accés que queden lliures (no connectats a cap dispositiu en la topologia actual) han estat **apagats administrativament** mitjançant la comanda *shutdown*. Aquesta és una pràctica recomanada de seguretat: si un port està inactiu, es deixa *down* de manera que ningú pugui connectar un dispositiu sense autorització i accedir a la xarxa. Alternativament, es podria col·locar aquests ports en una VLAN específica "VLAN buida" sense cap connexió, però la forma més senzilla és tancar-los. Si en un futur cal utilitzar algun d'aquests ports, l'administrador habilitarà (*no shutdown*) i assignarà la VLAN apropiada en el moment oportú.
- **Altres mesures addicionals:** Encara que fora de l'abast mínim, es podrien mencionar altres configuracions realitzades o recomanades: per exemple, *disable CDP* o LLDP en ports públics (per no revelar informació de la infraestructura), configurar *port security* en ports d'accés per limitar quines MAC poden connectar-se (aquest mecanisme permet associar una MAC al port i, si se'n connecta una de diferent, el port es pot desactivar automàticament). En aquest projecte bàsic, no obstant, no s'ha aplicat *port-security* per simplicitat i perquè pot complicar les simulacions, però seria una millora factible. També es deixa la VLAN 1 (per defecte) buida sense assignar dispositius, i es procura no utilitzar credencials per defecte ni serveis innecessaris als dispositius.

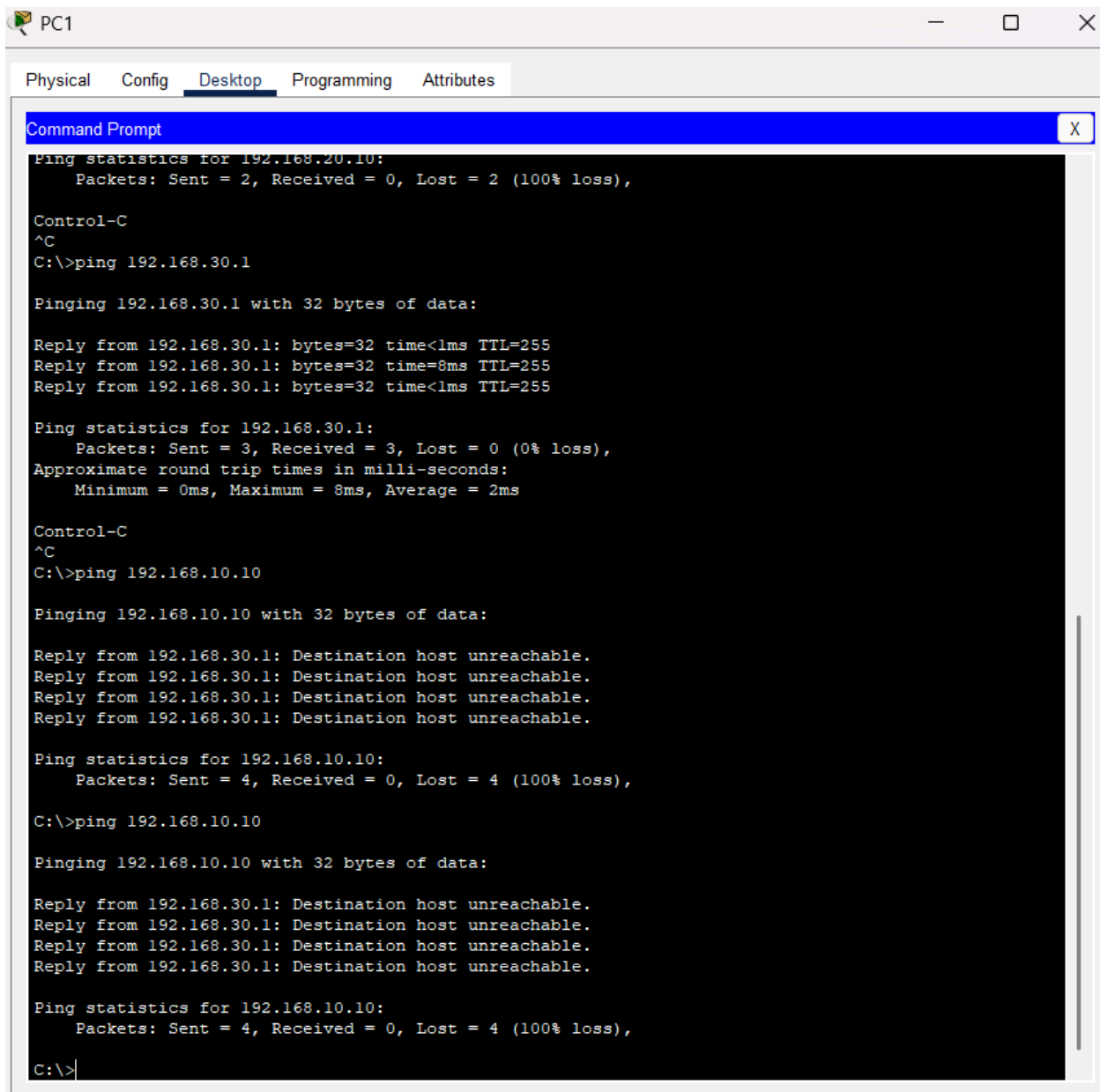
Amb aquestes configuracions, la xarxa ha millorat significativament el seu perfil de seguretat: cada VLAN resta aïllada segons les polítiques establertes, i l'accés als equips de gestió de la xarxa està protegit per contrasenya. S'ha reduït la superfície d'atac apagant ports sobrants i s'han establert controls sobre el trànsit entre segments, tot mantenint la funcionalitat requerida.

## Validació de la Xarxa i Resultats de les Proves

Després d'aplicar les configuracions de seguretat, s'han realitzat noves proves per **validar el comportament de la xarxa** conforme als requeriments. A continuació es detallen els resultats més rellevants:

El PC situat a la VLAN Pública no pot accedir a dispositius de la VLAN Administració, demostrant l'efectivitat de les ACL configurades al router:

### Ping bloquejat per ACL des de VLAN Pública a VLAN Administració



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.20.10:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time=8ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

Control-C
^C
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

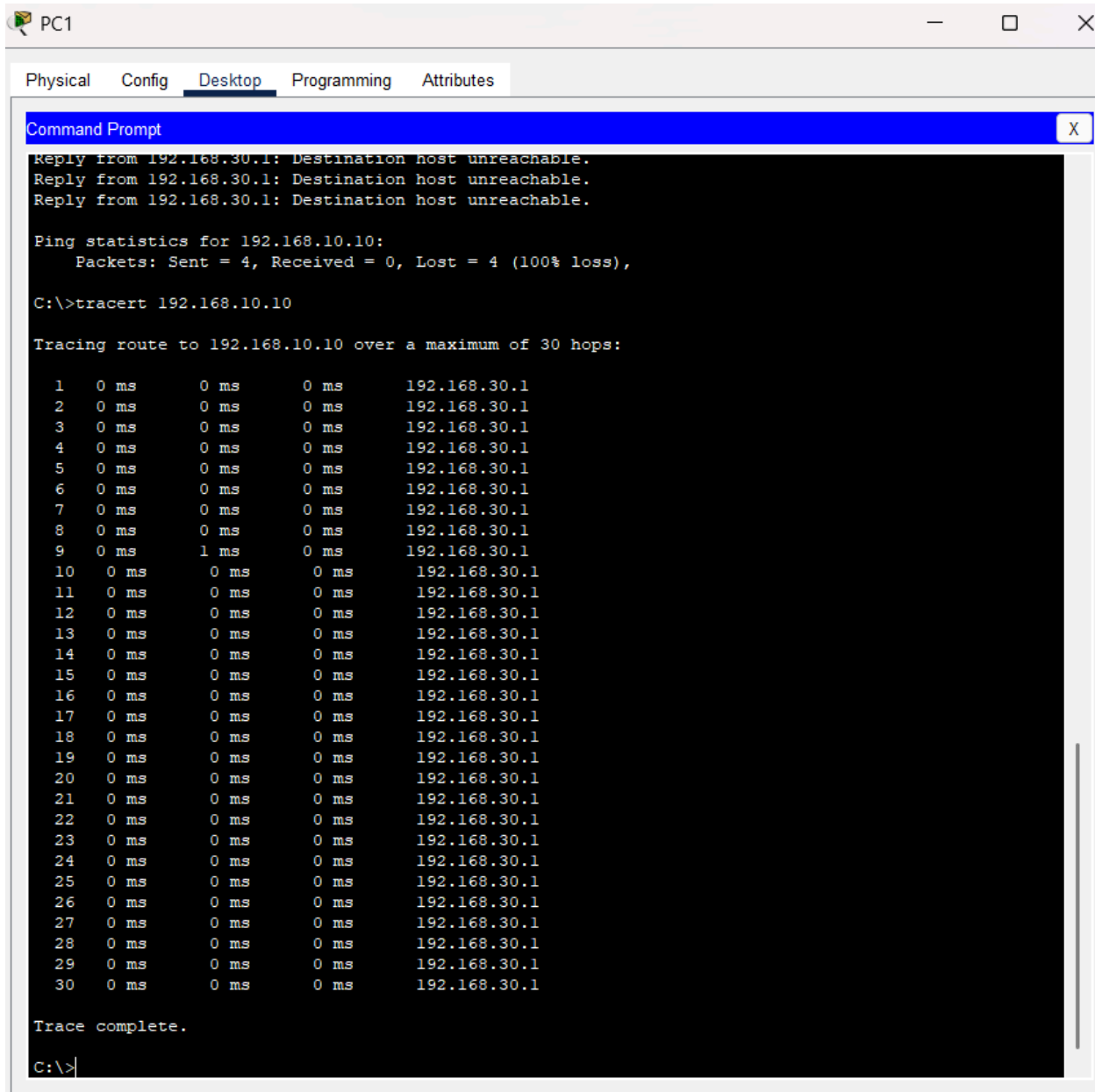
Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



- **Aïllament de VLAN Pública verificat:** Tal com es pretenia, els dispositius de la VLAN Pública **ja no poden accedir a recursos interns**. En la simulació, el *PC Públic* (192.168.30.x) intenta fer *ping* al PC d'Administració (192.168.10.x) i a la càmera (192.168.20.x). Tots dos intents fallen (host unreachable o timeout), indicant que l'ACL del router està bloquejant aquests paquets. Aquest resultat és esperat i desitjat: la xarxa pública queda restringida. Cal destacar que abans d'implementar l'ACL aquests pings tenien resposta, i ara correctament no en tenen, demostrant l'efectivitat de la llista de control d'accés.
- **Connectivitat interna mantinguda:** Els dispositius d'Administració i Vigilància continuen podent comunicar-se entre ells si cal. Per exemple, es comprova que el PC d'Administració pot accedir al servidor de vídeo (en cas de tenir-ne) o fer ping a la càmera de vigilància. En el nostre cas, un ping del PC Admin a la IP de la càmera (192.168.20.100) té resposta satisfactòria. Això indica que l'ACL aplicada no impedeix aquesta comunicació (tal com la vam dissenyar, només filtra trànsit entrant de VLAN 30). També un ping des de PC Admin a un hipotètic host públic 192.168.30.x funcionaria, ja que l'ACL no bloqueja eixe trànsit en sentit invers; no obstant, no és un cas d'ús necessari però demostra que l'ACL és específica i no provoca bloquejos col·laterals.
- **Encaminament i taules de routing:** Mitjançant comandes `show ip route` al router, es valida que hi figuren les rutes directament connectades a 192.168.10.0/24, 192.168.20.0/24 i 192.168.30.0/24 via les subinterfícies adequades. Les taules ARP als dispositius també mostren les MAC del router corresponents a cada VLAN (gateway). Tot això indica que la configuració lògica de VLANs i subxarxes és correcta.

- **Proves de traceroute post-ACL:** S'ha repetit un traceroute des de l'host Públic cap a un host d'Administració per veure el comportament. Ara el traceroute es queda aturat al primer salt (el router) i no arriba a destí, consistent amb el fet que el router està denegant el trànsit més enllà. Aquesta és una confirmació addicional que l'ACL filtra els paquets com esperat.



The screenshot shows a window titled "PC1" with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the results of a ping and a traceroute to the IP address 192.168.10.10.

```
Reply from 192.168.30.1: Destination host unreachable.  
Reply from 192.168.30.1: Destination host unreachable.  
Reply from 192.168.30.1: Destination host unreachable.  
  
Ping statistics for 192.168.10.10:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>tracert 192.168.10.10  
  
Tracing route to 192.168.10.10 over a maximum of 30 hops:  
  
  0  0 ms    0 ms    0 ms    192.168.30.1  
  1  0 ms    0 ms    0 ms    192.168.30.1  
  2  0 ms    0 ms    0 ms    192.168.30.1  
  3  0 ms    0 ms    0 ms    192.168.30.1  
  4  0 ms    0 ms    0 ms    192.168.30.1  
  5  0 ms    0 ms    0 ms    192.168.30.1  
  6  0 ms    0 ms    0 ms    192.168.30.1  
  7  0 ms    0 ms    0 ms    192.168.30.1  
  8  0 ms    0 ms    0 ms    192.168.30.1  
  9  0 ms    1 ms    0 ms    192.168.30.1  
 10  0 ms    0 ms    0 ms    192.168.30.1  
 11  0 ms    0 ms    0 ms    192.168.30.1  
 12  0 ms    0 ms    0 ms    192.168.30.1  
 13  0 ms    0 ms    0 ms    192.168.30.1  
 14  0 ms    0 ms    0 ms    192.168.30.1  
 15  0 ms    0 ms    0 ms    192.168.30.1  
 16  0 ms    0 ms    0 ms    192.168.30.1  
 17  0 ms    0 ms    0 ms    192.168.30.1  
 18  0 ms    0 ms    0 ms    192.168.30.1  
 19  0 ms    0 ms    0 ms    192.168.30.1  
 20  0 ms    0 ms    0 ms    192.168.30.1  
 21  0 ms    0 ms    0 ms    192.168.30.1  
 22  0 ms    0 ms    0 ms    192.168.30.1  
 23  0 ms    0 ms    0 ms    192.168.30.1  
 24  0 ms    0 ms    0 ms    192.168.30.1  
 25  0 ms    0 ms    0 ms    192.168.30.1  
 26  0 ms    0 ms    0 ms    192.168.30.1  
 27  0 ms    0 ms    0 ms    192.168.30.1  
 28  0 ms    0 ms    0 ms    192.168.30.1  
 29  0 ms    0 ms    0 ms    192.168.30.1  
 30  0 ms    0 ms    0 ms    192.168.30.1  
  
Trace complete.  
  
C:\>
```

- **Altres comprovacions:** Es revisen configuracions com show vlan brief als switches per assegurar que els ports estan a la VLAN correcta (per exemple, el port de PC Admin apareix a VLAN 10, etc.), i show interface status per verificar que els ports no utilitzats estan efectivament en disabled. Tot concorda amb la configuració prevista. També es fa un test connectant un PC de prova a un port apagat per veure que no té accés fins que l'administrador l'activi – en Packet Tracer això es veu perquè l'enllaç roman down.

En conjunt, els resultats de les proves confirmen que la xarxa funciona de manera **viable i segura**: hi ha **connectivitat entre les parts que ho requereixen** (p. ex. accés d'Administració a Vigilància) i **isolament on cal** (p. ex. aïllant els convidats/públic). Els objectius funcionals es compleixen, ja que es poden fer arribar paquets entre VLANs via router quan està permès, i els objectius de seguretat també, bloquejant trànsit no desitjat.

## Conclusions i Millores Futures

En conclusió, s'ha dissenyat i implementat una proposta de **Xarxa Corporativa Segura** per al Complex Esportiu Municipal complint els requisits establerts. La solució presenta una topologia senzilla (un router i dos switches) però eficaç, amb **segmentació mitjançant VLANs** per aïllar trànsits d'administració, vigilància i públic. S'han satisfet els objectius inicials: els equips de cada departament es troben en xarxes separades i optimitzades, s'ha configurat encaminament inter-VLAN per permetre comunicació quan cal i s'han aplicat mesures bàsiques de seguretat (ACLs, contrasenyes, tancament de ports) per protegir la infraestructura i les dades.

**Beneficis obtinguts:** La segmentació realitzada millora la **seguretat i gestió de la xarxa**. Cada VLAN actua com una xarxa independent amb les seves pròpies regles, de manera que la comunicació entre VLANs queda regulada pel router i les ACLs. Això ha permès, per exemple, garantir que els usuaris públics no tinguin accés a sistemes interns ni a càmeres de seguretat, alhora que el personal intern pot treballar sense interferències del trànsit de convidats. A més, la reducció de dominis de broadcast per VLAN pot millorar el rendiment de la LAN i evita que dispositius IoT o de convidats generin trànsit innecessari a la xarxa d'administració.

**Limitacions:** Val a dir que aquesta és una xarxa petita i amb mecanismes de seguretat bàsics. En un entorn real podrien fer falta solucions més robustes. Per exemple, no s'ha inclòs cap **firewall dedicat** o sistema de detecció d'intrusions que filtrés tràfic cap a Internet o entre segments amb criteris més avançats. Tampoc s'ha tractat la segmentació de la xarxa Wi-Fi pública respecte a Internet (s'assumeix que simplement té accés a Internet però no a la LAN interna). La disponibilitat és un altre punt: amb un sol router, no hi ha redundància en cas de fallada d'aquest. Igualment, un sol enllaç troncal entre switches pot ser un punt dèbil (en entorns reals s'usarien protocols com Spanning Tree i llinks redundants o EtherChannel per garantir tolerància a fallades).

**Millores futures proposades:**

- Implementar dispositius de seguretat perimetral: per exemple, afegir un firewall entre la xarxa interna i la connexió a Internet, amb polítiques que controlin també el trànsit sortint i entrant de la xarxa del complex. Això és especialment important si serveis com el ticketing han de ser accessibles des d'Internet, o per prevenir atacs dirigits als dispositius IoT.
- **VLAN de gestió:** Actualment no s'ha creat una VLAN específica de gestió per als propis switches i router. Seria aconsellable tenir, per exemple, una VLAN de gestió (ex: VLAN 99) amb una subxarxa dedicada (potser 192.168.99.0/24) on només el personal d'IT tingui accés, i moure-hi les IPs de gestió dels switches. Això aïlla completament l'accés d'administració de la infraestructura fora de les VLAN de producció.
- **Control d'accés més fi en VLAN Vigilància:** Es podria afegir ACLs addicionals per assegurar que només certs equips (p. ex. un servidor d'enregistrament o els PCs de seguretat) puguin accedir a les càmeres, i no tota la VLAN Administració sencera. Això minimitzaria l'exposició en cas que un PC d'oficina fos compromès, per exemple. També es podrien segmentar dispositius IoT en més VLANs si n'hi ha de diferents tipus (una per càmeres, altra per sensors, etc.) segons el principi de mínima confiança.
- **Xarxa pública amb portal captiu i VLAN separada per convidats:** Per a millorar l'experiència dels usuaris i la seguretat, es podria implementar un portal captiu per la Wi-Fi pública, requerint autenticació o acceptació de termes. Això podria anar de la mà amb col·locar la Wi-Fi en una DMZ que només dona accés a Internet però no a sistemes interns. També es podria habilitar un servidor DHCP dedicat per VLAN pública amb controls (com *IP source guard*).
- **Ús de commutadors de capa 3:** En lloc d'un router físic independent, una millora de rendiment seria utilitzar un **switch capa 3** per fer l'encaminament intern entre VLANs. Això reduiria la latència i potencialment augmentaria l'ample de banda entre segments (ja que un switch de capa 3 pot commutar paquets entre VLANs a velocitats de backplane, vs. un router que podria ser més lent). També permetria funcionalitats avançades com routing dinàmic intern, QoS per VLAN (p. ex. prioritzar vídeo de vigilància) i llistes de control d'accés a nivell de maquinari.
- **Redundància i escalabilitat:** Si el complex creix, es podrien afegir més switches distribuïts (p. ex. un switch a zona de piscines, un altre a gimnàs) formant un troncet amb S1/S2. En aquest cas, caldria vigilar l'STP i potser replantejar una arquitectura jeràrquica (core/distribution/access). També es podria contemplar tenir dos routers o un protocol de failover (HSRP/VRRP) per assegurar que si cau l'encaminador principal, la xarxa no quedi inutilitzada.