perplexity

Btw here is all the desription that need to be solved:

10.0.0.0/9
VLAN10 813 állomás 2001:DB8:ACDC:10::/64
VLAN20 119 állomás 2001:DB8:ACDC:30::/64

1.Feladat
R1 - SSH admin/cisco
Lo0 - 95.95.95.0/30
VLAN10 címeit PAT → Lo0
alapértelmezett út a Lo0
G0/0 beállítása
DHCPv4 és SLAAC+DHCPv6
Syslog - 3-as vagy súlyosabb

2.Feladat:
S1 - SSH max 1 user admin/cisco
F0/5 - VLAN10
F0/15 - VLAN30
Sticky portbiztonság → dobja és naplózza
Felügyeleti IP mindkét VLAN-ban, mindkét 3.rétegbeli protokolba

3.Feladat:
R1 és S1 mentése TFTP-vel PC2-re

Below is a complete Packet Tracer configuration for the three tasks. First, we define the subnetting for the required host counts and IPv6 prefixes. Then we configure R1 (SSH, Loopback, sub-interfaces, PAT, DHCPv4/v6, syslog), S1 (SSH, VLANs, port security, management SVIs, SSH session limit), and finally show how to back up both devices to PC2 via TFTP.

A summary of the addressing plan:

VLAN	Hosts needed	IPv4 prefix	Mask	IPv6 prefix
10	813	10.0.0.0/22	255.255.252.0	2001:DB8:ACDC:10::/64
20/30	119	10.0.4.0/25	255.255.255.128	2001:DB8:ACDC:30::/64
-	-	**Loopback0:**	/30 (95.95.95.0)	-

1. Router R1 Configuration

Basic settings and SSH

```
R1> enable
R1# configure terminal
R1(config)# hostname R1
R1(config)# ip domain-name local.lab
R1(config)# username admin privilege 15 secret cisco
R1(config)# crypto key generate rsa modulus 2048
R1(config)# ip ssh version 2
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

(SSH setup requires hostname, domain, RSA keys, and line vty config)[1] [2]

Loopback0 and default route

```
R1(config)# interface loopback0
R1(config-if)# ip address 95.95.95.1 255.255.255.252
R1(config-if)# ip nat outside
R1(config-if)# exit

R1(config)# ip route 0.0.0.0 0.0.0.0 95.95.95.2
```

(Loopback for PAT outside and default gateway)[3]

Router-on-a-Stick and NAT/PAT

```
! Sub-interface for VLAN10
R1(config)# interface gigabitEthernet0/0.10
R1(config-if)# encapsulation dot1Q 10
R1(config-if)# ip address 10.0.0.1 255.255.252.0
R1(config-if)# ip nat inside
R1(config-if)# ipv6 address 2001:DB8:ACDC:10::1/64
R1(config-if)# exit

! Sub-interface for VLAN30
R1(config)# interface gigabitEthernet0/0.30
R1(config-if)# encapsulation dot1Q 30
R1(config-if)# ip address 10.0.4.1 255.255.255.128
R1(config-if)# ip nat inside
R1(config-if)# ipv6 address 2001:DB8:ACDC:30::1/64
R1(config-if)# exit

! PAT for all VLAN10 hosts
R1(config)# access-list 1 permit 10.0.0.0 0.0.3.255
R1(config)# ip nat inside source list 1 interface loopback0 overload
```

(802.1Q sub-interfaces and PAT configuration)[4]

DHCPv4 pools

```
R1(config)# ip dhcp excluded-address 10.0.0.1 10.0.0.10
R1(config)# ip dhcp excluded-address 10.0.4.1 10.0.4.10

R1(config)# ip dhcp pool VLAN10
R1(config-dhcp)# network 10.0.0.0 255.255.252.0
R1(config-dhcp)# default-router 10.0.0.1
R1(config-dhcp)# exit

R1(config)# ip dhcp pool VLAN30
R1(config-dhcp)# network 10.0.4.0 255.255.255.128
R1(config-dhcp)# default-router 10.0.4.1
R1(config-dhcp)# exit
```

(DHCP for both VLANs)[4]

IPv6 SLAAC + DHCPv6

```
R1(config)# ipv6 unicast-routing

R1(config)# ipv6 dhcp pool VLAN10-V6
R1(config-dhcpv6)# address prefix 2001:DB8:ACDC:10::/64
R1(config-dhcpv6)# dns-server 2001:4860:4860::8888
R1(config-dhcpv6)# exit

R1(config)# interface g0/0.10
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp server VLAN10-V6
R1(config-if)# exit

R1(config)# interface g0/0.30
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp server VLAN10-V6
R1(config-if)# exit
```

(Stateless address autoconfig and DHCPv6)[4]

Syslog to PC2

```
R1(config)# logging host 10.0.4.11
R1(config)# logging trap errors
```

(Syslog severity 3 and higher)[5]

2. Switch S1 Configuration

Basic settings and SSH (max 1 session)

```
S1> enable
S1# configure terminal
```

```
S1(config)# hostname S1
S1(config)# ip domain-name local.lab
S1(config)# username admin privilege 15 secret cisco
S1(config)# crypto key generate rsa modulus 2048
S1(config)# ip ssh version 2
S1(config)# line vty 0 4
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# session-limit 1
S1(config-line)# exit
```

(SSH plus session-limit)[1]

VLANs and access ports

```
S1(config)# vlan 10
S1(config-vlan)# name Clients
S1(config-vlan)# exit
S1(config)# vlan 30
S1(config-vlan)# name Guests
S1(config-vlan)# exit

S1(config)# interface range fa0/5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# switchport port-security
S1(config-if-range)# switchport port-security maximum 1
S1(config-if-range)# switchport port-security violation restrict
S1(config-if-range)# switchport port-security mac-address sticky
S1(config-if-range)# exit

S1(config)# interface range fa0/15
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 30
S1(config-if-range)# switchport port-security
S1(config-if-range)# switchport port-security maximum 1
S1(config-if-range)# switchport port-security violation restrict
S1(config-if-range)# switchport port-security mac-address sticky
S1(config-if-range)# exit
```

(Port security with sticky MACs and violation restrict/log)[6]

Trunk to R1

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 10,30
S1(config-if)# exit
```

(802.1Q trunk setup)[4]

Management SVIs for IPv4 and IPv6

```
S1(config)# interface vlan 10
S1(config-if)# ip address 10.0.0.2 255.255.252.0
S1(config-if)# ipv6 address 2001:DB8:ACDC:10::2/64
S1(config-if)# no shutdown
S1(config-if)# exit

S1(config)# interface vlan 30
S1(config-if)# ip address 10.0.4.2 255.255.255.128
S1(config-if)# ipv6 address 2001:DB8:ACDC:30::2/64
S1(config-if)# no shutdown
S1(config-if)# exit

S1(config)# ip default-gateway 10.0.0.1
S1(config)# ipv6 route ::/0 2001:DB8:ACDC:10::1
```

(Management IPs in both VLANs, IPv4 and IPv6)[4]

Syslog to PC2

```
S1(config)# logging host 10.0.4.11
S1(config)# logging trap warnings
```

(Syslog severity ≥4)[5]

3. Backups to PC2 via TFTP

On PC2 (10.0.4.11) enable the TFTP server under **Desktop** → **TFTP**.

On R1:

```
R1# copy running-config tftp:
Address or name of remote host []? 10.0.4.11
Destination filename [running-config]? R1-backup
```

On S1:

```
S1# copy running-config tftp:
Address or name of remote host []? 10.0.4.11
Destination filename [running-config]? S1-backup
```

(TFTP backup commands)[5] [7]

With these configurations, R1 and S1 support SSH, VLANs, PAT, DHCPv4/v6, port security, syslog, and TFTP backups exactly as required.

⁂

1. IMG_20250416_083932909_HDR.jpg

2. https://www.taufiknurhuda.web.id/2022/06/10/how-to-backup-and-restore-configuration-on-cisco-packet-tracer/
3. https://sites.radford.edu/~hlee3/classes/backup/itec451_spring2017/Cisco/CCNA2_RSE_spring2017/Lab Source Files_solutions/6.3.3.7 Lab - Configuring 802.1Q Trunk-Based Inter-VLAN Routing - solution.pdf
4. https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html
5. https://community.cisco.com/t5/switching/unable-to-backup-switch/td-p/4190327
6. https://szit.hu/doku.php?id=oktatas%3Ahalozat%3Acisco%3Arouter
7. https://itskillbuilding.com/cisco/device-management/backup-restore-cisco-router-switch-configuration-files-tftp/