Configure Win 10 VPN, via internet, to/from my router only.

https://www.bing.com/copilotsearch?q=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&FORM=CSSCOP

**You can set up your router as a VPN server with IPsec or PPTP, enable port forwarding, and configure Windows 10’s built-in VPN client to securely connect via the internet directly to your router’s VPN service.**

**Step 1: Configure Your Router as a VPN Server**

* 1. **Access your router’s admin interface:**
	Connect to your router’s LAN IP (e.g., http://192.168.1.1 or http://www.asusrouter.com) via a web browser.
	2. **Enable VPN server features:**
		+ Find the VPN server settings in the advanced settings menu, often under **VPN**, **VPN Server**, or **Remote Access**.
		+ Enable an appropriate VPN protocol your router supports (commonly **IPsec with L2TP** or **PPTP**). For security, IPsec is preferred over PPTP.
		+ Configure VPN authentication by creating a username and password for VPN clients.
		+ Set up a pre-shared key (for IPsec) if required.
	3. **Specify remote IP address pool:**
	Your router will assign VPN clients IP addresses. Define a range that does not overlap with your LAN subnet.
	4. **Configure WAN access:**
	Ensure your router has a **public IP address** or set up **Dynamic DNS (DDNS)** if your ISP assigns dynamic IPs, so you can reach your router from the internet.
	5. **Enable port forwarding or VPN passthrough:**
		+ For PPTP, forward TCP port 1723 and allow GRE protocol (protocol 47).
		+ For L2TP/IPsec, open UDP ports 500, 1701, and 4500.
		Many routers have dedicated VPN passthrough settings; ensure they are enabled.
	6. **Apply and save settings; reboot the router if necessary.**

**Step 2: Configure Windows 10 VPN Client to Connect to the Router**

* 1. **Open VPN settings:**
	Go to **Settings > Network & Internet > VPN** and click **+ Add a VPN connection**.
	2. **Fill in the VPN details:**
		+ **VPN provider:** Select **Windows (built-in)**
		+ **Connection name:** Give it a recognizable name (e.g., "Home Router VPN")
		+ **Server name or address:** Enter your router's public IP or DDNS hostname
		+ **VPN type:** Choose according to your router’s configuration:
			- For IPsec/L2TP, select **L2TP/IPsec with pre-shared key**
			- For PPTP, select **Point to Point Tunneling Protocol (PPTP)**
		+ **Type of sign-in info:** Select **Username and password**
		+ Enter the username and password you configured on the router for VPN access.
	3. **Save the connection.**
	4. **Connect to the VPN:**
	From the VPN settings window or the network icon in the system tray, select your VPN connection and click **Connect**. Enter credentials if requested.

**Step 3: Optional - Restrict Traffic to VPN Only (Kill Switch)**

To ensure all internet traffic goes through the VPN tunnel and no traffic leaks outside it:

* 1. Use firewall rules or Windows advanced settings to **block traffic outside the VPN interface**, allowing only the VPN interface for internet access.
	2. Alternatively, modify routing tables after connection (e.g., remove the default gateway route for the normal network adapter), so traffic only routes through the VPN.
	3. Some VPN clients support a **kill switch** feature that disables network traffic if the VPN disconnects.

**Additional Tips and Notes**

* 1. **Static local IP:** Assign your PC a static local IP in your LAN to avoid issues with routes if your IP changes.
	2. **Firmware:** Update your router firmware to the latest version to ensure VPN support and security.
	3. **Testing:** Always test the VPN connection from an external network (e.g., mobile hotspot or friend's internet) to verify it works from the internet.
	4. **Security:** Use IPsec rather than PPTP if possible, as PPTP is outdated and less secure.
	5. **Router compatibility:** Configuration steps vary between router brands and models; consult your router’s documentation for VPN setup details.

By following these steps, **you will configure your router as a VPN server accessible over the internet and connect to it from Windows 10 using the built-in VPN client, ensuring your PC communicates securely through your router’s VPN only**.

[ASUS](https://www.bing.com/ck/a?!&&p=fdfe03a701ad9c0f23cc50a3bfe1e4f4c8d6e53937ccdd6863f0f0de3710cd16JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly93d3cuYXN1cy5jb20vc3VwcG9ydC9mYXEvMTA0NDM5Ny8&ntb=1" \t "_blank)**[+4](https://www.bing.com/ck/a?!&&p=fdfe03a701ad9c0f23cc50a3bfe1e4f4c8d6e53937ccdd6863f0f0de3710cd16JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly93d3cuYXN1cy5jb20vc3VwcG9ydC9mYXEvMTA0NDM5Ny8&ntb=1" \t "_blank)**

**[Configuring Windows to only allow traffic through VPN](https://www.bing.com/ck/a?!&&p=ea9878b33b691b9a313237587a4e4ed505b28d6513bcb1ab7f1bdce2808e2ff3JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly9zdXBlcnVzZXIuY29tL3F1ZXN0aW9ucy8xNTkwNTIxL2NvbmZpZ3VyaW5nLXdpbmRvd3MtdG8tb25seS1hbGxvdy10cmFmZmljLXRocm91Z2gtdnBu&ntb=1" \t "_blank)**

[](https://www.bing.com/ck/a?!&&p=ea9878b33b691b9a313237587a4e4ed505b28d6513bcb1ab7f1bdce2808e2ff3JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly9zdXBlcnVzZXIuY29tL3F1ZXN0aW9ucy8xNTkwNTIxL2NvbmZpZ3VyaW5nLXdpbmRvd3MtdG8tb25seS1hbGxvdy10cmFmZmljLXRocm91Z2gtdnBu&ntb=1" \t "_blank)

[https://superuser.com › questions › configuring-windows-to-only-allow-traffic-through-vpn](https://www.bing.com/ck/a?!&&p=ea9878b33b691b9a313237587a4e4ed505b28d6513bcb1ab7f1bdce2808e2ff3JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly9zdXBlcnVzZXIuY29tL3F1ZXN0aW9ucy8xNTkwNTIxL2NvbmZpZ3VyaW5nLXdpbmRvd3MtdG8tb25seS1hbGxvdy10cmFmZmljLXRocm91Z2gtdnBu&ntb=1" \t "_blank)

**[[VPN] How to set up IPsec VPN connection in Windows 10 (Firmware ... - ASUS](https://www.bing.com/ck/a?!&&p=fdfe03a701ad9c0f23cc50a3bfe1e4f4c8d6e53937ccdd6863f0f0de3710cd16JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly93d3cuYXN1cy5jb20vc3VwcG9ydC9mYXEvMTA0NDM5Ny8&ntb=1" \t "_blank)**

[](https://www.bing.com/ck/a?!&&p=fdfe03a701ad9c0f23cc50a3bfe1e4f4c8d6e53937ccdd6863f0f0de3710cd16JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly93d3cuYXN1cy5jb20vc3VwcG9ydC9mYXEvMTA0NDM5Ny8&ntb=1" \t "_blank)

[https://www.asus.com › support › faq](https://www.bing.com/ck/a?!&&p=fdfe03a701ad9c0f23cc50a3bfe1e4f4c8d6e53937ccdd6863f0f0de3710cd16JmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly93d3cuYXN1cy5jb20vc3VwcG9ydC9mYXEvMTA0NDM5Ny8&ntb=1" \t "_blank)

**[Connect to a VPN in Windows - Microsoft Support](https://www.bing.com/ck/a?!&&p=cf8c973f272db20f44c242c43d2aaf7be4c5240858e8cbbb3a13ecad3fefeefaJmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly9zdXBwb3J0Lm1pY3Jvc29mdC5jb20vZW4tdXMvd2luZG93cy9jb25uZWN0LXRvLWEtdnBuLWluLXdpbmRvd3MtM2QyOWFlYjEtZjQ5Ny1mNmI3LTc2MzMtMTE1NzIyYzEwMDlj&ntb=1" \t "_blank)**

[](https://www.bing.com/ck/a?!&&p=cf8c973f272db20f44c242c43d2aaf7be4c5240858e8cbbb3a13ecad3fefeefaJmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly9zdXBwb3J0Lm1pY3Jvc29mdC5jb20vZW4tdXMvd2luZG93cy9jb25uZWN0LXRvLWEtdnBuLWluLXdpbmRvd3MtM2QyOWFlYjEtZjQ5Ny1mNmI3LTc2MzMtMTE1NzIyYzEwMDlj&ntb=1" \t "_blank)

[https://support.microsoft.com › en-us › windows](https://www.bing.com/ck/a?!&&p=cf8c973f272db20f44c242c43d2aaf7be4c5240858e8cbbb3a13ecad3fefeefaJmltdHM9MTc0OTA4MTYwMA&ptn=3&ver=2&hsh=4&fclid=11a7bf5b-4b86-6674-382c-aa9e4aae6741&psq=configure+Win+10+VPN%2c+via+internet%2c++to%2ffrom+my+router+only&u=a1aHR0cHM6Ly9zdXBwb3J0Lm1pY3Jvc29mdC5jb20vZW4tdXMvd2luZG93cy9jb25uZWN0LXRvLWEtdnBuLWluLXdpbmRvd3MtM2QyOWFlYjEtZjQ5Ny1mNmI3LTc2MzMtMTE1NzIyYzEwMDlj&ntb=1" \t "_blank)





**Visa alla**

**[configure Win 10 VPN, via internet, to/from my router only](https://www.bing.com/search?q=configure%20Win%2010%20VPN%2C%20via%20internet%2C%20to%2Ffrom%20my%20router%20only" \t "_blank)**

**[Microsoft Bing-sökning](https://www.bing.com/search?q=configure%20Win%2010%20VPN%2C%20via%20internet%2C%20to%2Ffrom%20my%20router%20only" \t "_blank)**

**Källor**

[**Super User**](https://superuser.com/questions/1590521/configuring-windows-to-only-allow-traffic-through-vpn)**https://superuser.com › questions › configuring-windows-to-only-allow-traffic-through-vpn**

**Configuring Windows to only allow traffic through VPN**

**I would like to configure Windows 10 to only allow traffic through a VPN connection. For example, Firefox won't have internet access if the VPN is not connected. I want to be able …**

[**Microsoft**](https://support.microsoft.com/en-us/windows/connect-to-a-vpn-in-windows-3d29aeb1-f497-f6b7-7633-115722c1009c)**https://support.microsoft.com › en-us › windows**

**Connect to a VPN in Windows - Microsoft Support**

**Select the Start button, then select Settings > Network & Internet > VPN > Add a VPN connection. In Add a VPN connection, do the following: For VPN provider, choose Windows (built-…**

[**windows101tricks.com**](https://windows101tricks.com/configure-vpn-on-windows-10/)**https://windows101tricks.com**

**How to Setup a VPN (Virtual Private Network) on Windows 10**

**Configure The Router for Incoming VPN. Router Configuration: Enable PPTP and Generic Route Encapsulation (GRE) on the Router. Depending on the type of router, you need to either en…**

[**DrayTek**](https://www.draytek.com/support/knowledge-base/5390)**https://www.draytek.com › support › knowledge-base**

**L2TP over IPsec from Windows 10 to Vigor Router - DrayTek**

**This document introduces how to set up Vigor Router as a VPN server for L2TP over IPsec, as well as how to use Windows 10 built-in VPN feature to establish a VPN to Vigor Router an…**

[**ASUS**](https://www.asus.com/support/faq/1044397/)**https://www.asus.com › support › faq**

**[VPN] How to set up IPsec VPN connection in Windows 10 (Firmware ... - ASUS**

**1. Connect your computer to the router via wired or WiFi connection and enter your router LAN IP or router URL http://www.asusrouter.com to the WEB GUI. For more details, please re…**

**Alla länkar**

[**Super User**](https://superuser.com/questions/1590521/configuring-windows-to-only-allow-traffic-through-vpn)**superuser.com › questions › 1590521 › configuring-windows-to-only-allow-traffic-through-vpn**

**Configuring Windows to only allow traffic through VPN**

**I would like to configure Windows 10 to only allow traffic through a VPN connection. For example, Firefox won't have internet access if the VPN is not connected. I want to be able to turn this setting off.**

[**How-To Geek**](https://www.howtogeek.com/835185/how-to-set-up-your-windows-pc-as-a-vpn-router/)**www.howtogeek.com › 835185 › how-to-set-up-your-windows-pc-as-a-vpn-router**

**How to Set Up Your Windows PC as a VPN Router - How-To Geek**

**To set up a virtual router wirelessly on Windows 10 and Windows 11, your device needs to be able to broadcast Wi-Fi, not just receive it. Almost all modern laptops can do this, but this is less the case for desktop PCs. To check, you need to open the Windows command prompt by typing "cmd" in the search bar. Then, type the following:**

[**ASUS**](https://www.asus.com/support/faq/1044397/)**www.asus.com › support › faq › 1044397**

**[VPN] How to set up IPsec VPN connection in Windows 10 (Firmware ... - ASUS**

**1. Connect your computer to the router via wired or WiFi connection and enter your router LAN IP or router URL http://www.asusrouter.com to the WEB GUI. For more details, please refer to How to enter the router setting page(Web GUI) 2. Click [VPN] from the left Advanced Settings > [VPN Server] page. 3. Turn on IPsec VPN Server**

[**TheWindowsClub**](https://www.thewindowsclub.com/configure-vpn-connection-windows)**www.thewindowsclub.com › configure-vpn-connection-windows**

**How to configure VPN connection in Windows 11/10 - The Windows Club**

**This screenshot tutorial will show you how to set up and configure VPN Connection so that your Windows 11/10 computer will accept VPN connections.**

[**Microsoft**](https://support.microsoft.com/en-us/windows/connect-to-a-vpn-in-windows-3d29aeb1-f497-f6b7-7633-115722c1009c)**support.microsoft.com › en-us › windows › connect-to-a-vpn-in-windows-3d29aeb1-f497-f6b7-7633-115722c1009c**

**Connect to a VPN in Windows - Microsoft Support**

**Select the Start button, then select Settings > Network & Internet > VPN > Add a VPN connection. In Add a VPN connection, do the following: For VPN provider, choose Windows (built-in). In the Connection name box, enter a name you'll recognize (for example, My Personal VPN).**

[**Infosec Institute**](https://www.infosecinstitute.com/resources/operating-system-security/how-to-configure-vpn-in-windows-10/)**www.infosecinstitute.com › resources › operating-system-security › how-to-configure-vpn-in-windows-10**

**How to configure VPN in Windows 10 | Infosec - Infosec Institute**

**This article has defined the three basic connection types of VPN and illustrated how to configure a VPN server on a Mikrotik router. We also provided a guide on how to set up a VPN session using the built-in Windows 10 tool.**

[**DrayTek**](https://www.draytek.com/support/knowledge-base/5390)**www.draytek.com › support › knowledge-base › 5390**

**L2TP over IPsec from Windows 10 to Vigor Router - DrayTek**

**This document introduces how to set up Vigor Router as a VPN server for L2TP over IPsec, as well as how to use Windows 10 built-in VPN feature to establish a VPN to Vigor Router and access the Vigor Router's LAN network.**

[**Digital Citizen**](https://www.digitalcitizen.life/how-create-configure-and-use-vpn-connection-windows-10/)**www.digitalcitizen.life › how-create-configure-and-use-vpn-connection-windows-10**

**How to add and use a VPN in Windows 10 (all you need to know)**

**How to manually add a VPN connection in Windows 10. How to add a VPN, configure a VPN, connect to a VPN, and disconnect from it.**

[**windows101tricks.com**](https://windows101tricks.com/configure-vpn-on-windows-10/)**windows101tricks.com › configure-vpn-on-windows-10**

**How to Setup a VPN (Virtual Private Network) on Windows 10**

**Configure The Router for Incoming VPN. Router Configuration: Enable PPTP and Generic Route Encapsulation (GRE) on the Router. Depending on the type of router, you need to either enable PPTP or create a port forward to port 1723. If your router has an additional setting for PPTP or VPN, make sure it’s enabled.**

[**Windows Central**](https://www.windowscentral.com/how-manually-configure-vpn-windows-10)**www.windowscentral.com › how-manually-configure-vpn-windows-10**

**How to manually configure a VPN on Windows 10**

**If you have a VPN subscription and would like to set things up manually, the process should take only a few minutes. Here's what you need to know to get everything working properly.**

[**WindowsLoop**](https://windowsloop.com/using-windows-vpn-options/)**windowsloop.com › using-windows-vpn-options**

**How To Set Up VPN with Built-in VPN Client on Windows 10**

**Here’s how to set up the built-in VPN on Windows: Press the “ Start ” key. Search and open “ VPN Settings.” Click the “ Add VPN ” button. Select “ Windows (built-in) ” from the VPN provider dropdown. Type a name in the “ Connection name ” field. Type the IP address or domain address in the “ Server name or address ” field.**

[**Windows Report**](https://windowsreport.com/vpn-remote-desktop-windows-10/)**windowsreport.com › vpn-remote-desktop-windows-10**

**How to Use VPN for Remote Desktop on Windows [Step-by-Step]**

**A complete guide on how to set up a VPN with Remote Desktop on Windows 10, from enabling Remote Desktop to connecting to the remote PC.**

[**ExpressVPN**](https://www.expressvpn.com/blog/how-to-install-vpn-on-router/)**www.expressvpn.com › blog › how-to-install-vpn-on-router**

**How to set up a VPN on your router - ExpressVPN**

**2. Enable bridge mode on your Xfinity router. This will allow your router to act as a modem only, and pass all traffic through to your VPN-enabled router. 3. Connect your VPN-enabled router to your Xfinity router using an Ethernet cable. 4. Configure your VPN on your router. This will vary depending on the VPN provider and router model.**

[**BleepingComputer**](https://www.bleepingcomputer.com/vpn/guides/how-to-setup-a-vpn-on-your-router/)**www.bleepingcomputer.com › vpn › guides › how-to-setup-a-vpn-on-your-router**

**How to setup a VPN on your router: Detailed walkthrough - BleepingComputer**

**Learn how to set up a VPN on your router and ensure all of your devices are protected. Follow our easy step-by-step guide to get started.**

[**Private Internet Access**](https://www.privateinternetaccess.com/blog/set-up-windows-vpn/)**www.privateinternetaccess.com › blog › set-up-windows-vpn**

**How to Install a VPN on Windows 10 & 11 - Private Internet Access**

**Learn how to set up a VPN on Windows 11 or 10 using manual setup or an app. See if you need a VPN on your PC.**

[**Reddit**](https://www.reddit.com/r/mikrotik/comments/sxs34g/how_to_access_mikrotik_router_over_vpn/)**www.reddit.com › r › mikrotik › comments › sxs34g › how\_to\_access\_mikrotik\_router\_over\_vpn**

**How to access Mikrotik router over VPN? : r/mikrotik - Reddit**

**Now I am able to connect to my home network from the internet no problem. However, I can only ping the router, but I cannot access any services that run on the router: Can't resolve internal domain names via the router's built-in DNS server. Can't use Winbox to change router settings.**

[**NETGEAR**](https://kb.netgear.com/23854/How-do-I-enable-the-VPN-feature-on-my-NETGEAR-router-using-a-Windows-computer)**kb.netgear.com › 23854 › How-do-I-enable-the-VPN-feature-on-my-NETGEAR-router-using-a-Windows-computer**

**How do I enable the VPN feature on my NETGEAR router using a Windows ...**

**Currently, only OpenVPN version 2.7.1 or earlier work with NETGEAR routers. To enable the VPN feature: Launch a web browser from a computer or mobile device that is connected to your router’s local network. Visit www.routerlogin.net A login window displays. Enter your router’s username and password. The default username is admin.**

https://copilot.microsoft.com/chats/WHEz4BUjetCJfWnymkueR

I dag

**Du sa**

configure Win 10 VPN, via internet, to/from my router only

**Copilot sa**

Below is a detailed walkthrough that covers two common approaches. In one scenario you use your router’s built‑in VPN server so that when you connect from Windows 10 via the internet your VPN session terminates at the router (letting you access your home or LAN devices, including router administration). In the other scenario you configure Windows 10 as a VPN server—but then you tailor it so that only your router or its local network is accessible. Both methods require that you set up your home network and firewall/NAT rules appropriately.

**Scenario 1: Using Your Router’s VPN Server**

If your router supports VPN server functionality (many modern routers offer PPTP, L2TP/IPsec, or even OpenVPN), you can have the VPN session end at the router. This means remote clients (like your Windows 10 laptop) connect over the internet directly to your router. Typically you then can access your local network devices (and optionally, only management traffic if you wish).

**Step 1. Configure Your Router**

1. **Enable the VPN Server:**
	* Log into your router’s administrative console (for example, via an IP such as 192.168.1.1).
	* Find the VPN section. Enable the VPN server feature and choose a protocol—L2TP/IPsec is a common and secure choice.
	* Enter a pre‑shared key (if required) and set up one or more user accounts with credentials.
2. **Set the VPN IP Pool:**
	* Configure a range of IP addresses that the router will assign to VPN clients. This range should be on the same subnet as your local network (or routed appropriately) if you want seamless access.
3. **Port Forwarding / Firewall Settings:**
	* If your router is behind another NAT or if your ISP also provides a NAT device, ensure that the needed ports are open. For L2TP/IPsec, forward:
		+ UDP 500
		+ UDP 4500
		+ (and possibly ESP protocol)
	* Make sure the router’s firewall permits the VPN connections.
4. **Dynamic DNS Consideration:**
	* If your public IP address is dynamic, configure DDNS in the router so you can reliably access it via a domain name.

*This step is similar to the instructions referenced in guides such as the one by DrayTek on setting up an L2TP VPN with a router*1*.*

**Step 2. Configure the Windows 10 VPN Client**

1. **Open VPN Settings:**
	* Go to **Settings → Network & Internet → VPN**.
	* Click **Add a VPN connection**.
2. **Enter Connection Details:**
	* **VPN Provider:** Choose “Windows (built-in).”
	* **Connection Name:** Give it a descriptive name (e.g., “Home Router VPN”).
	* **Server Name or Address:** Enter your router’s public IP address or DDNS domain.
	* **VPN Type:** Select the type that matches your router’s configuration (e.g., “L2TP/IPsec with pre-shared key”).
	* **Pre-shared Key:** Enter the key you configured on your router.
	* **Sign-in Information:** Choose **Username and password** and fill in the credentials you set up.
3. **(Optional) Enable Split Tunneling:**
	* If you want only local (home network) traffic to be routed through the VPN rather than all internet traffic, tweak the connection properties:
		+ Open the **Control Panel → Network and Sharing Center → Change adapter settings**.
		+ Right-click the VPN connection → **Properties**.
		+ Under the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties → Advanced**.
		+ Uncheck **Use default gateway on remote network**. This ensures that only traffic destined for your home network (for example, the router or local devices) is sent via the VPN.
4. **Test the Connection:**
	* Connect to the VPN from Windows 10.
	* Check connectivity by trying to access your router’s admin page or by pinging a local IP address.
	* Use command-line tools like ipconfig to see the assigned IP from the VPN pool.

*This outlines a typical setup for having your Windows 10 client connect to a router’s VPN server and limiting the scope to your home network (router only or LAN only)*1*.*

**Scenario 2: Using Windows 10’s Built‑in VPN Server (Restricted to Local Router/LAN Access)**

An alternative is to set up Windows 10 itself as a VPN server. This approach is rarely used in place of a router-based solution, but if you decide to host the VPN service on a Windows 10 machine, you can restrict the network so that once connected the remote user can only access your PC and (if properly routed) your router’s local management interface.

**Step 1. Set Up an Incoming VPN Connection on Windows 10**

1. **Access the Incoming Connection Setup:**
	* Open the **Control Panel → Network and Sharing Center**.
	* Click on **Change adapter settings**.
	* Press **Alt** to bring up the menu bar. Choose **File → New Incoming Connection**.
2. **Select Users and Configure Access:**
	* Pick the user accounts that will have VPN access.
	* Select **through the Internet** when prompted for connection type.
3. **Configure IP Address Assignment:**
	* In the next steps, you can specify which IP address pool is used for VPN clients. To limit access (for instance, to allow only certain accesses such as the route to the router), set the IP range so that it’s on the same subnet or carefully manage routing policies.
4. **Firewall and NAT Considerations:**
	* Forward port 1723 (for PPTP, if you choose that protocol) on your network’s router to your Windows 10 PC.
	* Make sure that Windows Firewall isn’t blocking the VPN service.

*This method is discussed by various guides on setting up a VPN server on Windows 10 (for example, see PureInfotech’s guide)*2*.*

**Step 2. Restricting VPN Traffic to “Router Only”**

Since a Windows 10 incoming connection normally gives you access to the PC’s network interfaces, you may want to ensure that once a VPN client connects, the routes added do not send all traffic through the remote computer. For restricting access:

* **Adjust Routing:** Manually edit the routing table of the Windows 10 VPN server so that only certain subnets (e.g., the router’s IP or the local LAN you want to expose) are advertised to the client.
* **Firewall Rules:** Use Windows Firewall or a third‑party firewall to block unwanted traffic from the VPN interface. Only allow traffic aimed at your router’s local IP address (or a defined range).

This method tends to be more complex and requires careful configuration with routing and firewall policies.

**Choosing the Best Approach**

For many users, having the router manage VPN connections is both more secure and more convenient than having a full‑time Windows VPN server. Dedicated router hardware is designed to keep the VPN session stable and makes firewall/NAT traversal simpler because it’s installed at the edge of your network. If your only goal is to remotely access your router (or devices on its LAN) via the internet—and not necessarily to route all your internet traffic through VPN—using your router’s VPN server with split tunneling (unchecking “Use default gateway on remote network”) on your Windows client is often the simplest, most secure method.

**Next Steps and Additional Considerations**

* **Firmware Updates & Security:** Ensure that both your router and Windows 10 are fully updated to protect against vulnerabilities.
* **Testing:** Always test from an external network (using mobile data or a different Wi-Fi) to confirm that the VPN connection works as intended.
* **Documentation:** Check your router’s manual or support resources, as the specifics of enabling and configuring the VPN server vary.
* **Advanced Routing:** If you are comfortable with command line and network administration, consider fine-tuning your routing tables (using the route command) to further restrict VPN traffic.

By following these steps, you’ll have a secure VPN connection that connects directly to your router over the internet, whether you’re using your router’s VPN functionality directly or leveraging Windows 10’s built‑in services with extra routing control.

Would you like further details on configuring advanced security settings (such as IPSec parameter adjustments) or on troubleshooting common connectivity issues?

[1www.draytek.com](https://www.draytek.com/support/knowledge-base/5390)[2pureinfotech.com](https://pureinfotech.com/setup-vpn-server-windows-10/)

Redigera det här svaret

Quiz my understanding of VPN setup processWhat are common issues when setting up a VPN?How do different VPN protocols compare?



Think Deeper

Logga in



OpenVPN or other protocols like IKEv2

Avoid using Panda VPN apps simultaneously on devices connected to the router VPN, as this can cause conflicts.

https://www.bing.com/copilotsearch?q=panda+VPN+configuration+to+my+router+only&FORM=CSSCOP

Copilot Search

Copilot Search delivers AI-powered insights, helping you explore topics, uncover relevant instant answers, and connect ideas seamlessly.

www.bing.com



https://copilot.microsoft.com/chats/Bz2dCAzVbFYPtSA2Z7msT

I dag

Du sa

server = router?

Copilot sa

The functions of a server and a router are quite distinct, even though in some setups a single device might provide both roles.

Server: A server is a computer or software system designed to manage, host, and deliver various services—such as websites, databases, or file storage—to client devices over a network. Its roles revolve around processing data, managing resources, and responding to requests from other devices.

Router: In contrast, a router is dedicated to directing data packets between different networks. It manages network traffic, determines optimal data paths, and ensures that data is efficiently delivered from one network segment to another. Routers are optimized for packet handling and connection management rather than data processing.

That said, in some cases—particularly in smaller or home network configurations—a device can be set up to perform both functions. For example, a home router might include basic server capabilities like running a DHCP server, providing network address translation (NAT), or even hosting a small web interface for management. In larger or more critical network environments, though, combining these roles can lead to performance and security challenges, which is why dedicated devices are generally used for each function.

Could you share more about your scenario or what you’re aiming to achieve with the idea of equating a server with a router? This will help me pinpoint the best explanation or solution for your situation.

Redigera det här svaret

Can you explain the main differences between server and router?

How do servers and routers work together in a network?

Skicka meddelande till Copilot

Think Deeper

Logga in

L2TP allows the creation of a virtual private dialup network (VPDN)[5] to connect a remote client to its corporate network by using a shared infrastructure, which could be the Internet or a service provider's network.

https://en.wikipedia.org/wiki/Layer\_2\_Tunneling\_Protocol

Introduction

A virtual private dial-up network (VPDN) allows a private network dial in service to span across to remote access servers (defined as the L2TP Access Concentrator [LAC]).

When a Point-to-Point Protocol (PPP) client dials into a LAC, the LAC determines that it should forward that PPP session on to an L2TP Network Server (LNS) for that client. The LNS then authenticates the user and starts the PPP negotiation. Once PPP setup has completed, all frames are sent through the LAC to the client and the LNS.

<https://www.cisco.com/c/en/us/support/docs/dial-access/virtual-private-dialup-network-vpdn/20980-vpdn-20980.html>

**---**

**Router med pass through eller endpoint**

Om den anställdes dator är kopplad till en router måste routern ha stöd för VPN pass through för att VPN-tunneln ska kunna upprättas. Den funktionen har i princip alla routrar idag. Det som kan variera mellan olika routermodeller är hur många sådana tunnlar de kan släppa igenom samtidigt.



*Router med VPN pass through som släpper igenom VPN-tunneln.*

Routerfunktionen VPN pass through ska inte förväxlas med VPN endpoint. VPN pass through gör att routern kan släppa igenom VPN-tunnlar som slutar hos en dator. När en dator i det lokala nätverket upprättar en VPN-tunnel är det endast den datorn som blir ansluten till tunneln (och skickar sin trafik genom den). Routerfunktionen VPN endpoint är betydligt ovanligare bland konsumentroutrar. När den funktionen aktiveras blir själva routern slutpunkten i VPN-tunneln. Alla datorer som ansluter till den ­routern blir automatiskt också anslutna till VPN-tunneln och deras trafik skickas genom den. Det är en bra lösning i företagssammanhang där alla datorer i en filial ska vara anslutna till huvudnätverket. I stället för att en egen VPN-tunnel upprättas från varje ­enskild ­dator, kan datorernas gemensamma router integrera hela det lokala filialnätverket i huvud­nätverket.



*Routerfunktionen VPN endpoint gör så att alla klienter som ansluter till routern kopplas till VPN-servern.*

---

https://www.kjell.com/se/kunskap/hur-funkar-det/internet/lokala-natverk/vpn-tunnlar

https://copilot.microsoft.com/chats/CxCXijp4HNzYp4Ba6cCji

I dag

**Du sa**

how does a vpn functioning? From my computer via isp/internet and router to my camera?

**Copilot sa**

A VPN (Virtual Private Network) works by creating a secure and encrypted connection between your device (like your computer) and a VPN server. This tunnel protects your data from being intercepted as it travels across the internet.

Here’s how it functions in your scenario:

1. **Your Computer** initiates a connection to the VPN service.
2. **Encryption & Routing**: The VPN encrypts your data and routes it through a secure VPN server before sending it to its destination.
3. **ISP & Internet**: Your internet service provider (ISP) only sees encrypted traffic between your computer and the VPN server, but it can't see your actual data or final destination.
4. **Router & Camera**: If you’re trying to access your camera remotely, the VPN helps by masking your location and ensuring a secure connection between your computer and the network where the camera is located.

If your camera is behind a router in your local network, you may need to configure port forwarding or set up a VPN directly on your router for seamless access. Some cameras also support direct VPN connections for added security.

Would you like help choosing a VPN service or setting up a secure connection?

Redigera det här svaret

What are the security benefits of using a VPN?How can I set up a VPN on my router?Can you help me securely access my camera through a VPN?



Snabbt svar

Logga in



I dag

**Du sa**

how can I acces a camera from my computer via isp and router?

**Copilot sa**

Accessing a camera remotely through your ISP and router involves configuring your network to allow external connections. Here’s an overview of the steps:

1. **Find the Camera’s Local IP Address** – Check your router's client list or access your camera’s settings to find its local IP.
2. **Configure Port Forwarding** – Log into your router’s settings and create a rule to forward traffic from an external port to the camera’s IP and port.
3. **Get Your Public IP Address** – Visit a site like whatismyip.com to find your ISP-assigned public IP.
4. **Set Up Dynamic DNS (Optional)** – If your ISP changes your public IP periodically, use Dynamic DNS services to associate it with a domain.
5. **Enable Secure Authentication** – Make sure your camera requires a strong password to prevent unauthorized access.
6. **Test Remote Access** – Try connecting from an external network using your public IP and forwarded port.

⚠️ **Important Security Note:** Opening ports can expose your network to cyber risks. Consider using VPNs, encrypted connections, or cloud-based camera services instead.

Would you like guidance on a specific step?

Redigera det här svaret

Can you explain how to set up port forwarding?What are the benefits of using a VPN instead?What troubleshooting steps can I take if it doesn't work?



Snabbt svar

Logga in



I dag

**Du sa**

how can I acces a camera from my computer via isp and router? RTSP Port 554

**Copilot sa**

Accessing your computer’s camera from outside your local network using the RTSP protocol on port 554 involves configuring your router to forward incoming traffic to the camera’s private IP address. Here are detailed steps to help you set it up:

1. **Assign a Static IP:** Ensure the camera is configured with a static IP address on your local network. This prevents the camera’s IP from changing over time, which is crucial for reliable port forwarding. If your camera supports DHCP reservation, use that option in your router’s settings.
2. **Configure Port Forwarding on Your Router:** In your router’s administration interface, find the port forwarding (or virtual server) section. Here, create a rule that forwards an external port to the camera’s internal IP and port 554.
	* **Single Camera:** You can keep the external port as 554 if it isn’t already in use by another service.
	* **Multiple Cameras:** If you have more than one camera, note that you cannot forward the same external port to multiple internal addresses directly. Instead, assign different external ports (for example, 10001, 10002, etc.) and map each to the respective camera’s internal port 554. When accessing the camera remotely, you would then use your public IP address combined with the designated external port (e.g., rtsp://public-ip:10001/stream) 1.
3. **Protocol Considerations:** RTSP typically uses TCP for control and UDP for streaming data. While most port forwarding rules configure TCP traffic, some routers allow you to specify UDP as well or to forward both protocols. Check your router’s documentation to ensure that both control and data channels are appropriately forwarded. Some users have also resolved issues by configuring their media player (like VLC) to use “RTP over RTSP (TCP)” instead of UDP, which can circumvent certain forwarding issues 2.
4. **Security Best Practices:** Exposing devices to the internet can invite security risks such as brute force attacks or exploitation of known vulnerabilities. To mitigate these risks, consider the following:
	* Use strong, unique credentials for your camera.
	* Regularly update the firmware.
	* Restrict access by IP whitelisting, if possible.
	* Consider alternative methods like setting up a VPN (e.g., OpenVPN or WireGuard) to securely access your network remotely rather than directly exposing the camera’s port 3.
5. **Testing Your Setup:** After configuring port forwarding, test the connection by accessing your public IP address with the designated port from an external network (not from inside your own network, as NAT loopback may not work). Tools like VLC can be used to verify if the RTSP stream is accessible remotely.

Each step here is critical for ensuring both functionality and security. Remember that network configurations can vary by router model and ISP, so consult your device manuals and support resources if you encounter issues.

If you’d like to explore additional related topics, we can discuss more advanced security setups like VLAN segmentation for your cameras or dive into troubleshooting specific streaming client configurations.

[1ipcamtalk.com](https://ipcamtalk.com/threads/two-cameras-same-rtsp-port-how-to-proceed.9699/)[2superuser.com](https://superuser.com/questions/875823/unable-to-remotely-view-ip-cameras-rtsp-stream)[3www.cctv-services.com](https://www.cctv-services.com/how-to-set-up-cctv-camera-port-forwarding-on-your-router/)

Redigera det här svaret

What troubleshooting steps should I take if it doesn't work?What are safer alternatives to port forwarding?How can I optimize my network for better camera performance?



Think Deeper

Logga in



I dag

**Du sa**

How functioning DCS-2330L from my computer via isp and Dlink and my router and my camera or direct to my camera?

**Copilot sa**







3 videor

Let’s break down the main options for operating your DCS-2330L from your computer via your ISP, your D-Link router, and your camera:

**1. Local Network (Direct, within your LAN)**

* **Connection:** The camera should be connected to your router, either using an Ethernet cable or wirelessly (using WPS or manual Wi-Fi setup). Once connected, your router will assign it a local IP address (via DHCP).
* **Access:** From your computer (which is on the same local network), you can open a web browser and enter the camera’s IP address. This brings up its configuration and live view page. This method is straightforward and doesn’t involve your ISP beyond delivering internet service to your home.

**2. Remote Access (Using Your ISP)**

* **Remote Viewing Options:** To access your camera from outside your local network, you have two main paths:
	+ **Port Forwarding:** You can configure your router to forward a specific port (often port 80 or a custom port set in the camera’s settings) from your public IP (provided by your ISP) to the camera’s local IP address. This allows you to type your public IP address (or a domain linked to it via dynamic DNS) from a remote location to view the feed. Keep in mind that if your ISP assigns you a dynamic IP, you might need to set up a dynamic DNS so you can always know what your public address is.
	+ **Cloud Service (mydlink):** D-Link offers the mydlink cloud service. This service allows you to remotely view and manage your camera without manually setting up port forwarding. You register the camera via the D-Link provided installation wizard, which associates it with your mydlink account. Once registered, you simply log into your account online or via a mobile app, and you can access your camera securely.

**3. Direct Connection to the Camera**

* **Bypassing the Router:** While it might be technically possible to connect your computer directly to the camera using an Ethernet cable, it isn’t generally recommended. Routers not only assign IP addresses but also provide a layer of security and network management. The typical and supported setup involves the camera being behind your router—even if you plan on accessing it directly within your home network.

**Summary of the Workflow**

* **Initial Setup:** Use D-Link’s installation wizard (downloadable from their website) to connect the camera to your router. The wizard will guide you through connecting the power, wiring (or connecting wirelessly), and verifying the LED indicators (for instance, a solid green LED often signals proper connectivity) 12.
* **Local Testing:** On your computer, access the camera’s web-based interface by entering the assigned local IP address.
* **Remote Access:** Either configure port forwarding on your D-Link router to access the camera via your public/ISP-assigned IP address or enable mydlink cloud services for a more straightforward, managed solution.

This multi-step approach ensures that your camera is not only accessible locally with minimal fuss but also remotely using either manual networking techniques or the built-in cloud services provided by D-Link. Remote access through your ISP means you’re leveraging your home’s internet connection while the router acts as the midpoint between the camera and the outside world.

If you’re curious about advanced configurations—such as managing dynamic IP addresses with a dynamic DNS service, or fine-tuning firewall rules—you might also want to explore networking topics like NAT configuration and security best practices. Additionally, some users find that using the D-Link’s mobile app can simplify live viewing and alerts, especially when away from home. Would you like to dig deeper into these aspects?

[1www.dlink.com](https://www.dlink.com/uk/en/support/faq/cameras-and-surveillance/dcs-series/dcs-2330l/how-do-i-set-up-and-install-my-dcs-2330l)[2support.dlink.com](https://support.dlink.com/resource/PRODUCTS/DCS-2330L/REVA/DCS-2330L_REVA_QIG_1.00_EN.PDF)

Redigera det här svaret

What are some best practices for securing my camera?How does port forwarding work for camera access?What are the differences between mydlink and port forwarding?



Think Deeper

Logga in



https://copilot.microsoft.com/chats/RXuDabjX2QiC5QrujawQZ

I dag

**Du sa**

How functioning DCS-2330L and D-Link and the mydlink cloud services?

**Copilot sa**

The DCS-2330L is a wireless outdoor HD network camera that comes integrated with D-Link’s mydlink cloud services, designed to simplify remote access and management of your camera. Here’s how the system works:

1. **Camera Setup and Network Connection:** The camera can be configured in one of two ways:
	* **Zero Configuration Setup (with a D-Link Cloud Router):** If you have a dedicated D-Link Cloud Router, the router automatically assigns your network settings (both wired and wireless) to the camera. In this scenario, the camera is plugged into the router (using Ethernet initially or via a wireless WPS process), and the camera then appears on your mydlink account almost automatically.
	* **Easy Setup (for other routers):** If you don’t have a D-Link Cloud Router, you can use a Setup Wizard available for both Windows and Mac systems. The wizard walks you through connecting the camera to your router, configuring the necessary network settings, and registering the camera with your mydlink account. This initial setup ensures that the camera is properly connected to your local network and ready for remote interaction 12.
2. **Registering with mydlink Cloud Services:** Once your camera is connected, you log into your mydlink account via the mydlink portal at www.mydlink.com. When the mydlink system detects your device, it prompts you to add the camera to your account. Registering your camera with mydlink enables:
	* **Remote Access:** You can view the live feed from your camera from anywhere using the mydlink website or the mydlink mobile app.
	* **Cloud Management:** The mydlink cloud service provides centralized management of your device, which includes remote monitoring, playback of recorded content (if you use an SD card), and other cloud features designed to simplify home or business security management. This process essentially links your physical device to a cloud account, making it accessible over the internet for monitoring and control 1.
3. **Benefits and Key Functions:**
	* **Remote Viewing and Monitoring:** With the camera registered on mydlink, you can access live video feeds and recorded clips from anywhere with an internet connection.
	* **Easy Device Management:** The integration with the mydlink cloud system makes device management straightforward—updates, configuration changes, and basic troubleshooting can be performed through the centralized portal or app.
	* **Flexibility in Network Setup:** Whether you have the dedicated cloud router or use another router with the Setup Wizard, the camera is designed to work with your existing network infrastructure while still providing the benefits of cloud connectivity and remote access 12.

In essence, the DCS-2330L works by first establishing a local network connection—either through automatic configuration with compatible D-Link hardware or via a manual setup process—and then linking the camera to your mydlink account. This integration allows you to harness cloud services for remote monitoring, configuration, and management, making home or business surveillance both accessible and manageable from virtually anywhere.

If you’re curious about potential security implications or additional features such as cloud storage options, there’s a broader conversation on securing cloud-connected devices and the evolution of smart home security systems. These topics can deepen your understanding of how integrated devices and cloud services work together in today's digital landscape.

[1support.dlink.com](https://support.dlink.com/resource/PRODUCTS/DCS-2330L/REVA/DCS-2330L_REVA_QIG_1.00_EN.PDF)[2www.dlink.com](https://www.dlink.com/-/media/Consumer_Products/DCS/DCS%202330L/Manual/DCS_2330L_Manual_1_01_WW.pdf)

Redigera det här svaret

What are some unique features of the DCS-2330L?What are the security implications of using mydlink cloud services?Is the DCS-2330L compatible with other cloud platforms?



Think Deeper

Logga in



https://copilot.microsoft.com/chats/YSBnQEe6UjbMUmyViytZg

I dag

**Du sa**

How functioning the mydlink cloud services?

**Copilot sa**

The mydlink cloud services are designed to simplify how you manage and monitor your network devices, such as cameras and routers, regardless of where you are. Here's how they function:

1. **Easy Device Registration and Setup:** When you sign up for a mydlink account, you register your mydlink-enabled devices using the mobile app or the web portal. The setup process is streamlined so that even users without extensive technical expertise can quickly add devices to their account1.
2. **Remote Access and Monitoring:** Once your devices are registered, they establish a secure connection with D-Link’s cloud servers. This setup allows you to access and control your devices—including viewing live video streams from your cameras or managing your network settings—directly from smartphones, tablets, or computers. This connectivity enables you to keep an eye on your home or small business from anywhere in the world12.
3. **Cloud Storage and Device Management:** Some mydlink devices offer cloud storage capabilities, allowing you to record and store footage that can later be accessed for review. This functionality means you can check recorded events, set alerts, or even share this content with others if needed. This centralized management is intended to provide both convenience and enhanced security1.
4. **Simplified Networking Management:** Beyond just cameras, mydlink cloud services extend to other network devices like routers, giving you the ability to monitor and adjust network settings remotely. This ensures that you remain in control of your digital environment, whether you’re at home or on the move1.

In essence, mydlink’s cloud system bridges the gap between physical devices in your home or office and modern, secure remote management, making it a powerful tool for both security and convenience.

There’s more to explore in this ecosystem—for instance, you might be interested in how the platforms safeguard your data or the specific capabilities of various mydlink-enabled products. Let me know which aspect intrigues you further!

[1www.mydlink.com](https://www.mydlink.com/content/productfamily)[2www2.dlink.com](http://www2.dlink.com/us/en/resource-centre/how-to-guides/how-to-monitor-your-home-from-anywhere-anytime)

Redigera det här svaret

What additional features do mydlink cloud services offer?How does mydlink ensure data security and privacy?What are the steps to set up mydlink services?



Think Deeper

Logga in



live1.sdp

https://copilot.microsoft.com/chats/7jdCwLjkEdMoratUi2brX

I dag

**Du sa**

live1.sdp

**Copilot sa**

Hmm, that looks like a filename—specifically one typically used for streaming media with the SDP (Session Description Protocol) format. It’s often part of a URL for a live video or audio feed, like from a surveillance camera or a media broadcast.

If you're trying to open or stream it, you’d usually need a media player that supports network streams, such as VLC Media Player. Just paste the full network URL (something like rtsp:// or http://your-server/live1.sdp) into the player’s network stream input.

Want help figuring out how to stream it or what it might be used for?

Redigera på en sida

What is the SDP format used for?What media players support SDP files?How does SDP compare to other streaming protocols?



Think Deeper

Logga in



**Du sa**

What media players support SDP files?

**Copilot sa**

SDP (Session Description Protocol) files aren’t media files on their own; they describe how a multimedia session is set up—providing details like network addresses, codec information, and timing. This means that any media player that supports network streaming and RTP/RTSP protocols is likely able to use an SDP file to initiate a stream. Here are some prominent examples:

* **VLC Media Player:** VLC is renowned for its robust support of various streaming protocols. It can easily open an SDP file—either by dragging the file into its interface or by using the "Open Network Stream" option. VLC then parses the details provided in the SDP file and establishes the media session accordingly. This flexibility makes it a top choice for handling SDP-described streams [1][5].
* **Windows Media Player:** While primarily geared toward local media playback, Windows Media Player also supports streaming protocols. When set up properly with the necessary codecs and network configurations, it can interpret and use an SDP file to play network streams [1].
* **MPlayer/MPV:** These open-source, command-line-friendly media players are common in the Linux community. They support network streams described by SDP files, allowing for efficient playback even on less resource-intensive systems.

There are also other players—such as QuickTime Player or RealPlayer—that may offer some SDP compatibility, though their ease of use and flexibility for this purpose might not match that of VLC or the aforementioned options.

Beyond these, it’s always good to check if your media player of choice supports network streaming and whether it requires any specific configuration when dealing with SDP files. If you’re setting up a network stream or troubleshooting playback issues, ensuring that the SDP file is correctly formatted and that your network settings match the described session can be just as important as the player itself.

If you’re curious about the underlying structure of SDP files or want more insights into how protocols like RTP and RTSP interact with these media players, there’s a fascinating world of streaming session management to explore.

Redigera på en sida

Explain the structure of SDP files.What are the differences between RTP and RTSP?In what situations are SDP files used?



Think Deeper

Logga in



<https://copilot.microsoft.com/chats/BNMTF2nm2uVb3kaU6JKsF>

I dag

**Du sa**

live1.sdp via http?

**Copilot sa**

The live1.sdp file is typically used in RTSP (Real-Time Streaming Protocol) streams from IP cameras or media servers. Accessing it via HTTP depends on how the camera or server is configured.

Some IP cameras or streaming devices allow HTTP access to streams using URLs like:

http://<camera-ip>/live1.sdp

However, this isn't always supported. For example, some VIVOTEK cameras changed their default access name from live.sdp to live1s1.sdp in newer firmware versions, which affected compatibility with third-party software like VLC1.

If you're trying to stream via HTTP and it's not working, here are a few things to check:

* Make sure the device supports HTTP streaming (some only support RTSP).
* Confirm the correct access path (e.g., live1.sdp, live1s1.sdp, etc.).
* Check if the stream is MJPEG, H.264, or another format—this affects compatibility.
* Ensure the correct port is open (usually 80 for HTTP, 554 for RTSP).

If you’re working with a specific camera or software, I can help you find the right URL format. Just let me know the model or setup!

[1vivotek.zendesk.com](https://vivotek.zendesk.com/hc/en-001/articles/900006469063--All-Cameras-Unable-to-get-HTTP-RTSP-streaming-via-3rd-party-software-after-upgrading-firmware-to-0x13-or-above-and-restore-to-factory-default)

Redigera på en sida

**Du sa**

live1.sdp via http?

**Copilot sa**

The file named live1.sdp is typically an SDP (Session Description Protocol) file used by RTSP (Real-Time Streaming Protocol) systems to describe media sessions from IP cameras or media servers. In most cases, it is not meant to be accessed directly via HTTP—its purpose is to be fetched by an RTSP client that performs the protocol handshake to set up a media stream.

That said, some cameras or streaming devices include an embedded HTTP server that can serve an SDP file as the configuration for their stream. For example, certain IP cameras have historically allowed both RTSP and HTTP access, where a URL might look like this:

Kopiera

http://<ip-address>/live1.sdp

However, whether this works depends heavily on the device's specific firmware and configuration. Some vendors even change the default access names as part of firmware updates. For instance, certain models (such as some VIVOTEK cameras) have switched their default naming from live.sdp to names like live1s1.sdp after a firmware upgrade, which can lead to compatibility issues if the expected file or endpoint isn’t available [2].

If your goal is to stream live video in a browser or another application that expects an HTTP source, you might need to use a media server (or transcoder) that takes the RTSP stream—usually defined by that SDP file—and delivers it in a browser-friendly protocol such as HLS (HTTP Live Streaming) or WebRTC. Direct HTTP access of an SDP file is less common because the SDP file itself merely describes the session; it is the RTSP handshake that initiates the live stream.

To summarize:

* **RTSP vs. HTTP:** The live1.sdp file is primarily for RTSP clients, not for direct retrieval over HTTP, unless your device has been explicitly configured to serve it that way.
* **Device specifics:** Ensure your camera or streaming device supports HTTP delivery for the stream. If it doesn’t, you’ll have to work with RTSP or set up a conversion.
* **Firmware quirks:** Be aware of firmware changes (such as default stream naming conventions) that might affect which SDP file is available.

Would you be interested in exploring ways to convert an RTSP stream to HTTP or learning more about configuring these camera endpoints for your specific needs?

Redigera på en sida

What are the main differences between RTSP and HTTP?How can I set up an RTSP to HTTP conversion?What are common issues with SDP files and solutions?



Think Deeper

Logga in



https://copilot.microsoft.com/chats/x3VYFprsaSTup9QGdcPyL

I dag

**Du sa**

RTSP Example: rtsp://192.168.0.2/live1.sdp

**Copilot sa**

That RTSP URL is a classic example used to access a media stream. Here's a deeper look:

1. **Understanding the Structure:** The URL rtsp://192.168.0.2/live1.sdp is built with the RTSP (Real Time Streaming Protocol) scheme. The parts break down as follows:
	* **rtsp://** — This indicates that the resource is accessed using RTSP.
	* **192.168.0.2** — This is the IP address of the streaming server or device.
	* **/live1.sdp** — The path points to an SDP (Session Description Protocol) file that describes the details of the media stream (such as formats, codecs, and timing).
2. **Common Usage Scenarios:** RTSP is typically used in environments that require real-time streaming, like surveillance systems, IP cameras, or live event broadcasting. The SDP file provides the necessary information for a client to understand how to decode and playback the stream.
3. **How to Use It:**
	* **Media Players:** Most modern media players, like VLC, support RTSP. You can open VLC, navigate to “Media” > “Open Network Stream,” and paste the URL. The player will use the SDP information to set up the stream automatically.
	* **Programming Libraries:** If you're integrating this into an application, many multimedia frameworks (such as FFmpeg, GStreamer, or even Python’s OpenCV with VideoCapture) can use RTSP URLs. This is particularly useful for applications that monitor or record real-time video feeds.
4. **Things to Consider:**
	* **Network Requirements:** Since RTSP operates over networks, ensure that the device with IP 192.168.0.2 is reachable and that no firewall or network configuration blocks the necessary ports.
	* **Latency and Performance:** RTSP is optimized for low-latency streaming, but bandwidth, the server’s hardware, and client processing can all affect playback quality.
	* **Security:** Be aware that RTSP streams often aren't encrypted by default. If the content is sensitive, consider using secure methods or tunnels (like VPNs) to protect the stream.

This example serves as a practical introduction to setting up and accessing live streaming media. If you’re experimenting with streaming in development or configuring network cameras—and you’re looking to optimize stream performance or troubleshoot potential issues—I can dive deeper into those topics. What aspect intrigues you the most?

Redigera på en sida

What are other applications of RTSP in technology?How can I optimize RTSP streaming performance?Can you show me code examples for using RTSP?



Think Deeper

Logga in





DCS-4712E / DCS-2330L

RTSP Port: 554

RTSP Rule: rtsp://ip/livestreamid.sdp

RTSP Example: rtsp://192.168.0.2/live1.sdp

Multicast

Stream ID: 1

Video Port: 25330

Video Address: 238.255.255.255

Stream ID: 2

Video Port: 25340

Video Address: 238.255.255.255

Stream ID: 3

Video Port: 25350

Video Address: 238.255.255.255

HTTP port: 80

Access name for stream1: video1.mjpg

Access name for stream2: video2.mjpg

Access name for stream3: video3.mjpg

RTSP

Authentication: Digest

RTSP port: 554

Access name for stream1: live1.sdp

Access name for stream2: live2.sdp

Access name for stream3: live3.sdp

HTTP: HTTP Port is the port you allocate in order to connect to the IP camera via a standard web browser.

HTTPS: HTTPS Port in a IP camera connects it with a PC via a secure web browser.

RTSP: RTSP Port is the port you allocate in order to connect to a IP camera by using streaming mobile device(s), such as a mobile phone or PDA.

PPPOE

User Name: admin

Password: ••••••••••••

Confirm Password: ••••••••••••

IP Address: Empty

PPPOE Settings

Enable Disable

User Name

Password

Confirm password

PPPoE Status: PPPoE is inactive.

PPPoE Setting: If you use the IP camera to connect directly to the Internet, you will need to enter the username and password, which were given to you when you set up your account with your Internet Service Provider. If the camera is behind a router or a gateway, you do not need to configure this setting.

Multicast

Enable multicast for stream 1

Multicast group address: 239.1.1.1

Multicast video port: 6550

Multicast RTCP video port: 6551

Multicast audio port: 6552

Multicast RTCP audio port: 6553

Multicast TTL [1~255]: 64

Enable multicast for stream 2

Multicast group address: 239.1.1.2

Multicast video port: 6554

Multicast RTCP video port: 6555

Multicast audio port: 6556

Multicast RTCP audio port: 6557

Multicast TTL [1~255]: 64

Enable multicast for stream 3

Multicast group address: 239.1.1.3

Multicast video port: 6558

Multicast RTCP video port: 6559

Multicast audio port: 6560

Multicast RTCP audio port: 6561

Multicast TTL [1~255]: 64

Multicast: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 ~ 3.

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save network bandwidth.

Multicast RTP video, audio port/Multicast RTCP video, audio port: The ports can be changed to values between 1024 and 65534. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

**Please, can you turn on the internet access? Reset your password #353192560**

**PA**

Peter Adolfsson

Svara

Svara alla

Vidarebefordra



Till:​cs@lycamobile.se​

Tor 2025-06-19 12:54



**Hög prioritet**

Hi again... I had put the sim LycaMobile in my iPhone mini 12 and I have a home wifi. My iPhone is connected via wifi now.

I can login to my LycaMobile via two factor authentication and via my iPhone and wifi.

I have more than half data remaining.

BUT when I shut down the wifi I have no internet access more. Can not access my LycaMoble via my iPhone.

Same problem now via iPhone as my router, no internet access.

The problem must be yours now, not my iPhone or my router.

Please, can you turn on the internet access? or can I get an ip-adress etc?

Thank you from Peter

**Från:** Peter Adolfsson <Peter.Adolfsson.bkg405h@outlook.com>
**Skickat:** Måndag, 16 juni 2025 20:33
**Till:** Support desk <cs@lycamobile.se>
**Ämne:** Sv: VB: Reset your password #353192560

Hello! and thank you from Peter.

Please, read the answer in bold:

**Från:** Support desk <cs@lycamobile.se>
**Skickat:** Måndag, 16 juni 2025 10:54
**Till:** peter.adolfsson.bkg405h@outlook.com <Peter.Adolfsson.bkg405h@outlook.com>
**Ämne:** Re: VB: Reset your password #353192560

Dear Peter,

Thank you for contacting Lycamobile. We are sorry for the late response.

If you have not registered your number, then it is not possible to login with password. You do not need to register with Bank-ID. You can register with Photo-ID on our website. You can dial \*105# to view the phone number.

If you have already registered the SIM and you still need help to reset the password, can we help you. For us to assist you, we need a little more information to verify you. Please reply to this email with the following information.

- Lycamobile number: **+46 76 434 xx xx**

- Are you the owner of the SIM card? Yes/No: **Yes**

- Provide your full name and date of birth:  **Peter Adolfsson 1963072xxxx**

Please note, that we cannot guarantee that the SIM-card can work in a router.

**The SIM-card has functioning very well in my router until I did write wrong password many times via my computer and...**

**... I sent an e-mail to support that I was worried about the big prize 1,2 SEK per 1 MB (1200 SEK per 1 GB) if I do not know if the data is over 1 GB.**

To efficiently manage your account, we recommend installing the Lyca Mobile app, available on the App Store for iOS or the Play Store for Android. For more details on our offerings, plans, and services, please visit [www.lycamobile.se.](http://vcyv5qqi.r.eu-central-1.awstrack.me/L0/http%3A//www.lycamobile.se./1/0107019777f22e6c-a88fc52d-b787-4d31-8114-4ad89ca4aadd-000000/qdrICH-YanSMjv-MWZ-Ye38VOIE%3D211) You can also reach our Customer Care Team Monday to Friday, 9 a.m. to 6 p.m. at 3332 from Lycamobile or 08-520 549 77, or access our chatbot, LIA, on our website for assistance.

**I have not the number +46 76 434 xx xx in my phone now, only +46 70 385 31 71.**

**I think if I put the sim-card LycaMobile in my phone I can reset my password and change to another password via LycaMobile network only data, no SMS/MMS/Phone.**

**I hope I can login to my LycaMobile via my computer after new password but I think it does not function, only via my phone and mobile nr +46 76 434 88 95 and two-factor authentication.**

Kind regards,
**Lina**
Lycamobile Customer Care

On Mon, Jun 16, 2025 at 7:13 AM UTC, Peter Adolfsson <peter.adolfsson.bkg405h@outlook.com> wrote:

|  |  |  |
| --- | --- | --- |
|  | Du får inte ofta e-post från peter.adolfsson.bkg405h@outlook.com. [Läs om varför det här är viktigt](http://vcyv5qqi.r.eu-central-1.awstrack.me/L0//care/attachment/external-link%3Fq%3Dhttps%253A%252F%252Faka.ms%252FLearnAboutSenderIdentification/1/0107019777f22e6c-a88fc52d-b787-4d31-8114-4ad89ca4aadd-000000/ol_Jq3elSJh2mIqSZqgd69PuLXc%3D211) |  |

|  |
| --- |
| **EXTERNAL EMAIL:** Do not click any links or open any attachments unless you trust the sender and know the content is safe. |

Hello again... I think the only solution is to reset my password is to change my sim-card from my router to my phone.

I think I can get a code for two factor authentication if the sim is in my phone, not in the router.

Is it right?

I shall try to swap my sim from router to phone maybe about 3-4 days and I hope to get a number (two factor authentication).

Do you agree?

Thank you from Peter

**Från:** Peter Adolfsson <Peter.Adolfsson.bkg405h@outlook.com>
**Skickat:** den 13 juni 2025 17:23
**Till:** Cs Sweden <cs@lycamobile.se>
**Ämne:** VB: Reset your password

**Från:** Peter Adolfsson <Peter.Adolfsson.bkg405h@outlook.com>
**Skickat:** den 13 juni 2025 17:21
**Till:** lycamobile@lycamobile.se <lycamobile@lycamobile.se>
**Ämne:** Sv: Reset your password

Hello... I can not reset my password.

I can not clicking "here" because of no address or hyperlink to click on.

Soon I must pay 1,2 sek per MB!!! Help!!! Maybe I must destroy my card...

Best regards from Peter Adolfsson, Piteå, Sweden.

**Från:** lycamobile@lycamobile.se <lycamobile@lycamobile.se>
**Skickat:** Fredag, 13 juni 2025 17:10
**Till:** Peter.Adolfsson.bkg405h@outlook.com <Peter.Adolfsson.bkg405h@outlook.com>
**Ämne:** Reset your password

Hi PETER ADOLFSSON,
Your Temporary Password is xxx
We’ve received a request to reset your password.
You can do this by clicking here.
If you didn’t make this request, please contact customer services by dialling 3332 (93#) from your Lyca SIM, or 0734973737 / 0852054977 from another phone, or by emailing us at cs@lycamobile.se for more information.
Thank you,
The Lyca Family

**LIA: I’ve successfully Unblocked your number for you.**

**PA**

Peter Adolfsson

Svara

Svara alla

Vidarebefordra





Till:​Cs Sweden​

Mån 2025-06-23 21:11

I’ve successfully Unblocked your number for you.

20:57:41

Is there anything else I can help you with today?

Yes

No

20:57:41

The number you have provided is blocked.

So please wait while we connect you to a live agent. Please wait a few moments.

20:40:24

Thank you for contacting Lyca Mobile , currently no agents are available, our opening hours are Monday to Friday - 09am to 06pm, Alternatively you can send us an email to cs@lycamobile.se \*T & C apply

Good Day! This is LIA, your Lycamobile Intelligent assistant.

Thank you!!!   from Peter

https://freedns.afraid.org/faq/#11

Question: (FAQ item #11)

What does the "Broken 08/30/2012" mean?

Answer:

For new domains:

If you have a domain and you see this message within freedns.afraid.org, this simply means your domain was found to not be correctly delegated to ns1 through ns4.afraid.org on the Internet.

1 subdomains

bkg405h.nfshost.com (Broken since : 07/26/2022 : contact owner) [ add ]

 camera.bkg405h.nfshost.com (G) A 46.230.173.135

Add

3 dynamic update candidates! (A and AAAA records)

bkg405h.nfshost.com [ add ]

camera.bkg405h.nfshost.co... Direct URL | Wget Script | Curl Script | Edit Record | quick cron example 46.230.173.135

camera.nfshost.com [ add ]

camera.nfshost.com Direct URL | Wget Script | Curl Script | Edit Record | quick cron example

www.camera.nfshost.com Direct URL | Wget Script | Curl Script | Edit Record | quick cron example

Check All Showing 3 records

Active dynamic entries Check Active

 camera.bkg405h.nfshost.com 46.230.173.135 http://sync.afraid.org/u/vhuJFUqGpJPshzEaJp2Mvhpr/

Generate a: cron script

Not currently enabled for dynamic updates (check box, and then click enable at bottom to activate) Check Inactive

 www.camera.nfshost.com

 camera.nfshost.com

Action: Enable Dynamic DNS...

Found domain delegation errors [ Check Delegations ]

 bkg405h.nfshost.com Status : BROKEN, 07/26/2022 (for 1 consecutive day)

[ delete bkg405h.nfshost.com ]

Tracing to bkg405h.nfshost.com[a] via A.ROOT-SERVERS.NET, maximum of 3 retries

A.ROOT-SERVERS.NET [.] (198.41.0.4)

|\\_\_\_ d.gtld-servers.net [com] (192.31.80.30)

| |\\_\_\_ ns.bos1.nearlyfreespeech.net [nfshost.com] (204.13.89.97) Got authoritative answer

| |\\_\_\_ ns.bos1.nearlyfreespeech.net [nfshost.com] (2607:ff18:8001:0152:0053:0000:0000:0001) Not queried

| |\\_\_\_ ns.phx8.nearlyfreespeech.net [nfshost.com] (208.94.117.33) Got authoritative answer

| |\\_\_\_ ns.phx8.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0008) Not queried

| |\\_\_\_ ns.phx7.nearlyfreespeech.net [nfshost.com] (208.94.117.1) Got authoritative answer

| |\\_\_\_ ns.phx7.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0007) Not queried

| |\\_\_\_ ns.phx6.nearlyfreespeech.net [nfshost.com] (208.94.116.161) Got authoritative answer

| |\\_\_\_ ns.phx6.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0006) Not queried

| |\\_\_\_ ns.phx5.nearlyfreespeech.net [nfshost.com] (208.94.116.129) Got authoritative answer

| |\\_\_\_ ns.phx5.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0005) Not queried

| |\\_\_\_ ns.phx4.nearlyfreespeech.net [nfshost.com] (208.94.116.97) Got authoritative answer

| |\\_\_\_ ns.phx4.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0004) Not queried

| |\\_\_\_ ns.phx2.nearlyfreespeech.net [nfshost.com] (208.94.116.33) Got authoritative answer

| |\\_\_\_ ns.phx2.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0002) Not queried

| |\\_\_\_ ns.phx3.nearlyfreespeech.net [nfshost.com] (208.94.116.65) Got authoritative answer

| |\\_\_\_ ns.phx3.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0003) Not queried

| \\_\_\_ ns.phx1.nearlyfreespeech.net [nfshost.com] (208.94.116.1) Got authoritative answer

| \\_\_\_ ns.phx1.nearlyfreespeech.net [nfshost.com] (2607:ff18:0080:0053:0000:0000:0000:0001) Not queried

Checked @ 2022-07-27 02:28:59 in 0.87 seconds

FreeDNS.afraid.org

Free DNS Hosting, Dynamic DNS Hosting, Static DNS Hosting, subdomain and domain hosting.

https://freedns.afraid.org/

http://mooo.com/

nslookup

server ns1.afraid.org

bkg405h.mooo.com

nslookup –type=soa mooo.com

https://www.lulearcklubb.se/Galleri/Video/

Klubblokalen

Banan http://77.110.47.81:1064/ Login: xxx, Lösenord: xxx (Port 1064)

Entrè http://77.110.47.81:1066/ Login: xxx, Lösenord: xxx (Port 1066)

Kök http://77.110.47.81:1068/ Login: xxx, Lösenord: xxx (Port 1068)

Luleå R/C Center

Fältet: På gång

Buggybanan: På gång

https://media.abelko.se/Manualer/WMPro/anvisningar-net1-altel-router-143.pdf

https://www.teracommobil.se/wp-content/uploads/2019/01/4G-WiFi-router-User-Manual.pdf

https://www.teracommobil.se/vanliga-fragor-om-min-router/

 För att nå din router från ett externt nätverk, det vill säga när du inte är ansluten direkt till den via det lokala nätverket, behövs en Fast IP-adress. Med denna adress kan du även nå de enheter som är ansluta till routern när du befinner dig utanför nätverket. En Fast IP-adress kostar 59kr/mån och beställningen görs hos vår kundservice.

https://www.teracommobil.se/fragor-om-nat-och-tackning/

 Vi erbjuder Privata dynamiska IP-adresser (NAT). NAT står för Network Adress Translation och innebär att flera abonnenter delar på en och samma IP-adress ut mot internet. Detta för att IP-adresserna ska räcka till för alla användare på internet. NAT-tekniken används av de flesta internetoperatörer.

 Skillnaden mellan en dynamisk och fast IP adress är att användaren hela tiden har samma IP-adress ut mot internet om den har en fast IP-adress. För de flesta användare brukar en dynamisk IP-adress räcka då det vid vanligt användande inte spelar någon roll om IP-adressen är dynamisk eller fast.

 Vissa tjänster kräver dock en Fast IP för att fungera med Teracom Mobils nät. T.ex. VPN-anslutningar eller övervakning via webbkamera från en annan plats än lokalt vid din router.

 Vid behov kan vi till företagskunder erbjuda publika fasta IP-adresser. Kontakta kundservice.

https://www.networkwebcams.co.uk/blog/2010/02/16/remotely-access-ip-camera/

Satellite links / ISP blocking

There are ISPs out there that block remote access on certain ports. It’s very common on GPRS and satellite links and will often prevent access from the internet completely. If you have a lot of trouble accessing it’s a good idea to give the ISP a call to confirm with them what you are doing is possible. Sometimes a change of port number to something other than 80 can sort things out.

https://reolink.com/blog/p2p-ip-camera/

Well, each P2P security camera or network video recorder (NVR) is identified with a unique ID number (UID) registered and integrated at the developer level, which is used to ping the P2P server (merely for connection, not a proxy) via network P2P IP camera apps or software for Mac/Windows.

 Note that you can’t view P2P IP cameras on web browsers remotely without port forwarding, because most web browsers are not built-in with P2P technology infrastructure.

https://www.remote.it/resources/connecting-to-axis-ip-cameras

Security | Opening ports on your router or firewall is extremely dangerous. Open ports are scannable by anyone on the internet. The risk is when legitimate services are exploited via security vulnerabilities or when malicious services are introduced via malware. Criminals can use these services in addition to open ports to gain unauthorized access to devices and networks. Which leads to criminals being able to access your data.

 View how many Axis devices have open ports on the Internet. Shodan Scan and Report

https://support.ajax.systems/en/ip-camera-integration/

It is not recommended to use the following network ports: 20, 21, 22, 53, 80, 110, 138, 139, 443, 3306, 3128, 3389, 5900 as they are most often used by various utility services.

 Keep in mind that the external port must be accessible (open in the router settings and not occupied by any service). This can be checked using online services, for example: 2ip.io. If you have problems with the determination of an open port, contact your internet provider.

 IP cameras use port 554 by default but the port number may differ for different manufacturers. The exact value can be found in the device manual.

Windows 10

VPN

Lägg till en VPN-anslutning

DCS-4712E

Kan inte ansluta till DCS-4712E

The remote connection was not made because the attempted VPN tunnels failed. The VPN server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the security parameters required for IPsec negotiation might not be configured properly.

Stäng

https://www.kjell.com/se/kunskap/hur-funkar-det/internet/lokala-natverk/vpn-tunnlar

PPTP (rekommenderas inte)

Det finns flera olika protokoll för att sätta upp och skicka trafik genom en VPN-tunnel. Vilka protokoll som kan användas bestäms tillsammans av VPN-servern och VPN-­klienten (d.v.s. datorn, mobilen, surfplattan eller routern som ska anslutas till servern). Både VPN-servern och VPN-klienten måste ha stöd för protokollet för att det ska kunna användas.

 PPTP (Point-to-Point Tunneling Protocol) är ett väl utbrett VPN-protokoll. Det finns inbyggt stöd för PPTP-tunnlar i Windows, macOS, Android och iOS. Det inbyggda stödet i kombination med att användaren endast behöver ange serveradress, användarnamn och lösenord, gör det synnerligen enkelt att sätta upp en PPTP-tunnel. Nackdelen med PPTP är säker­heten. Det finns flera kända och icke-åtgärdade säkerhetshål i PPTP som gör att protokollet enbart bör användas som en sista utväg. En avlyssningsbar krypterad tunnel är dock bättre än ingen tunnel alls.

L2TP/IPsec

L2TP/IPsec är en kombinationslösning. L2TP (Layer 2 Tunneling Protocol) används för att sätta upp själva tunnelanslutningen. Sedan används IPsec (IP security) för att få tunneln krypterad och säker.

 L2TP/IPsec är likt PPTP välutbrett. Det finns inbyggt stöd för L2TP/IPsec i Windows, Mac OS, Android och iOS. Till skillnad från PPTP är L2TP/IPsec fritt från kända säkerhetshål och anses därför vara säkert.

https://www.top10vpn.com/guides/vpn-passthrough/

Is VPN Passthrough the Same as a VPN Client?

VPN passthrough and a VPN client are two different things. A VPN client is an application installed on your device that allows you to configure your VPN’s connection settings. It’s through the VPN client that you choose your server, adjust your settings, and enable the connection.

 VPN passthrough is a feature on your router that allows VPN clients to connect to the server using older protocols. It’s enabled in your router’s settings.

What’s the Difference Between VPN Passthrough and a VPN Router?

A VPN router is simply a WiFi router with virtual private network (VPN) software installed on it. It encrypts all of the traffic that passes through your WiFi network, allowing you to protect all of your devices at the same time.

 You can buy VPN routers with VPN software already installed on them, or you can flash some router models with custom firmware like OpenWrt or FreshTomato. VPN routers support modern VPN protocols like OpenVPN and Wireguard, and they provide other advanced functionalities, too.

 VPN routers are the endpoint of the VPN connection; the VPN tunnel is established between the VPN server and the router. In effect, the router acts as the VPN client. This is useful when devices such as games consoles, smart TVs, or IoT devices need to connect to a VPN but do not support applications natively.

 This is very different from VPN passthrough, which is a feature on normal routers that allows VPN traffic to literally pass through the router. In this case, the VPN client is on your device.

https://www.lifewire.com/pppoe-internet-access-home-networks-817525

Problems With PPPoE

PPPoE connections might require special MTU settings to function properly. Providers tell their customers if their network requires a specific MTU value—numbers like 1492 (the maximum PPPoE supports) or 1480 are common. Home routers support an option to set the MTU size manually when needed.

https://www.teracommobil.se/nyheter/artiklar/vpn-sakrar-trafiken-for-affarskritisk-applikationer/

Net1 erbjuder Mobilt VPN som tjänst för att skydda företagets datatrafik. Tjänsten är flexibel och skalbar från några enstaka anslutningar till flera tusen. I tjänsten ingår även utökad support med ett dedikerat teknik- och supportteam, ett unikt telefonnummer och e-postadress för snabbare service.

http://www.teracommobil.se/wp-content/uploads/2018/02/Guide-VPN-Teracom-Mobil.pdf

Tekniken bakom tjänsten

Du som kund tilldelas ett eget APN (Access Point Name) dit bara dina egna abonnemang får ansluta. Autentisering kan ske både via SIM-kort och via företagets egen Radius-server. Utöver autentisering kan företagets Radius-server hantera annan konfiguration av routrarna, som till exempel tilldelning av IP-adresser.

 Trafiken är separerad i nätet med hjälp av IP/MPLS genom hela Teracom Mobils nätinfrastruktur och via en avlämningsrouter varifrån kopplas företaget in, antingen via en fast anslutning separerad från internet, eller via en VPN-tunnel (IPSsec) över internet.

https://www.teracommobil.se/nyheter/kundcase/linde-energi-sakrade-sina-it-system-i-enlighet-med-det-kommande-nis-direktivet/

Publicerad: 20 maj 2017

I takt med att Linde Energis verksamhet växer ökar även behovet av en skalbar och effektiv kommunikationslösning. Nu går Linde Energi från Bergslagen, norra Örebro, från 56 separata VPN-tunnlar till en mobil helhetslösning som tillgodoser hela uppkopplingsbehovet.

 – Genom att gå från egna VPN till en helhetslösning från en leverantör får vi bättre kontroll på utrustningen och säkrare kontakt med stationerna.

 Weine Ohlson är IT-ansvarig på Linde Energi. Som ensam på IT-avdelningen köper han både in extern drift och får hjälp av kommunen med att drifta och underhålla systemen. Att gå från 56 separata VPN till en helhetslösning ger en stor tidsbesparing och ökar säkerheten markant.

https://www.nordiskaprojekt.se/2018/02/23/linde-energi-valjer-privat-nat-fran-net1/

---

... separata VPN-tunnlar för varje enskild uppkopplingspunkt.

---

Istället för 56 VPN-tunnlar skapas en gemensam VPN-tunnel för all kommunikation.

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html#~steps-to-setup-a-vpn

Step 1: Line up key VPN components

To get started, you'll need a VPN client, a VPN server, and a VPN router. The downloadable client connects you to servers around the world, so employees everywhere can access your small business network. The client can be used on devices like smartphones and laptops, even if workers are using public Wi-Fi networks.

 To secure and encrypt all network traffic, you'll also need a VPN router. Many routers come with VPN clients built-in.

http://192.168.0.2/live1.sdp

http://192.168.0.2/asppage/common/home.asp?id=1

ASP (Active Server Pages)

[https://bkg405h.mooo.com/192.168.0.2:554](https://bkg405h.mooo.com/192.168.0.2%3A554)

[https://bkg405h.mooo.com/rtsp://192.168.0.2/live1.sdp](https://bkg405h.mooo.com/rtsp%3A//192.168.0.2/live1.sdp)

[rtsp://bkg405h.mooo.com:554/live1.sdp](https://bkg405h.mooo.com/rtsp%3A//192.168.0.2/live1.sdp)

[rtsp://bkg405h.mooo.com:192.168.0.2/live1.sdp](https://bkg405h.mooo.com/rtsp%3A//192.168.0.2/live1.sdp)

[rtsp://bkg405h.mooo.com/192.168.0.2/live1.sdp](https://bkg405h.mooo.com/rtsp%3A//192.168.0.2/live1.sdp)

”Just paste the full network URL (something like rtsp:// or http://your-server/live1.sdp) into the player’s network stream input.”

<http://your-server/live1.sdp>

<http://192.168.0.2/live1.sdp> ?

rtsp://192.168.0.2/live1.sdp

rtsp://192.168.0.2/live2.sdp

rtsp://ip/livestreamid.sdp

1. The URL rtsp://192.168.0.2/live1.sdp is built with the RTSP (Real Time Streaming Protocol) scheme. The parts break down as follows:
	* **rtsp://** — This indicates that the resource is accessed using RTSP.
	* **192.168.0.2** — This is the IP address of the streaming server or device.
	* **/live1.sdp** — The path points to an SDP (Session Description Protocol) file that describes the details of the media stream (such as formats, codecs, and timing).

https://copilot.microsoft.com/chats/SH6Y7eTe5L5TnCwvNok5e

I dag

**Du sa**

Port Forwarding: rtsp://bkg405h.mooo.com:554/live1.sdp or rtsp://bkg405h.mooo.com:192.168.0.2/live1.sdp or rtsp://bkg405h.mooo.com/192.168.0.2/live1.sdp? Withs is ok?

**Copilot sa**

The correct RTSP URL largely depends on how your port forwarding is configured on your router. Here's a quick breakdown:

1. rtsp://bkg405h.mooo.com:554/live1.sdp This is the standard format if you've forwarded external port **554** on your public IP to the camera's RTSP port internally. It's clean and likely the correct one if your setup is straightforward.
2. rtsp://bkg405h.mooo.com:192.168.0.2/live1.sdp This format is *not* valid. RTSP URLs should include the **host** (your domain or IP) and then the **path**—you shouldn't include a private IP in the URL path like that.
3. rtsp://bkg405h.mooo.com/192.168.0.2/live1.sdp Same as above—this format is incorrect because it embeds a local IP in the path section, which RTSP clients wouldn’t understand.

**Conclusion:** Stick with the first one: rtsp://bkg405h.mooo.com:554/live1.sdp

Also, make sure:

* The camera is reachable at 192.168.0.2 locally.
* Port 554 is properly forwarded in your router settings to the camera's RTSP port.
* Any firewall or ISP-level NAT isn’t blocking the port.

If you're still unsure, I can help you double-check your port forwarding setup or even help test RTSP links using a tool like VLC. Just let me know how you'd like to continue!

Redigera på en sida

**Du sa**

Port Forwarding: rtsp://bkg405h.mooo.com:554/live1.sdp or rtsp://bkg405h.mooo.com:192.168.0.2/live1.sdp or rtsp://bkg405h.mooo.com/192.168.0.2/live1.sdp? Which one is okay?

**Copilot sa**

The correct URL is:

Kopiera

rtsp://bkg405h.mooo.com:554/live1.sdp

Here's why:

1. **Standard Format:** The URL rtsp://bkg405h.mooo.com:554/live1.sdp uses the proper scheme (rtsp), host (bkg405h.mooo.com), and port (554, which is the default for RTSP). This is exactly what you need if your router forwards external port 554 to your camera’s internal RTSP port.
2. **Improper Inclusion of Local IP:** The URLs
	* rtsp://bkg405h.mooo.com:192.168.0.2/live1.sdp and
	* rtsp://bkg405h.mooo.com/192.168.0.2/live1.sdp

are incorrect because they improperly include the local IP address (192.168.0.2). In the first, the local IP is used as the port, which is invalid since ports must be numeric values between 1 and 65535. In the second, the local IP is erroneously added to the path. Port forwarding works by mapping an external port on your public IP (or domain) to a device on your internal network; you don’t include the internal address in the URL itself.

1. **Conclusion:** If your port forwarding is set up correctly (forwarding port 554 on the external interface to the camera's RTSP port), using rtsp://bkg405h.mooo.com:554/live1.sdp is the proper configuration.

If you have any more questions or need further clarification about configuring your network or testing the URL with software like VLC, feel free to ask!

Redigera på en sida

Can you explain how port forwarding works?What are common issues with RTSP port forwarding?What software can I use to test RTSP streams?



Think Deeper

Logga in



https://copilot.microsoft.com/chats/NuBLbXijCLoXR3uibYZQ3

I dag

**Du sa**

How can I open port 554? Is the port closed by isp?

**Copilot sa**

Port 554 is typically used for RTSP (Real Time Streaming Protocol), often by IP cameras or streaming servers. If you're having trouble with it, here’s how to approach it:

**1. Check if the Port Is Open**

You can use an online tool like Port Checker or HostingChecker’s Open Port Tool to test if port 554 is open on your public IP. Make sure the device or service using the port is running when you test.

**2. Router and Firewall Settings**

If the port appears closed:

* **Log into your router** and set up port forwarding for TCP/UDP 554 to the internal IP of your device.
* **Check your firewall** (on your computer or router) to ensure it’s not blocking the port.

**3. ISP Blocking**

Some ISPs block certain ports to prevent unwanted traffic. While port 554 isn’t commonly blocked, it’s possible. You can test this by:

* Temporarily placing your device in a DMZ (Demilitarized Zone) on your router.
* Using a tool like Firebind or running a port scan from an external network to see if the port is reachable1.

If all else fails and the port remains closed despite correct local settings, your ISP might indeed be blocking it. In that case, contacting them directly or using a VPN that supports port forwarding could be a workaround.

Want help walking through the port forwarding setup for your specific router?

[1superuser.com](https://superuser.com/questions/10903/is-there-a-simple-way-to-detect-isp-port-blocking)

Redigera på en sida

How do I access my router settings?What router model do I have?What other ports should I know about?



Snabbt svar

Logga in



Connection failed:

VLC could not connect to "bkg405h.mooo.com:554".

Your input can't be opened:

VLC is unable to open the MRL 'rtsp://bkg405h.mooo.com:554/live1.sdp'. Check the log for details.

https://copilot.microsoft.com/chats/YFJj1TGHvR3hrBqqJYMxx

I dag

**Du sa**

A VPN that supports port forwarding

**Copilot sa**

If you're looking for a VPN that supports port forwarding, here are some solid options:

* **Private Internet Access (PIA)** – Offers built-in port forwarding on its desktop and Android apps. It's known for fast speeds and a large server network1.
* **PrivateVPN** – Includes dedicated port forwarding and P2P servers. While its server network is smaller, it’s a good pick for secure torrenting and remote access2.
* **PureVPN** – A budget-friendly choice with a wide server network and port forwarding support2.
* **IVPN** – A lesser-known but privacy-focused VPN that supports port forwarding and is open-source2.

Each of these has its own setup process, so once you pick one, check their guide for enabling port forwarding on your device. Want help choosing based on your specific use case—like gaming, torrenting, or remote access? I’ve got you.

[1www.safetydetectives.com](https://www.safetydetectives.com/blog/best-vpns-with-port-forwarding/)[2privacysavvy.com](https://privacysavvy.com/vpn/best/vpns-with-port-forwarding/)

Redigera på en sida

**Du sa**

a VPN that supports port forwarding

**Copilot sa**

VPNs that support port forwarding allow you to let incoming connections hit a specific port on your device—ideal for activities like torrenting, remote desktop access, hosting game servers, or running personal servers behind NAT. However, note that because port forwarding does expose a specific entry point to your network, careful configuration and robust security measures are essential.

Here are some of the top options:

* **Private Internet Access (PIA):** PIA is widely recommended for its built-in port forwarding feature accessible directly via its desktop and Android apps. It’s well-regarded for having an extensive server network, providing robust P2P capabilities, and maintaining solid performance for tasks that benefit from port forwarding. Reviews from multiple sources note PIA as a leading choice for secure torrenting and remote access applications12.
* **PrivateVPN:** This service offers dedicated port forwarding and is optimized for P2P activities. Although its server network may be smaller than some competitors, PrivateVPN provides specific setups intended to maximize performance on applications like streaming services and remote access. It’s a strong choice if you’re looking for a secure yet straightforward port forwarding experience1.
* **PureVPN:** PureVPN provides a budget-friendly option while still supporting port forwarding. Its extensive server network ensures that you can often find a nearby server to maintain speed and security, making it useful if you’re balancing cost with performance. Reviews mention that its port forwarding capabilities make it attractive for users needing remote connectivity or enhanced torrenting speeds1.
* **IVPN:** For those who prefer a more privacy-focused and open-source approach, IVPN offers port forwarding in conjunction with strong security features. While it may not have the same level of mainstream recognition as some others, its transparent approach makes it worth considering if privacy is a top priority1.

It’s important to note that some other popular VPNs, like **NordVPN**, do not natively support port forwarding (or require router configuration workarounds), so if that feature is essential to you, you’ll want to lean toward alternatives like PIA or PrivateVPN.

Before subscribing, consider your primary use case—torrenting, hosting remote services, gaming, etc.—and review detailed setup guides provided by the VPN service to make sure that the port forwarding configuration meets your needs. You might also want to check for any associated risks or extra configuration steps required to secure the forwarded ports without compromising your overall network security.

Would you like to explore how port forwarding works in-depth or dive into specific setup instructions for any of these VPNs?

[1privacysavvy.com](https://privacysavvy.com/vpn/best/vpns-with-port-forwarding/)[2www.safetydetectives.com](https://www.safetydetectives.com/blog/best-vpns-with-port-forwarding/)

Redigera på en sida

How does port forwarding benefit specific applications?What are the security risks of using port forwarding?How do I configure port forwarding on my VPN?



Think Deeper

Logga in



Router:

Device & SIM Info

Device Model: ALR-U270

IMEI: xxx

Router Version: CPE2\_U270\_Tera\_v1.0.7

LTE Version: ATL2\_AT\_2.1.55

UICCID: xxx

IMSI: xxx

Server:

OS Name Microsoft Windows XP Professional

Version 5.1.2600 Service Pack 3 Build 2600

OS Manufacturer Microsoft Corporation

System Name HPCOMPAQ

System Manufacturer Hewlett-Packard

System Model HP d530 SFF(DN204S)

System Type X86-based PC

Processor x86 Family 15 Model 2 Stepping 9 GenuineIntel ~2793 MHz

BIOS Version/Date Hewlett-Packard 786B2 v1.11, 2003-07-10

SMBIOS Version 2.3

Windows Directory C:\WINDOWS

System Directory C:\WINDOWS\system32

Boot Device \Device\HarddiskVolume1

Locale United States

Hardware Abstraction Layer Version = "5.1.2600.5512 (xpsp.080413-2111)"

User Name HPCOMPAQ\Peter Adolfsson

Time Zone W. Europe Daylight Time

Total Physical Memory 1 024,50 MB

Available Physical Memory 714,32 MB

Total Virtual Memory 2,00 GB

Available Virtual Memory 1,96 GB

Page File Space 2,39 GB

OpenVPN-v2.5.4.exe / OpenVPN\_v2.5.4\_for\_XP\_20220123.7z

Client:

Win10 VPN?

https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html#~steps-to-setup-a-vpn

Step 1: Line up key VPN components

To get started, you'll need a VPN client, a VPN server, and a VPN router. The downloadable client connects you to servers around the world, so employees everywhere can access your small business network. The client can be used on devices like smartphones and laptops, even if workers are using public Wi-Fi networks.

 To secure and encrypt all network traffic, you'll also need a VPN router. Many routers come with VPN clients built-in.

https://copilot.microsoft.com/chats/XMA6tvKQ19XtPEG5Mne4F

I dag

**Du sa**

vpn server software for windows xp

**Copilot sa**

Running a VPN server on Windows XP is a bit of a throwback, but there are still a few options that can work with some effort:

**🛠️ VPN Server Software Options for Windows XP**

1. **OpenVPN for Windows XP** A community-patched version of OpenVPN v2.5.4 has been rebuilt to support Windows XP and Server 2003. It includes:
	* Support for stronger ciphers like AES-256-CBC
	* Updated TAP driver with improved network speed
	* Fixes for known XP-specific bugs You can find it on SourceForge.
2. **SoftEther VPN** While newer versions may not officially support XP, older builds of SoftEther VPN Server might still run. It's known for:
	* Multi-protocol support (OpenVPN, L2TP/IPSec, SSTP)
	* High performance and flexibility You’ll need to dig into archived versions for XP compatibility.
3. **Le VPN (OpenVPN Setup)** Le VPN offers a guide for setting up OpenVPN on Windows XP using their service. It’s more of a client-side setup, but could be adapted for server use with technical know-how. Check out their installation guide.

Keep in mind that Windows XP is no longer supported by Microsoft, so using it as a VPN server poses serious security risks. If possible, consider running the VPN server on a more modern OS and connecting to it from XP instead.

Want help setting one of these up or exploring safer alternatives?

Redigera på en sida

**Du sa**

vpn server software for windows xp

**Copilot sa**

Here are the main ways you can turn an XP box into a VPN server:

1. OpenVPN (patched for XP) A community rebuild of OpenVPN 2.5.4 runs on Windows XP/SP3 (and Server 2003). You get AES-256-CBC support, a 1 Gbps TAP driver, and XP-specific bug fixes. Grab it from SourceForge and follow the included README to install and configure your server and clients1.
2. Windows XP’s built-in PPTP/L2TP server No extra software needed—just XP Professional’s “Incoming Connection” wizard: • Open Network Connections → New Connection Wizard. • Select “Accept incoming connections” and pick “Through the Internet.” • Enable “Allow callers to connect to” your local LAN and assign user accounts. You’ll wind up with a PPTP VPN server; for L2TP/IPsec add manual registry tweaks and preshared keys.
3. SoftEther VPN (legacy build) SoftEther’s early-2010 releases ran on XP. You won’t find an “XP” tag on the main site, but if you dig archived builds (v1.x–v2.x) they install and run just fine, providing multi-protocol support (OpenVPN, L2TP, SSTP) and a GUI manager. Check the project’s archive on SourceForge or the University of Tsukuba site for installers1.

Security note: XP no longer gets patches, so any VPN you expose to the Internet risks compromise. If you just need remote-access for an XP client, it’s far safer to host your VPN on a modern OS (Windows Server, Linux, or even a home router) and let XP be a client.

— Want step-by-step help configuring one of these, or suggestions for low-cost hardware you can turn into a more secure VPN host? Let me know!

[1sourceforge.net](https://sourceforge.net/projects/openvpn-for-windows-xp/)

Redigera på en sida

Can you provide a step-by-step guide for OpenVPN?How do OpenVPN and SoftEther compare?What are the best practices for securing a VPN on XP?



Think Deeper

Logga in

