CISCO C1121-4P MANAGED ROUTER CONFIG. EXPLAINATION

```
hostname MUMB-HOME-01
!
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service unsupported-transceiver
no platform punt-keepalive disable-kernel-core
!
enable secret 5 $1$TpEX$TbJz5Vkqj4hPy9i32kJWD0  ! Replace with your encrypted secret
!
username admin privilege 15 secret 5 @dm!N Replace with your own
!
ip domain name <Name>.local
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
!
ip routing
!
interface GigabitEthernet0/0/0
 description Uplink to ISP1
 ip address dhcp
 no shutdown
!
interface GigabitEthernet0/0/1
 description Uplink to ISP2 (Backup/Load Balance)
 ip address dhcp
 no shutdown
!
interface GigabitEthernet0/1/0
 description Downlink - VLAN 10 (Work Devices)
 switchport mode access
 switchport access vlan 10
 no shutdown
!
interface GigabitEthernet0/1/1
 description Downlink - VLAN 20 (Smart TV & IoT)
 switchport mode access
 switchport access vlan 20
 no shutdown
!
interface GigabitEthernet0/1/2
 description Downlink - VLAN 30 (IP CCTV)
 switchport mode access
 switchport access vlan 30
 no shutdown
!
interface GigabitEthernet0/1/3
```

```
 description Downlink - VLAN 40 (Guest Network)
 switchport mode access
 switchport access vlan 40
 no shutdown
!
vlan 10
 name Work-PC
!
vlan 20
 name IoT-SmartTV
!
vlan 30
 name CCTV-Cams
!
vlan 40
 name Guest-WiFi
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8 1.1.1.1
!
ip dhcp pool VLAN20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 1.1.1.1
!
ip dhcp pool VLAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.4.4
!
ip dhcp pool VLAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 1.0.0.1
!
line con 0
 login local
!
line vty 0 4
 login local
 transport input ssh
!
banner login ^C
*** Authorized Access Only ***
This is a configured Cisco ISR. Unauthorized access is prohibited and monitored.
^C
!
snmp-server community public RO
snmp-server location "Edge Router"
!
end
```

1. System Identity and Essential Services

```
hostname MUMB-HOME-01
```

- Sets the device's hostname for CLI identification and logging.

```
service tcp-keepalives-in
Service tcp-keepalives-out
```

- Ensures TCP session health checks — important for Telnet/SSH management sessions.

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
```

- Adds date/time with milliseconds to debug and log outputs — critical for real-time troubleshooting and audit trails.

```
service password-encryption
```

- Obscures plaintext passwords in the config (Type 7). Basic security hygiene.

```
service sequence-numbers
```

- Adds sequence numbers to syslog messages. Helps with log correlation.

```
service unsupported-transceiver
```

- Allows third-party SFPs (non-optics) — commonly used for cost savings.

```
no platform punt-keepalive disable-kernel-core
```

- Enables kernel crash dumps. Helpful for TAC diagnostics.

2. Secure Access Configuration

```
enable secret 5 $1$TpEX$TbJz5Vkqj4hPy9i32kJWD0
```

- Type 5 encrypted password for privileged EXEC mode (used with enable command).

```
username admin privilege 15 secret 5 @dm!N
```

- Creates a local user admin with full rights (privilege 15) and secure password. (Though technically, this @dm!N isn't Type 5 yet — you'd want to encrypt this).

🔒 Note: You should hash the password or use CLI to convert to a Type 5 secret.

```
ip domain name <Name>.local
crypto key generate rsa modulus 2048
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 3
```

- These lines:
  - Define local domain (needed for SSH keys)
  - Generate a 2048-bit RSA key pair
  - Enforce SSHv2 (recommended)
  - Secure session timeouts and login attempts

3. WAN (Uplink) Interfaces

```
interface GigabitEthernet0/0/0
 description Uplink to ISP1
 ip address dhcp
 no shutdown
```

- WAN Port 1 for **primary ISP**, gets IP via DHCP.

```
interface GigabitEthernet0/0/1
 description Uplink to ISP2 (Backup/Load Balance)
 ip address dhcp
 no shutdown
```

- WAN Port 2 for secondary ISP (load balancing or failover setup).

4. LAN (Customer-Facing) Ports – VLAN Segmented

Each LAN port is mapped to a VLAN for isolated traffic:

```
interface GigabitEthernet0/1/0
 description Downlink - VLAN 10 (Work Devices)
 switchport mode access
 switchport access vlan 10
 no shutdown

interface GigabitEthernet0/1/1
 description Downlink - VLAN 20 (Smart TV & IoT)
 switchport mode access
 switchport access vlan 20
 no shutdown

interface GigabitEthernet0/1/2
 description Downlink - VLAN 30 (IP CCTV)
 switchport mode access
 switchport access vlan 30
 no shutdown

interface GigabitEthernet0/1/3
 description Downlink - VLAN 40 (Guest Network)
 switchport mode access
 switchport access vlan 40
 no shutdown
```

5. VLAN Declarations

```
vlan 10
 name Work-PC
...
vlan 40
```

- Logical VLAN IDs with descriptive labels — standard practice for scalability.

6. DHCP Configuration per VLAN

Each VLAN has its own DHCP pool and subnet:

```
ip dhcp excluded-address 192.168.10.1 192.168.10.10
```

- Reserves addresses for static/manual assignments (e.g., NAS, servers).

```
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8 1.1.1.1
 name Guest-WiFi
```

- DHCP config for VLAN10. Each VLAN follows a similar pattern (VLAN20 to VLAN40), with unique networks and DNS choices.

7. Access Lines Configuration

```
line con 0
 login local
```

- Local user login enabled on the console port.

```
line vty 0 4
 login local
 transport input ssh
```

- Local user login via SSH only on virtual terminal (VTY) lines.

| Telnet is disabled (best practice). SSH is enforced for encrypted access.

8. Banner Message

```
!
banner login ^C
*** Authorized Access Only ***
This is a configured ISR. Unauthorized access is prohibited and monitored.
^C
!
```

- Standard legal/notice banner for security compliance and deterrence.

9. SNMP for Monitoring

```
snmp-server community public RO
snmp-server location "Edge Router"
```

- Basic SNMP v2 config for read-only access.

| For production, use SNMPv3 with authentication & encryption.

✓ Summary of Key Capabilities

Feature Area	Configuration Summary
WAN Redundancy	Dual ISP on DHCP uplink ports
LAN Segmentation	VLANs 10–40 for PC, IoT, CCTV, Guests
Security	SSH login, encrypted passwords, login banners
User Access	Local admin user with full privilege
DHCP per VLAN	Unique scopes and DNS servers
SNMP	Monitoring enabled (read-only)
Scalability	Modular, VLAN-aware design; supports more ports/devices

****