Routing

static routing

default route (alapértelmezett útvonal) => a nem ismert címeket itt küldi ki:

```
ip route 0.0.0.0 0.0.0.0 [g0/0]
```

A `192.168.10.0/24` (`255.255.255.0`) hálózatot a `10.1.1.3`-as címnél lehet elérni. Itt a `10.1.1.3` a *next hop IP*:

```
ip route [192.168.10.0] [255.255.255.0] [10.1.1.3]
```

Ugyanezt a hálózatot itt a `g0/1`-es porton lehet elérni, az abba a hálózatba szánt csomagokat a porton küldi ki. Ez az *exit interface*.

```
ip route [192.168.10.0] [255.255.255.0] [g0/1]
```

Floating static route (`200`-as *administrative distance*), azaz backup route:

```
ip route [192.168.10.0] [255.255.255.0] [g0/1] [200] ! ha el van hagyva,
1
```

OSPF

wildcard maszkokat használ (subnet maszk bitjeinek negálása)

```
router ospf [1]

    router-id [1.1.1.1]

    network [10.0.0.0] [0.0.0.255] area [0]



    passive-interface default ! alapból így az összes interface passzív
lesz

    no passive-interface [g0/0]



    area 0 authentication message-digest ! area szintű hitelesítés



int [g0/0]

    ip ospf authentication message-digest

    ip ospf message-digest-key 1 md5 [#Aa12345]
```

DHCP / statikus címkiosztás

IPv4

```
ip dhcp excluded-address [192.168.10.1] [192.168.10.10] ! intervallum
rezerválása

ip dhcp excluded-address [192.168.10.254] ! egy darab rezerválása



ip dhcp pool [VLAN10-POOL]

    network [192.168.10.0] [255.255.255.0]
```

```
    default-router [192.168.10.1]
    dns-server [8.8.8.8]
    lease [7] ! napokban
```

IPv6

```
ipv6 unicast-routing
```

statikus IPv6

```
int [g0/1]
    ipv6 address [2001:db8:10::1/64]
    no shut
```

SLAAC

Nincs DHCPv6 szerver, a kliensek maguknak generálnak címeket.

```
int [g0/1]
    no ipv6 nd other-config-flag
    no ipv6 nd managed-config-flag
    ipv6 address [2001:db8:10::1/64]
    ipv6 address [2001:db8:10::/64]
```

```
    no shut
```

Stateless DHCPv6 (DHCPv6 + SLAAC)

Van DHCPv6 szerver, a kliensek maguknak generálnak címeket, és egyéb (pld DNS) infókat a DHCPv6 szervertől kérnek.

```
ipv6 dhcp pool [DHCPV6-STATELESS]

    dns-server [2001:4860:4860::8888]



interface [g0/1]

    ipv6 enable

    no ipv6 nd managed-config-flag

    ipv6 nd other-config-flag

    ipv6 address [2001:db8:20::1/64]

    ipv6 dhcp server [DHCPV6-STATELESS]
```

Stateful DHCPv6

Van DHCPv6 szerver, a kliensek tőle kapják a címük.

```
ipv6 dhcp pool [DHCPV6-STATEFUL]

    address prefix [2001:db8:40::/64]

    dns-server [2001:4860:4860::8888]
```

```
interface g0/2

    ipv6 enable

    ipv6 nd managed-config-flag

    ipv6 nd prefix-default no-autoconfig

    ipv6 dhcp server [DHCPV6-STATEFUL]
```

STP (spanning-tree)

STP módok, elsődleges, másodlagos

Mode	Name	Description
STP	PVST	Original STP, slow convergence (~30-50s). One instance per VLAN (Cisco enhancement).
RSTP	Rapid PVST+	Faster convergence (~1-2s), backward-compatible with 802.1D. One instance per VLAN (Cisco enhancement).
MSTP	MST (Multiple STP)	Maps multiple VLANs to a single STP instance, scalable for large networks.
PVST+	PVST+	Cisco’s proprietary version of 802.1D with one STP instance per VLAN.
Rapid PVST+	Rapid PVST+	Cisco’s proprietary version of RSTP with one instance per VLAN.

```
spanning-tree mode pvst        ! Standard STP (Per-VLAN)

spanning-tree mode rapid-pvst  ! Rapid STP (Per-VLAN)

spanning-tree mode mst         ! Multiple STP Instances
```

Bridge priority (`24576`) beállítása (`10` -es VLAN). A legkissebb priority lesz a root bridge. Csak 4096-os lépésekben, az alapérték 32768:

```
spanning-tree vlan [10] priority [24576]
```

Vagy ha ez a cél:

```
spanning-tree vlan [10] root primary

spanning-tree vlan [10] root secondary ! backup
```

STP portok

Port roles

Port Role	Description
Root Port (RP)	The port on a non-root switch with the best path to the root bridge. There is only one root port per switch per VLAN. It forwards traffic toward the root.
Designated Port (DP)	The port on a network segment that is selected to forward frames toward and away from that segment. Each segment has one designated port. Usually, the port closest to the root bridge on that segment.
Alternate Port (AP)	A port that provides an alternate path to the root but is **blocking** to prevent loops. It can replace the root port if it fails.
Backup Port (BP)	A port that provides a redundant connection to the **same segment** as the designated port and is also in blocking state. Rarely used because physical redundant segments are uncommon.
Disabled Port	A port administratively shut down or otherwise disabled and does not participate in STP.

RSTP esetén csak:

- Root Port
- Designated Port
- Alternate Port / Backup Port

Port States

Port State	Description	Can Forward Frames?	Can Learn MAC Addresses?
Blocking	Listens for BPDUs, does not forward frames or learn MACs (except for BPDUs)	No	No
Listening	Processes BPDUs, prepares to forward, clears MAC table entries for port	No	No
Learning	Learns MAC addresses but does not forward frames yet	No	Yes
Forwarding	Forwards frames and learns MAC addresses	Yes	Yes
Disabled	Port is disabled, no STP participation	No	No

RSTP esetén csak:

- Discarding: Blocking + Listening + Disabled
- Learning
- Forwarding

BPDU guard & portfast

A `portfast` portok ignorálva lesznek STP számítások során, így gyorsabban konvergál a hálózat.

A BPDU guard pedig megakadályozza, hogy az adott porton bejövő BPDU-k (úgyszintén STP számításhoz) fel legyenek dolgozva.

```
! alapértelmezett

spanning-tree portfast default

spanning-tree bpduguard default



! interfészeken (csak access, nem lehet trunk)

int f0/1
```

```
    spanning-tree portfast

    spanning-tree bpduguard enable
```

ACL

Type	Description
Standard ACL	Filters source IP only (1-99)
Extended ACL	Filters source, destination, protocol, and ports (100+)
Named ACL	More readable and modifiable ACLs (standard/extended)
Direction	Meaning
in	Traffic **entering** the interface.
out	Traffic **leaving** the interface.

Továbbá a default esemény, hogy minden nem engedélyezettet tilt!

Nem mindig kell teljes IP cím tartomány, ha csak egy hosttal dolgozunk lecserélhetők a hálózatcím és wildcard bitek. A HTTP forgalom engedélyezése `10.0.0.140` számára és minden más tiltása mindenki másnak:

```
access-list 100 permit tcp host 10.0.0.140 eq 80 any
```

Standard ACL

Engedélyezi a `g0/1`-en bejövő forgalmat a `192.168.1.0/24` hálózattól (forráscímet vizsgál). A többit tiltja.

```
access-list 10 permit 192.168.1.0 0.0.0.255

access-list 10 deny any
```

```
int g0/1

    ip access-group 10 in
```

Extended ACL

Engedélyezi a `g0/1`-en kimenő, `192.168.1.0/24`-es hálózatból jövő HTTP(TCP, 80-as port) forgalmat, minden mást pedig tilt.

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80

access-list 100 deny ip any any



interface g0/1

    ip access-group 100 out
```

Named ACL

FTP tiltása, minden más engedélyezése.

```
ip access-list extended BLOCK_FTP

    deny tcp any any eq 21

    permit ip any any



interface g0/1

    ip access-group BLOCK_FTP in
```

NAT

Static NAT

Pld. van egy webszerver `192.168.1.100`-nál (privát), amit el kéne érni `203.0.113.5`-ös (publikus) címen.

Az `ip nat inside` jelzi a privát címtartományú portot, az `ip nat outside` pedig a külsőt.

```
interface [g0/0]

 ip address [203.0.113.1] [255.255.255.0]

 ip nat outside



interface [g0/1]

 ip address [192.168.1.1] [255.255.255.0]

 ip nat inside



ip nat inside source static [192.168.1.100] [203.0.113.5]
```

Dynamic NAT

Az ACL-el engedett IP című forgalmat kiengedi, a `203.0.113.10`-től `203.0.113.20`-ig tartó publikus tartományban lévő címek valamelyikével. (Ugyanúgy kell `ip nat inside` és `outside`

```
ip nat pool [MYPOOL] [203.0.113.10] [203.0.113.20] netmask
[255.255.255.0]

access-list [1] permit [192.168.1.0] [0.0.0.255]
```

```
ip nat inside source list [1] pool [MYPOOL]
```

PAT (Port Address Translation) / NAT Overload

Egy publikus interfészen (címen) több belső IP-t is kienged egyszerre, port alapon követi hogy kihez tartozik az adott traffic.

A `g0/0` port a külső, publikus port.

```
access-list [1] permit [192.168.1.0] [0.0.0.255]


ip nat inside source list [1] interface [g0/0] overload
```

Redundancia

FHRP (HSRP)

Feltéve, hogy több VLAN esetén is szeretnénk routeren:

```
int g0/0.[10]

    ip addr [192.168.10.2] [255.255.255.0] ! R saját címe

    ip helper-address [192.168.30.254] ! ha más hálózatban/VLANban van a
DHCP szerver

    standby version 2

    standby [10] ip [192.168.10.1] ! a virtuális IP

    standby [10] priority [95] ! magasabb kap prioritást
```

```
    standby [10] preempt ! vegye vissza
```

Link-aggregation (etherchannel)

-	Active	Passive
Active	✅	✅
Passive	✅	❌

-	Desirable	Auto
Desirable	✅	✅
Auto	✅	❌

```
int r f0/[1-2]

    sw mode trunk

    channel-group [1] mode [active]

int port-channel [1]

    sw mode trunk
```

VLANok

VLAN létrehozása

```
vlan 10

    name [SALES]

vlan 20
```

```
    name [josh]
```

Access, Trunk portok

```
int f0/1

    sw mode access

    sw access vlan [10]

int g0/1

    sw mode trunk

    sw trunk native vlan [99]

    sw trunk allowed vlan [10,20,30] ! ez meghatározza, hogy a trunk
vonalon milyen vlanokat enged
```

Inter-VLAN routing routeren (Router-on-a-Stick)

```
int g0/0.[10]

    encapsulation dot1Q [10]

    ip address [192.168.10.1] [255.255.255.0]

int g0/0.[20]

    encapsulation dot1Q [20] native

    ip address [192.168.20.1] [255.255.255.0]

int g0/0
```

```
    no shut
```

Inter-VLAN routing MSW-n

```
ip routing

int vlan [10]

    ip address [192.168.20.1] [255.255.255.0]

    no shut
```

VTP

mode	mit csinál?
server	VLAN definíciók szolgáltatása
client	VLAN definíciók alkalmazása
transparent	csak továbbítja a definíciókat, de nem alkalmazza

```
vtp mode [server]

vtp domain [xycompany]

vtp password [#Aa12345]

vtp version 2
```

Biztonsági beállítások

port security

Megtanulja a switch a porthoz rendelt MAC címeket, és ha ez túllépi a maximumot, akkor a protect, restrict vagy shutdown általi eljárást alkalmazza.

Meg lehet konkrétan adni egy MAC címet, vagy megtaníttatni sticky-vel.

Mode	Effect on Port	Notification / Logging	MAC Address Table
protect	Drops unauthorized traffic only	❌ No log or SNMP trap	✅ Keeps valid MACs
restrict	Drops unauthorized traffic	✅ Sends log/SNMP trap	✅ Keeps valid MACs
shutdown	Disables the port (error-disabled)	✅ Logs and SNMP trap	❌ Must be manually or auto-reenabled

```
int f0/1

    sw port-security

    sw port-security maximum [1]

    sw port-security violation [protect | restrict | shutdown]

    sw port-security mac-address [sticky | 1984.1984.1984]
```

exec timeout

Kiléptet `x` perc és `y` másodperc után.

```
line con 0

    exec-timeout [x] [y]
```

Távoli elérés

telnet switchen

```
hostname [S1]

ip domain-name [example.com]

ip default-gateway [192.168.0.1]

vlan [1]

    ip addr [192.168.0.2] [255.255.255.0]

    no shut

line vty 0 15

    password [passwd]

    login
```

SSH switchen

```
hostname [S3]

ena sec [passwd]

ip default-gateway [192.168.0.1]

ip domain-name [domain-name.hu]

crypto key generate rsa general-keys modulus [1024]

username [admin] secret [#Aa12345]

vlan [1]

    ip addr [192.168.0.2] [255.255.255.0]

    no shut

line vty 0 15
```

```
    login local

    transport input ssh
```

Gépen:

```
ssh -l [admin] [192.168.0.2]
```

plaintext jelszavak titkosítása

```
service password-encryption
```

Egyebek

Idő és NTP szerver beállítása

```
!! csak ha jelszavas

ntp authenticate

ntp authentication-key 1 md5 [#Aa12345]

ntp trusted-key 1

!! csak ha jelszavas

ntp server [192.168.1.100] key 1 ! key 1 csak ha jelszavas

clock timezone [UTC] [+2]
```

RADIUS

```
aaa new-model



radius server [RAD]

    address ipv4 [10.0.30.253] auth-port [1812] acct-port [1813] !
RADIUS szerver IP címe és portjai (auth authentication; acct accounting)

    key [#Aa12345]



aaa authentication login [SSH] group radius local ! belépést kezelje
RADIUS

aaa authentication enable [SSH] group radius local ! enable-t is



username [admin] secret [#Aa12345] ! fallback bejelentkezési adat



line vty 0 15

    login authentication [SSH]

    transport input ssh ! teljes SSH konfig kell akkor már
```

QoS voice VLAN

```
vlan [10]

    name [DATA]

vlan [20]

    name [VOICE]
```

```
mls qos



int [f0/1]

    sw mode access

    sw access vlan [10]

    mls qos trust cos

    sw voice vlan [20]
```

“factory reset”

```
erase startup-config

delete vlan.dat
```

GRE tunnel

Mindkét eszközön:

```
interface Tunnel0

    ip address [10.10.10.1] [255.255.255.0]  ! tunnel hálózata

    tunnel source [GigabitEthernet0/0]       ! másik R fele lévő
interfész

    tunnel destination [198.51.100.2]        ! másik R IP-je
```

```
ip route [192.168.2.0] [255.255.255.0] [10.10.10.2] ! 10.10.10.2 a másik
R IP-je, akkor ez a 192.168.2.0/24-et a tunnelen keresztül routeolja
```

TCP/UDP portok

🔐 Remote Access

Port	Protocol	Description
22	TCP	SSH (Secure Shell)
23	TCP	Telnet
3389	TCP	RDP (Remote Desktop)

🌐 Web and Email Services

Port	Protocol	Description
25	TCP	SMTP (Send Mail)
80	TCP	HTTP (Web Browsing)
110	TCP	POP3 (Retrieve Email)
143	TCP	IMAP (Retrieve Email)
443	TCP	HTTPS (Secure Web)
993	TCP	IMAPS (Secure IMAP)
995	TCP	POP3S (Secure POP3)

📡 Name Resolution & Time

Port	Protocol	Description
53	TCP/UDP	DNS
123	UDP	NTP (Network Time Protocol)

🖧 Networking Services

Port	Protocol	Description
67	UDP	DHCP (Server to Client)
68	UDP	DHCP (Client to Server)
546	UDP	DHCPv6 Client
547	UDP	DHCPv6 Server
69	UDP	TFTP (Used in VoIP)
161	UDP	SNMP (Monitoring)
162	UDP	SNMP Trap
514	UDP	Syslog

🎧 Voice, Video, and Media (VoIP & Streaming)

Port	Protocol	Description
5060	TCP/UDP	SIP (VoIP Signaling)
5061	TCP	SIP Secure (TLS)
2000	TCP	SCCP (Cisco VoIP Phones)
16384–32767	UDP	RTP (Voice Traffic)

🔐 Authentication & Security

Port	Protocol	Description
1812	UDP	RADIUS Authentication
1813	UDP	RADIUS Accounting
49	TCP	TACACS+
514	UDP	Syslog

🔁 File Transfer

Port	Protocol	Description
20	TCP	FTP (Data Transfer)

Port	Protocol	Description
21	TCP	FTP (Control/Login)
69	UDP	TFTP
989	TCP	FTPS (Data)
990	TCP	FTPS (Control)