



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for D-LINK DSR-250N. You'll find the answers to all your questions on the D-LINK DSR-250N in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual D-LINK DSR-250N
User guide D-LINK DSR-250N
Operating instructions D-LINK DSR-250N
Instructions for use D-LINK DSR-250N
Instruction manual D-LINK DSR-250N



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)
<http://yourpdfguides.com/dref/5324200>

Manual abstract:

192 Testing the LAN path from your PC to a remote device . @@ 52 Figure 30: Protocol binding setup to associate a service and/or LAN source to a WAN and/or destination network . 53 Figure 31: Routing Mode is used to configure traffic routing between WAN and LAN, as well as Dynamic routing (RIP) . 69 Figure 42: List of Available Profiles shows the options available to secure the wireless link . 76 Figure 46: List of configured access points (Virtual APs) shows one enabled access point on the radio, broadcasting its SSID . 82 Figure 51: WPS configuration for an AP with WPA/WPA2 profile . 87 Figure 54: Example where an outbound SNAT rule is used to map an external IP address (209. 225) to a private DMZ IP address (10. 90 Figure 55: The firewall rule configuration page allows you to define the To/From zone, service, action, schedules, and specify source/destination IP addresses as needed. . 91 Figure 56: The IPv6 firewall rule configuration page allows you to define the To/From zone, service, action, schedules, and specify source/ destination IP addresses as needed. 98 Figure 61: A available ALG support on the router. 102 Figure 64: Content Filtering used to block access to proxy servers and prevent ActiveX controls from being downloaded. 106 Figure 68: The following example binds a LAN host's MAC Address to an IP address served by DSR. If there is an IP/MAC Binding violation, the violating packet will be dropped and logs will be captured. 107 Figure 69: Intrusion Prevention features on the router . 108 Figure 70: Protecting the router and LAN from internet attacks . 109 Figure 71: Example of Gateway-to-Gateway IPsec VPN tunnel using two DSR routers connected to the Internet. 111 Figure 72: Example of three IPsec client connections to the internal network through the DSR IPsec gateway . 145 8 Unified Services Router User Manual Figure 98: Configured client routes only apply in split tunnel mode. 146 Figure 99: List of configured SSL VPN portals. The configured portal can then be associated with an authentication domain . 164 Figure 114: Log configuration options for traffic through router . 166 Figure 115: IP v6 Log configuration options for traffic through router . 170 Figure 119: Restoring configuration from a saved file will result in the current configuration being overwritten and a reboot . The second WAN port can be configured as a DMZ port allowing you to isolate servers from your LAN. Typical deployment and use cases scenarios are described in each section . For more detailed setup instructions and explanation of each configuration parameter, refer to the online help that can be accessed from each page in the router GUI. The LAN connection may be through the wired Ethernet ports available on the router, or on the initial setup is complete, the DSR may also be managed through its wireless interface as it is bridged with the LAN. With DHCP, PCs and other LAN devices can be assigned IP addresses as well as addresses for DNS servers , Windows Internet Name Service (WINS) servers , and the default gateway .

Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications the default DHCP and TCP/IP settings are satisfactory . if you want another PC on your network to be the DHCP server or if you are manually configuring the network works settings of all of your PCs , set the DHCP mode to on . DHCP relay can be used to forward DHCP lease information from another LAN device that is the network DHCP server; this is particularly useful for wireless clients . Instead of using a DNS server, you can use a Windows Internet Naming Service (WINS) server. You can also enable DNS proxy for the LAN. In the LAN Setup page, enter the following information for your router: In the DHCP section, select the DHCP mode: Figure 1 : Setup page for LAN TCP/IP settings 15 Unified Services Router User Manual 2. 1. 1 LAN DHCP Reserved IPs Setup > Network Settings > LAN DHCP Reserved IPs This router DHCP server can assign TCP/IP configuration to computers in the LAN explicitly by adding client's network interface hardware address and the IP address to be assigned to that client in DHCP server's database. Whenever DHCP server receives a request from client, hardware address of that client is compared with the hardware address list present in the database as, if an IP address is already assigned to that computer or device in the database, the customized IP address is configured on the device and IP address is assigned to the client automatically from the DHCP pool.

Associate with IP/MAC Binding : When the user enables this option the Computer Name, IP and MAC addresses are associated with the IP/MAC binding . The action that can be taken on list of reserved IP addresses are: Select: Select all the reserved IP addresses in the list . The following settings are used to configure the DHCPv6 server: In this case the router advertises the random (RA/DVD) must be configured on this device and ICM Pv6 router does cover every messages are used by the host for auto-configuration . Prefix Delegation The following settings are used to configure the Prefix Delegation : 4 Configuring IPv6 Router Advertisements Router Advertisement are an alternative to IPv4 DHCP as signmen ts for LAN clients , in that the router will assign an IP address and support in getting work in formation to devices that are configured to accept such details. The following settings are used to configure RA/DVD: The actual duration between advertisement is a random value between one third of the field and the field . Figure 5 : Configuring the Router Advertisement Daemon Advertisement Prefixes Advanced > IPv6 > IPv6 LAN > Advertisement Prefixes The router advertisements configured with advertisement prefixes allow the router to inform hosts how to perform static address auto configuration . router advertisement contains a list of subnets and prefixes that allow the router to determine which hosts and where they are .



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)
<http://yourpdfguides.com/dref/5324200>

The following prefix options are available for the router advertisement: Figure 6: IPv6 Advertisement Prefix Settings 2. LAN ports can be assigned unique VLAN IDs so that traffic to and from the physical port can be isolated from the general LAN. Figure 7: Adding VLAN members to the LAN 2.

By selecting one more VLAN membership options for a General or Trunk port, traffic can be routed between the selected VLAN membership IDs 25 Unified Services Router User Manual Figure 9: Configuring VLAN membership for a port 2. Each configured VLAN ID can map directly to a subnet within the LAN. Each LAN port can be assigned a unique IP address and a VLAN specific DHCP server can be configured to assign IP addresses to devices on the VLAN. The DMZ adds an additional layer of security to the LAN, as specific services/ports that are exposed to the internet on the DMZ do not have to be exposed on the LAN. There are no restrictions on the IP addresses subnet assigned to the DMZ port, other than the fact that it cannot be identical to the IP address given to the LAN interface of the gateway. If a network device is detected by UPnP, the router can open internet external ports for the traffic protocol required by that network device. Figure 13: UPnP Configuration UPnP Port map Table The UPnP Port map Table has the details of UPnP devices that respond to the router's advertisements. The following information is displayed for each detected device: Active: A yes/no indication whether the port of the UPnP device that established a connection is currently active Port (External Port): The external port supported by UPnP (if any) IP Address: The IP address of the UPnP device detected by the router Click Refresh to refresh the port map table and search for any new UPnP devices. Connecting to the Internet: WAN Setup This router has two WAN ports that can be used to establish a connection to the internet. The following ISP connection types are supported: DHCP, Static, PPPoE, PPTP, L2TP, 3G Internet (via USB modem).

It is assumed that you have arranged for internet service with your Internet Service Provider (ISP). By going through a few straightforward configuration pages you can take the information provided by your ISP to get your WAN connection up and online in internet access for your network. Figure 17: Internet Connection Setup Wizard You can start using the Wizard by logging in with the administrator password for the router. Once authenticated set the time zone that you are located in, and then choose the type of ISP connection type: DHCP, Static, PPPoE, PPTP, L2TP. User Name Password Secret (required for L2TP only) MPPE Encryption: For PPTP links, your ISP may require you to enable Microsoft Point-to-Point Encryption (MPPE). In such case, user has to take care of routing manually by configuring the routing from Static Routing page. connection type: To keep the connection always on, click Keep Connected. To log out after the connection is idle for a period of time (useful if your ISP costs are based on long times), click Idle Timeout and enter the time, in minutes, to wait before disconnecting in the Idle Time field. 2 WAN DNS Servers The IP addresses of WAN Domain Name Servers (DNS) are typically provided dynamically from the ISP but in some cases you can define the static IP addresses of the DNS servers. 39 Unified Services Router User Manual Figure 20: WAN configuration for Japanese MPPE (part 1) There are a few key elements of a multiple IP PPPoE connection: Primary and secondary connection names are concurrently Each session as a DNS server source for domain name lookup, this can be assigned by the ISP or configured through the GUI Figure 21: WAN configuration for Multiple PPPoE (part 2) 3. The primary and secondary DNS servers on the ISP's IPv6 network are used for resolving internet addresses, and these are provided along with the static IPes traffic that is received on any of its physical interfaces. Broadcast and multicast packets that arrive on the LAN interface are switched to the WAN and vice versa, if they do not get filtered by firewall or VPN policies. To maintain the LAN and WAN in the same broadcast domain select Transparent mode, which allows bridging of traffic from LAN to WAN and vice versa, except for router-terminated traffic and other management traffic. All DSR features (such as 3G modem support) are supported in transparent mode as a supplement to the LAN and WAN are configured to be in the same broadcast domain. In Only: The router accepts RIP information from other routers, but does not broadcast its routing table.

The authentication key valid lifetimes are configured to ensure that the routing information exchange is with current address supported routers detected on the LAN. The List of IPv4 Static Routes and List of IPv6 Static Routes share the same fields (with none except Active: Determines whether the route is active or inactive. A route can be added to the table and made inactive, if needed. Gateway: IP address of the gateway through which the destination host or network can be reached. Two routers having a common segment; their interfaces have to belong to the same area on that segment.

If Authentication Type is Simple thenospackets are authenticated using simple text key. ISATA specifies an IPv6-IPv4 compatibility address format as well as a means for site border discovery. ISATA also specifies the operation of IPv6 over a specific link layer - that being IPv4 used as a link layer for IPv6.



[You're reading an excerpt. Click here to read official D-LINK](http://yourpdfguides.com/dref/5324200)

[DSR-250N user guide](http://yourpdfguides.com/dref/5324200)

<http://yourpdfguides.com/dref/5324200>

There are a few key elements of WAN 3 configuration. DNS Server Source: Choose one of the following options: Get Dynamically from ISP: Choose this option if your ISP did not assign a static DNS IP address. Use These DNS Servers: Choose this option if your ISP assigned a static DNS IP address for you to use. Always complete the fields that are highlighted while in this section. The WAN Mode options are now available as there are two WAN ports for the gateway. Once the connection types and settings are configured and saved, navigate to the WAN status page (Setup > Internet Settings > WAN 3 Status) and Enable the WAN3 link to establish the 3G connection.

8 WAN Port Settings Advanced > Advanced Network > WAN Port Setup The physical ports and settings for each WAN link can be defined here. This is the largest packet size that can pass through the interface without fragmentation. This size can be increased, however larger packets can introduce network lag and bring down the interface speed. Note that a 1500 byte size packet is the largest allowed by the Ethernet protocol at the network layer. The port speed can be selected by the router when a unit is selected. With this option the optimal port settings are determined by the router and network. The duplex (half or full) can be defined based on the port speed, as well as one of the rates: 10 Mbps, 100 Mbps and 1000 Mbps (i.e. the default MAC address is defined during the manufacturing process for the interfaces, and can uniquely identify the router. You can customize each WAN port's MAC address as needed, either by letting the WAN port assume the current LAN host's MAC address or by entering a MAC address manually. In radio that allows you to create an access point for wireless LAN clients.

The security/authentication options are grouped in a wireless Profile, and each configured profile will be available for selection in the AP configuration menu. The profile defines various parameters for the AP, including the security between the wireless client and the AP, and can be shared between multiple APs in the same device when needed. Each virtual AP appears as an independent AP (unique SSID) to support different clients in the environment, but is actually running on the same physical radio integrated with the router. Profiles may be thought of as a group of AP parameters that can then be applied to one or more but multiple AP instances (SSIDs), thus avoid duplication if the same parameters are to be used on multiple AP instances or SSIDs. By going through a few straightforward configuration pages you can enable a Wi-Fi network on your LAN and allow support 802.

This key is the pre-shared key for WPA or WPA2 type security. Supported clients that have been given this PSK can associate with the AP. Personal Identification Number (PIN): The wireless device that supports WPS may have an alphanumeric PIN, and if entered in the field the AP will establish a link to the client. You need to be able to associate an AP with WPA/WPA2 security and also enable WPS in the Advanced > Wireless Settings > WPS page to use the WPS wizard. The authentication can be a pre-shared key (PSK), Enterprise mode with RADIUS server, or both.

WPA2: This security type uses CCMP encryption (and the option to add TKIP encryption) or either PSK (pre-shared key) or Enterprise (RADIUS Server) authentication. This mode allows legacy devices that only support WPA2 keys (such as an older wireless printer) to connect to a secure AP where all the other wireless clients are using WPA2. Figure 42: List of Available Profiles shows the options available to secure the wireless link. User Manual Encryption: select the encryption key size -- 64 bit WEP or 128 bit WEP. The larger size keys provide stronger encryption, thus making the key more difficult to crack. WEP Passphrase: enter an alphanumeric phrase and click Generate Key to generate a unique WEP key with length determined by the encryption key size. Next choose one of the key sizes to be used for authentication. WPA or WPA2 with PSK a pre-shared key (PSK) is a known phrase configured on the AP and client both and is used to authenticate the wireless client. A secondary RADIUS server provides redundancy in the event that the primary server cannot be reached by the router when needed. The Timeout and Retries fields are used to either move to a secondary server if the primary cannot be reached, or to give up the RADIUS authentication attempt if communication with the server is not possible. 74 Unified Services Router User Manual Figure 44: RADIUS server (External Authentication) configuration 4.

3 Creating and Using Access Points Setup > Wireless Settings > Access Points Once a profile (a group of security settings) is created, it can be assigned to an AP on the router. Each virtual AP that has a unique SSID appears as an independent access point to clients. 76 Unified Services Router User Manual Figure 46: List of configured access points (Virtual APs) shows one enabled access point on the radio, broadcasting its SSID. The clients connected to a particular AP can be viewed by using the Status Button on the List of Available Access Points. Traffic statistics are shown for the individual AP, as compared to the summary stats for each AP on the Statistics tab. Connected clients are sorted by the MAC address and indicate the security parameters used by the wireless link, as well as the time connected to this particular AP.



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)
<http://yourpdfguides.com/dref/5324200>

In clients are expected to access the LAN via this router, creating 3 VAPs will allow you to manage or shape traffic for each group of clients. In this way legacy clients can access the network without bridging down the overall throughput of more capable 802.11n clients. Since WPA2 is more secure, you may want to broadcast the SSID and not 77 Unified Services Router User Manual broadcast the SSID for the VAP with WEP since it is meant to be used for a few legacy devices in this scenario. Figure 47: Radio card configuration options The radio card is configured 802.

For example, changing the channel spacing to 40 MHz can improve bandwidth at the expense of support in earlier 802.

In clients. The available transmission channels are governed by regulatory constraints based on the region setting of the router.

Figure 48: Wi-Fi Multimedia Profile Name: This field allows you to select the available profiles in wireless settings. enable WMM: This field allows you to enable WMM to improve multimedia transmission. Default Class of Service: This field allows you to select the available Access Categories (voice, video, best effort, and background).

The inputs to this function are a PSK (configure by administrator from the WDS page) and an internal "magic" string (non-configurable). In effect the WDS links use TKIP/AES encryption, depending on the encryption configuration default AP. WDS Enable - This will enable the WDS link to use WDS encryption - Display the type of encryption used. This field in the WDS configuration radio network section displays the device's MAC address, which needs to be specified on the WDS peer for making a connection to the device (Similarly the WDS peers MAC address will have to be specified on the device for the WDS link to be established between the two devices). Personal Identification Number (PIN): The wireless device that supports WPS may have an alphanumeric PIN, if so add the PIN in this field.

82 Unified Services Router User Manual More than one AP can use WPS, but only one AP can be used to establish WPS links to client at any given time. Figure 51: WPS configuration for an AP with WPA/WPA2 profile 83 Chapter 5. Securing the Private Network You can secure your network by creating and applying rules that you router uses to selectively block and allow inbound and outbound Internet traffic. Report an alert when you want the router to send you You can, for example, establish restricted-access policies based on time-of-day, web addresses, and web address keywords. How you make your address known depends on how the WAN ports are configured; for this router you Unified Services Router User Manual may use the IP address if a static address is assigned to the WAN port, or if your WAN address is dynamic a DDNS (Dynamic DNS) name can be used. When the default outbound policy is always allow, you can't block hosts on the LAN from accessing Internet services by creating an outbound firewall rule for each service. figure 52: List of Available Firewall Rules. 2 Defining Rule Schedules Tools > Schedules Firewall rules can be enabled or disabled automatically if they are associated with a configured schedule. 3 Configuring Firewall Rules Advanced > Firewall Settings > Firewall Rules All configured firewall rules on the router are displayed in the Firewall Rules list. View the existing rules in the List of Available Firewall Rules table.

2. To edit or add an outbound or inbound services rule, do the following: Choose the From Zone to be the source of originating traffic: either the secure LAN, public DMZ, or insecure WAN. For an inbound rule WAN should be selected as the From Zone. 4. Choose the To Zone to be the destination of traffic covered by this rule. If the From Zone is the WAN, the to Zone can be the public DMZ or secure LAN. Similarly if the From Zone is the LAN, then the To Zone can be the public DMZ or insecure WAN. 5. Parameters that define the firewall rule include the following: 87 Unified Services Router User Manual Service: A NY means all traffic is affected by this rule. For a specific service the dropdown list has common services, or you can select a custom defined service. Source & Destination users: For each relevant category, select the users to which the rule applies: Inbound rules can use Destination NAT (DNAT) for managing traffic from the WAN. You can enable port forwarding for an incoming service specific rule (From Zone = WAN) by selecting the appropriate checkbox. This will allow the selected service traffic from the Internet to reach the appropriate LAN port via a port forwarding rule. If your ISP assigns you a public IP address, one of these can be used as your primary IP address on the WAN port, and the others can be assigned to servers on the LAN or DMZ. In this way the LAN/DMZ server can be accessed from the Internet by its alias public IP address.

7. Outbound rules can use Source NAT (SNAT) in order to map (bind) all LAN/DMZ traffic matching the rule parameters to a specific WAN interface or external IP address (usually provided by your ISP). Once the new modified rule parameters are saved, it appears in the master list of firewall rules. 89 Unified Services Router User Manual Figure 54: Example where an outbound SNAT rule is used to map an external IP address (209.30.90 Unified Services Router User Manual Figure 55: The firewall rule configuration page allows you to define the To/From zone, service, action, schedule, and specify source/destination IP addresses as needed. 91 Unified Services Router User Manual 5. 4 Configuring IPv6 Firewall Rules Advanced > Firewall Settings > IPv6 Firewall Rules All configured IPv6 firewall rules on the router are displayed in the Firewall Rules list. This list also indicates whether the rule is enabled (active) or not, and gives a summary of the From/To zone as well as the services or users that the rule affects.



[You're reading an excerpt. Click here to read official D-LINK](#)

[DSR-250N user guide](#)

<http://yourpdfguides.com/dref/5324200>

Figure 56 : The IPv6 fire wall rule configuration page allows you to define the To/From zone , service , action, schedule s , and specify source /destination IP address es as nee ded . In the example, CUSeeM (the video conference service used) connection s are allowed on ly from a s p ecified range of external IP addresses . If you arrange with your ISP to have more than one public IP address for your use, you can use the additional public IP addresses to map to servers on your LAN. The other addresses are available to your DMZ servers . Since we are trying to block HTTP requests, it is a service with To Zone: Insecure (WAN1/WAN2/WAN3) that is to be blocked according to schedule Weekend. 96 Unified Services Router User Manual 3. Select the Action to Block by Schedule, otherwise allow.

This will take a predefined schedule and make sure the rule is a blocking rule during the defined dates/times. All other times outside the schedule will not be affected by this firewall blocking rule. As we defined our schedule in schedule Weekend, this is available in the dropdown menu. We want to block the IP range assigned to the marketing group. Let's say they have IP 192. On the Source Users dropdown, select Address Range and add this IP range as the from and To IP addresses. 6. We want to block all HTTP traffic to any services going to the insecure zone. We don't need to change default QoS priority or Logging (unless desired) clicking apply will add this firewall rule to the list of firewall rules . 8.

The last step is to enable this firewall rule. Select the rule, and click Enable below the list to make sure the firewall rule is active. In the configuration menu you can define a range of ports and identify the traffic type (TCP/UDP/ICMP) for this service. Once defined, the new service will appear in the services list of the firewall rules configuration menu. 97 Unified Services Router User Manual Figure 59 : List of user defined services .

Figure 60 : Custom Services configuration Created services are available as options for firewall rule configuration . name: Name of the service for identification and management purposes . Type: The layer 3 Protocol that the service uses . (TCP, UDP, BOTH, ICMP or ICMPv6) Port Type: This field allows to select Port Range or Multiple Ports ICMP Type: This field is enabled when the layer 3 protocol (in the Type field) is selected as ICMP or ICMPv6. 6 ALG support Advanced > Firewall Settings > ALGs Application Level Gateways (ALGs) are security component that enhance the firewall and NAT support of the router to seamlessly support application layer protocols .

7 VPN Passthrough for Firewall Advanced > Firewall Settings > VPN Passthrough This router enables firewall settings can be configured to allow encrypted VPN traffic for IPsec, PPTP, and L2TP VPN tunnel connection s between the LAN and internet . a specific firewall rule or service is not appropriate to in route this passthrough support ; instead the appropriate check boxes in the VPN Passthrough page must be enabled . 100 Unified Services Router User Manual Figure 62 : Passthrough options for VPN tunnels . A well ports are not left open when not in use, thereby providing a level of security that port forwarding does not offer. Port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened . 101 Unified Services Router User Manual Figure 63 : List of Available Application Rule s showing 4 unique rules The application rule status page will list any active rules , i. Proxy services , which can be used to circumvent certain firewall rules and thus a potential security gap , can be blocked for all LAN devices . Java applet s can be prevented from being downloaded from internet sites , and similarly the gateway can prevent ActiveX controls from being downloaded via Internet Explorer. Forwarded security cookies , which typically contain sensitive information , can be blocked as well for all devices on the private network . 102 Unified Services Router User Manual Figure 64 : Content Filtering used to block access to proxy servers and prevent Active X controls from being downloaded .

For example, if the domain is added to this list then all of the following URLs are permitted access from the LAN: www. Export Blocked Keywords : This feature enables the user to export the keywords to be blocked to a csv file which can then be downloaded to the local host. This is IP/MAC Binding, and by enforcing the gateway to validate the source traffic's IP address with the unique MAC address of the configured LAN node , the administrator can ensure traffic from the IP address is not spoofed . The traffic's source IP address doesn't match up with the expected MAC address having the same IP address) the packets will be dropped and can be logged for diagnosis . 106 Unified Services Router User Manual Figure 68 : The following example binds a LAN host's MAC Address s to an IP address served by DSR. If there is an IP/MAC Binding violation, the violating packet will be dropped and logs will be captured . The checks can be enabled between the WAN and DMZ or LAN, and a run in conjunction will allow the administrator to see how many malicious intrusion attempts from the WAN have been detected and prevented . 12 Protecting from Internet Attacks Advanced > Advanced Network > Attack Checks Attacks can be malicious security breaches or unintentional network issues that render the router unusable. Attack checks allow you to manage WAN security such as controlling ping requests and is configured via ARP scan s . TCP and UDP flood attacks can be enabled to manage external user generated WAN responses .



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)
<http://yourpdfguides.com/dref/5324200>

A d d i t i o n a l l y c e r t a i n D e n i a l - o f - S e r v i c e (D o S) a t t a c k s c a n b e b l o c k e d . 108 Unified Services Router User Manual Figure 70 : P r o t e c t i n g t h e r o u t e r a n d L A N f r o m i n t e r n e t a t t a c k s W A N S e c u r i t y C h e c k s : E n a b l e S t e a l t h M o d e : I f S t e a l t h M o d e i s e n a b l e d , t h e r o u t e r w i l l n o t r e s p o n d t o p o r t s c a n s f r o m t h e W A N . U D P C o n n e c t i o n L i m i t : Y o u c a n s e t t h e n u m b e r o f s i m u l t a n e o u s a c t i v e U D P c o n n e c t i o n s t o b e a c c e p t e d f r o m a s i n g l e c o m p u t e r o n t h e L A N ; t h e d e f a u l t i s 25 I C S A S e t t i n g s : B l o c k I C M P N o t i f i c a t i o n : s e l e c t i n g t h i s p r e v e n t s I C M P p a c k e t s f r o m b e i n g i d e n t i f i e d a s s u c h . T h e f o l l o w i n g t y p e s o f t u n n e l s c a n b e c r e a t e d : i □ - F i g u r e 71 : E x a m p l e o f G a t e w a y - G a t e w a y I P s e c V P N t u n n e l u s i n g t w o D S R r o u t e r s c o n n e c t e d t o t h e I n t e r n e t 111 Unified Services Router User Manual Figure 72 : E x a m p l e o f t h r e e I P s e c c l i e n t c o n n e c t i o n s t o t h e i n t e r n a l n e t w o r k t h r o u g h t h e D S R I P s e c g a t e w a y 112 Unified Services Router User Manual 6 . S e l e c t t h e V P N t u n n e l t y p e t o c r e a t e i □ - S e t t h e C o n n e c t i o n N a m e a n d p r e - s h a r e d k e y : t h e c o n n e c t i o n n a m e i s u s e d f o r m a n a g e m e n t , a n d t h e p r e - s h a r e d k e y w i l l b e r e q u i r e d o n t h e V P N c l i e n t o r g a t e w a y t o e s t a b l i s h t h e t u n n e l i □ - C o n f i g u r e R e m o t e a n d L o c a l W A N a d d r e s s f o r t h e t u n n e l e n d p o i n t s i □ - R e m o t e G a t e w a y T y p e : i d e n t i f y t h e r e m o t e e n d p o i n t o f t h e t u n n e l b y F Q D N o r s t a t i c I P a d d r e s s i □ - R e m o t e W A N I P a d d r e s s / F Q D N : T h i s f i e l d i s e n a b l e d o n l y i f t h e p e e r y o u a r e t r y i n g t o c o n n e c t t o i s a G a t e w a y .

L o c a l W A N I P a d d r e s s / F Q D N : T h i s f i e l d c a n b e l e f t b l a n k i f y o u a r e n o t u s i n g a d i f f e r e n t F Q D N o r I P a d d r e s s t h a n t h e o n e s p e c i f i e d i n t h e W A N p o r t a t t a c k s c o n f i g u r a t i o n . 3 . C o n f i g u r e t h e S e c u r e C o n n e c t i o n R e m o t e A c c e s s i b i l i t y f i e l d s t o i d e n t i f y t h e r e m o t e n e t w o r k : i □ - R e v i e w t h e s e t t i n g s a n d c l i c k C o n n e c t t o e s t a b l i s h t h e t u n n e l . T h e W i z a r d w i l l c r e a t e a n A u t o I P s e c p o l i c y w i t h t h e f o l l o w i n g d e f a u l t v a l u e s f o r a V P N C l i e n t o r G a t e w a y p o l i c y (t h e s e c a n b e a c c e s s e d f r o m a l i n k o n t h e W i z a r d p a g e) : P a r a m e t e r E x c h a n g e M o d e I D T y p e L o c a l W A N I D R e m o t e W A N I D E n c r y p t i o n A l g o r i t h m A u t h e n t i c a t i o n A l g o r i t h m A u t h e n t i c a t i o n M e t h o d P F S K e y - G r o u p L i f e T i m e (P h a s e 1) L i f e T i m e (P h a s e 2) D e f a u l t v a l u e f r o m W i z a r d A g g r e s s i v e (C l i e n t p o l i c y) o r M a i n (G a t e w a y p o l i c y) F Q D N w a n _ l o c a l . O n c e t h e W i z a r d c r e a t e s t h e m a t c h i n g I K E a n d V P N p o l i c i e s r e q u i r e d b y t h e A u t o p o l i c y , o n e c a n m o d i f y t h e r e q u i r e d f i e l d s t h r o u g h t h e e d i t l i n k .

O n l y t h e d a t a p a y l o a d i s e n c r y p t e d a n d t h e I P h e a d e r i s n o t m o d i f i e d o r e n c r y p t e d . A s w e l l i n t h i s m o d e y o u c a n d e f i n e t h e s i n g l e I P a d d r e s s , r a n g e o f I P s , o r s u b n e t o n b o t h t h e l o c a l a n d r e m o t e p r i v a t e n e t w o r k s t h a t c a n c o m m u n i c a t e o v e r t h e t u n n e l . 115 Unified Services Router User Manual Figure 74 : I P s e c p o l i c y c o n f i g u r a t i o n O n c e t h e t u n n e l t y p e a n d e n d p o i n t s o f t h e t u n n e l a r e d e f i n e d y o u c a n d e t e r m i n e t h e P h a s e 1 / P h a s e 2 n e g o t i a t i o n t o u s e f o r t h e t u n n e l . T h e P h a s e 2 A u t o p o l i c y p a r a m e t e r s c o v e r t h e s e c u r i t y a s s o c i a t i o n l i f e t i m e a n d e n c r y p t i o n / a u t h e n t i c a t i o n d e t a i l s o f t h e P h a s e 2 k e y n e g o t i a t i o n . 116 Unified Services Router User Manual T h e V P N p o l i c y i s o n e h a l f o f t h e I K E / V P N p o l i c y p a i r r e q u i r e d t o e s t a b l i s h a n A u t o I P s e c V P N t u n n e l . T h e I P a d d r e s s e s o f t h e m a c h i n e o r m a c h i n e s o n t h e t w o V P N e n d p o i n t s a r e c o n f i g u r e d h e r e , a l o n g w i t h t h e p o l i c y p a r a m e t e r s r e q u i r e d t o s e c u r e t h e t u n n e l F i g u r e 75 : I P s e c p o l i c y c o n f i g u r a t i o n c o n t i n u e d (A u t o p o l i c y v i a I K E) A M a n u a l p o l i c y d o e s n o t u s e I K E a n d i n s t e a d r e l i e s o n m a n u a l k e y i n g t o e x c h a n g e a u t h e n t i c a t i o n p a r a m e t e r s b e t w e e n t h e t w o I P s e c h o s t s . t h e i n c o m i n g a n d o u t g o i n g s e c u r i t y p a r a m e t e r i n d e x (S P I) v a l u e s m u s t b e m i r r o r e d o n t h e r e m o t e t u n n e l 117 Unified Services Router User Manual e n d p o i n t . A s w e l l t h e e n c r y p t i o n a n d i n t e g r i t y a l g o r i t h m s a n d k e y s m u s t m a t c h o n t h e r e m o t e I P s e c h o s t e x a c t l y i n o r d e r f o r t h e t u n n e l t o e s t a b l i s h s u c c e s s f u l l y . N o t e t h a t u s i n g A u t o p o l i c i e s w i t h I K E a r e p r e f e r r e d a s i n s o m e I P s e c i m p l e m e n t a t i o n s t h e S P I (s e c u r i t y p a r a m e t e r i n d e x) v a l u e s r e q u i r e c o n v e r s i o n a t e a c h e n d p o i n t . R a t h e r t h a n c o n f i g u r e a u n i q u e V P N p o l i c y f o r e a c h u s e r , y o u c a n c o n f i g u r e t h e V P N g a t e w a y r o u t e r t o a u t h e n t i c a t e u s e r s f r o m a s t o r e d l i s t o f u s e r a c c o u n t s o r w i t h a n e x t e r n a l a u t h e n t i c a t i o n s e r v e r s u c h a s a R A D I U S s e r v e r .

F o r R A D I U S a t t a c k s P A P , t h e r o u t e r f i r s t c h e c k s i n t h e u s e r d a t a b a s e t o s e e i f t h e u s e r c r e d e n t i a l s a r e a v a i l a b l e ; i f t h e y a r e n o t , t h e r o u t e r c o n n e c t s t o t h e R A D I U S s e r v e r . 3 C o n f i g u r i n g V P N c l i e n t s R e m o t e V P N c l i e n t s m u s t b e c o n f i g u r e d w i t h t h e s a m e V P N p o l i c y p a r a m e t e r s u s e d i n t h e V P N t u n n e l t h a t t h e c l i e n t w i s h e s t o u s e : e n c r y p t i o n , a u t h e n t i c a t i o n , l i f e t i m e , a n d P F S k e y - g r o u p . O p e n s o u r c e s o f t w a r e (s u c h a s O p e n V P N o r O p e n s w a n) a s w e l l a s M i c r o s o f t I P s e c V P N s o f t w a r e c a n b e c o n f i g u r e d w i t h t h e r e q u i r e d I K E p o l i c y p a r a m e t e r s t o e s t a b l i s h a n I P s e c V P N t u n n e l . T h e r o u t e r a c t s a s a b r o k e r d e v i c e t o a l l o w t h e I S P ' s s e r v e r t o c r e a t e a T C P c o n t r o l c o n n e c t i o n b e t w e e n t h e L A N V P N c l i e n t a n d t h e V P N s e r v e r . O n c e t h e P P T P s e r v e r i s e n a b l e d , P P T P c l i e n t s t h a t a r e w i t h i n t h e r a n g e o f c o n f i g u r e d I P a d d r e s s e s o f a l l o w e d c l i e n t s c a n r e a c h t h e r o u t e r a t t h e P P T P s e r v e r . O n c e t h e L 2 T P s e r v e r i s e n a b l e d , L 2 T P c l i e n t s t h a t a r e w i t h i n t h e r a n g e o f c o n f i g u r e d I P a d d r e s s e s o f a l l o w e d c l i e n t s c a n r e a c h t h e r o u t e r a t t h e L 2 T P s e r v e r . 3 O p e n V P N S u p p o r t S e t u p > V P N S e t t i n g s > O p e n V P N > O p e n V P N C o n f i g u r a t i o n O p e n V P N a l l o w s p e e r s t o a u t h e n t i c a t e e a c h o t h e r u s i n g a p r e - s h a r e d s e c r e t k e y , c e r t i f i c a t e s , o r u s e r n a m e / p a s s w o r d . E n c r y p t i o n A l g o r i t h m : T h e c i p h e r w i t h w h i c h t h e p a c k e t s a r e e n c r y p t e d . C a n b e c h e c k e d o n l y w h e n t h e t l s k e y i s u p l o a d e d . T h e r o u t e r s u p p o r t s m u l t i p l e c o n c u r r e n t s e s s i o n s t o a l l o w r e m o t e u s e r s t o a c c e s s t h e L A N o v e r a n e n c r y p t e d l i n k t h r o u g h a c u s t o m i z a b l e u s e r p o r t a l i n t e r f a c e , a n d e a c h S S L V P N u s e r c a n b e a s s i g n e d u n i q u e p r i v i l e g e s a n d n e t w o r k r e s o u r c e a c c e s s l e v e l s .



[You're reading an excerpt. Click here to read official D-LINK](http://yourpdfguides.com/dref/5324200)

[DSR-250N user guide](http://yourpdfguides.com/dref/5324200)

<http://yourpdfguides.com/dref/5324200>

The remote user can be provided different options for SSL service through the router: Onces established, the host machine can access allocated network resources. The router administrator can define specific services or applications that are available to remote port forward in groups in standard of access to the full LAN like the VPN tunnel. Figure 85: List of groups Group configuration page allows to create a group with a different type of users. PPTP User: These are PPTP VPN tunnel LAN users that can establish a tunnel with the PPTP server on the WAN. L2TP User: These are L2TP VPN tunnel LAN users that can establish a tunnel with the L2TP server on the WAN.

Figure 86: User group configuration When SSLVPN users are selected, the SSLVPN settings are displayed with the following parameters as captured in SSLVPN Settings. If there are multiple workers, user can enter the details for up to two workers. IDA Base DN: This is the base domain name for the LDAP authentication server. If there are multiple LDAP authentication servers, user can enter the details for up to two LDAP Base DN. If there are multiple Active Directory domains, user can enter the details for up to two authentication domains.

The following parameters are configured: User Manual Disable Login: Enable to prevent the users of this group from logging in to the devices management interface(s). Deny Login from WAN interface: Enable to prevent the users of this group from logging in from a WAN (wide area network) interface. The following parameters are configured: Defined Broswers: This list displays the web browsers that have been added to the Defined Broswers list, upon which group policies can be defined. You can add to the list of Defined Broswers by selecting a client browser from the dropdown menu and clicking Add. The following parameters are configured: Defined Broswers: This list displays the web browsers that have been added to the Defined Broswers list, upon which group policies can be defined. You can add to the list of Defined Broswers by selecting a client browser from the dropdown menu and clicking Add. The list of available users are displayed in the List of Users page with User name, associated group and Login status. Click Delete to clear an existing user 136 Unified Services Router User Manual Figure 91: Available Users with login status and associated Group 7. The user set in group contains the following key components: The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global). Based on the selection of one of the above options, the appropriate configuration fields are required (i.e. As well the policy can be specified for one or all of the supported SSL VPN services).

The policy name, SSL service it applies to, destination (network resource or IP addresses) and permission (deny/permit) is outlined in a list of configuration policies for the router. Network resources are created with the following information Permission: The assigned resources defined by this policy can be explicitly permitted or denied. 1 Using Network Resources Setup > VPN Settings > SSL VPN Server > Resources Network resources are services or groups of LAN IP addresses that are used to easily create and configure SSL VPN policies. A network resource can be defined by configuring the following in the GUI: The table below lists some common applications and corresponding TCP port numbers: TCP Application FTP Data (usually not needed) FTP Control Protocol SSH Telnet SMTP (send mail) HTTP (web) POP3 (receive mail) NTP (network time protocol) Citrix Terminal Services VNC (virtual network computing) Port Number 20 21 22 23 25 80 110 123 1494 3389 5900 or 5800 142 Unified Services Router User Manual As a convenience for remote users, the host name (FQDN) of the network server can be configured to allow for IP address resolution. This host name resolution provides users with easy-to-remember FQDNs to access TCP application in standard of ferro prone IP addresses when using the Port Forwarding service through the SSL User Portal. To configure port forwarding, following are required: Allow users to access the private network servers by using a host name instead of an IP address, the FQDN corresponds to the IP address defined in the port forwarding host configuration selection. The client routes give the SSL client access to specific private networks, thereby allowing access control over specific LAN services. Client level configuration supports the following: Enable Split Tunnel Support: With a split tunnel, only resources which are referenced by client routes can be accessed over the VPN tunnel. With full tunnel support (if the split tunnel option is disabled the DSR acts in full tunnel mode) all addresses on the private network are accessible over the VPN tunnel. As well as static routes on the private LANs firewall (typically through the router) is needed to forward private traffic through the VPN Firewall to the remote SSL VPN client.

Figure 98: Configured client routes only apply in split tunnel mode Steps to Install / Uninstall SSL VPN tunnel in MAC OS 1. The configured portal can be associated with an authentication domain 7. There are various fields in the portal that are customizable for the domain, and this allows the router administrator to create and edit such as logging instructions, available services, and other user age and details in the portal visible to remote users.



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)
<http://yourpdfguides.com/dref/5324200>

Du rin g d o main s etup , co nfig u red p o r t al lay o u t s are av ailab le t o s elect fo r all u sers au th en t icat ed b y th e d o main . A s well , th e u sers as s ign ed t o th is p o r t al (th ro u g h th e ir au th en t icat io n d o main) can b e p resen t w it h o n e o r m o re o f th e ro u t e r s u p p o r t e d SSL s e r v ic e s s u c h a s th e VPN Tu n n e l p a g e o r P o r t F o r w a r d in g p a g e .

To co nfig u r e a p o r t al lay o u t an d th e m e , fo llo win g in fo r m at io n is n e e d e d : i n - P o r t al s it e t it le : Th e p o r t al w e b b r o w s e r w in d o w t it le t h at ap p e a r s w h e n th e clien t acc e s s e s th is p o r t al . D is p la y b a n n e r m e s s a g e o n th e lo g in p a g e : Th e u s e r h a s th e o p t io n t o e it h e r d is p la y o r h id e th e b a n n e r m e s s a g e in th e lo g in p a g e . A c t iv e X w e b c a c h e c l e a n e r : A n A c t iv e X c a c h e c o n t r o l w e b c l e a n e r c a n b e p u s h e d f r o m th e g a t e w a y t o th e clien t b r o w s e r w h e n e v e r u s e r s lo g in t o th is SSL VPN p o r t al . SSL VPN p o r t al p a g e t o d is p la y : Th e U s e r c a n e it h e r e n a b l e VPN t u n n e l p a g e o r P o r t F o r w a r d in g , o r b o t h d e p e n d in g o n th e SSL s e r v ic e s t o d is p la y o n th is p o r t al . O n c e th e p o r t al s e t t in g s a r e co nfig u r e d , th e n e w ly co nfig u r e d p o r t al is a d d e d t o th e lis t o f p o r t al lay o u t s .

USB M a s S t o r a g e : a l s o r e f e r r e d t o a s a h a r e p o r t a t t a c h e d , f i l e s o n a USB d i s k c o n n e c t e d t o th e D S R c a n b e a c c e s s e d b y L A N u s e r s a s a n e t w o r k d r i v e . S e l e c t th e ' C o n n e c t t o p r i n t e r u s i n g U R L ' r a d i o b u t t o n (' S e l e c t a s h a r e d p r i n t e r b y n a m e ' i n c a s e o f W i n d o w s 7) a n d g i v e th e fo llo win g U R L h t t p : / / < R o u t e r ' s L A N I P a d d r e s s > : 6 3 1 / p r i n t e r s / < M o d e l N a m e > (M o d e l N a m e c a n b e f o u n d in th e USB s e t t in g s p a g e o f r o u t e r ' s G U I) . Th e USB p r i n t e r c a n b e a c c e s s e d o n a n y L A N h o s t (w it h a p p r o p r i a t e p r i n t e r d r i v e r in s t a l l e d) c o n n e c t e d t o th e r o u t e r b y u s i n g th e fo llo win g co m m a n d in th e h o s t ' s a d d p r i n t e r s w in d o w h t t p : / / < R o u t e r ' s I P : 6 3 1 > / p r i n t e r s / < D e v ic e M o d e l > (D e v ic e M o d e l c a n b e f o u n d in th e USB s e t t in g s p a g e) . Th e USB p r i n t e r c a n b e a c c e s s e d o n a n y L A N h o s t (w it h a p p r o p r i a t e p r i n t e r d r i v e r in s t a l l e d) c o n n e c t e d t o th e r o u t e r b y u s i n g th e fo llo win g co m m a n d in th e h o s t ' s a d d p r i n t e r s w in d o w h t t p : / / < R o u t e r ' s I P : 6 3 1 > / p r i n t e r s / < D e v ic e M o d e l > (D e v ic e M o d e l c a n b e f o u n d in th e USB s e t t in g s p a g e) . Th e r e c e iv e d m e s s a g e s c a n b e s e e n in th e I n b o x a n d a l l o w s th e u s e r t o c r e a t e a n e w S M S . i f W A N 3 is u s e d in d e d ic a t e d w a n m o d e , lo a d b a l a n c in g m o d e o r i f 3 G USB D e v ic e is n o t c o n n e c t e d t o r o u t e r t h e n th e c o n t r o l s o n th is p a g e w ill b e g r e y e d o u t . F ig u r e 1 0 3 : S M S S e r v ic e S e n d S M S Th e fo llo win g d e t a il s a r e d is p la y e d in S M S I N B O X p a g e : i n - T im e S t a m p : D is p la y s th e t im e w h e n th e m e s s a g e w a s s e n t T e x t : D is p la y s th e c o n t e n t o f th e p a r t ic u l a r M e s s a g e . Th e fo llo win g a c t io n s a r e p e r f o r m e d : D e l e t e : D e l e t e s th e S M S h a v in g th a t p a r t ic u l a r S n o . Th e fo llo win g c e r t if ic a t e d a t a is d is p la y e d in th e lis t o f T r u s t e d (C A) c e r t if ic a t e s : C A I d e n t it y (S u b j e c t N a m e) : Th e c e r t if ic a t e is is s u e d t o th is p e r s o n o r o r g a n iz a t io n I s s u e r N a m e : Th is is th e C A n a m e th a t is s u e d th is c e r t if ic a t e E x p ir y T im e : Th e d a t e a f t e r w h ic h th is T r u s t e d c e r t if ic a t e b e c o m e s in v a l id A s e l f c e r t if ic a t e is a c e r t if ic a t e is s u e d b y a C A id e n t if y in g y o u r d e v ic e (o r s e l f s i g n e d i f y o u d o n a t t a n t w a n t th e id e n t it y p r o t e c t io n o f a C A) . th e A c t iv e S e l f C e r t if ic a t e 1 5 4 U n if i e d S e r v ic e s R o u t e r U s e r M a n u a l t a b l e lis t th e s e l f c e r t if ic a t e s c u r r e n t ly lo a d e d o n th e g a t e w a y .

Th e fo llo win g in fo r m at io n is d is p la y e d fo r e a c h u p lo a d e d s e l f c e r t if ic a t e : i n - Th is is h o u l d b e y o u r o f f ic i a l r e g is t e r e d o r c o m p a n y n a m e , a s I P s e c o r SSL VPN p e e r s a r e s h o w n th is f i e l d . T o r e q u e s t a s e l f c e r t if ic a t e t o b e s i g n e d b y a C A , y o u c a n g e n e r a t e a C e r t if ic a t e S i g n in g R e q u e s t f r o m th e g a t e w a y b y e n t e r in g id e n t if ic a t io n p a r a m e t e r s a n d p a s s in g it a l o n g t o th e C A f o r s i g n in g . O n c e s i g n e d , th e C A h e r e a f t e r T r u s t e d C e r t if ic a t e a n d s i g n e d c e r t if ic a t e f r o m th e C A a r e u p lo a d e d t o a c t iv a t e th e s e l f - c e r t if ic a t e v a l id a t in g th e id e n t it y o f th is g a t e w a y . th e s e l f c e r t if ic a t e is th e n u s e d in I P s e c a n d SSL c o n n e c t io n s w it h p e e r s t o v a l id a t e th e g a t e w a y a u t h e n t ic it y . F ig u r e 1 0 5 : C e r t if ic a t e s u m m a r y fo r I P s e c a n d H T T P S m a n a g e m e n t 1 5 5 U n if i e d S e r v ic e s R o u t e r U s e r M a n u a l 8 . Th e r o u t e r a d m in is t r a t o r c a n d e f in e a k n o w n P C , s in g l e IP a d d r e s s o r r a n g e o f IP a d d r e s s e s th a t a r e a l l o w e d t o a c c e s s th e G U I w it h H T T P S . W h e n a n e x t e r n a l S N M P m a n a g e r is p r o v id e d w it h th is r o u t e r a t t a c h e d M a n a g e m e n t I n f o r m at io n B a s e (M I B) f i l e , th e m a n a g e r c a n u p d a t e th e r o u t e r h i e r a r c h a l v a r i a b l e s t o v i e w o r u p d a t e c o nfig u r a t io n p a r a m e t e r s . th e r o u t e r a s a m a n a g e d d e v ic e h a s a n S N M P a g e n t th a t a l l o w s th e M I B c o nfig u r a t io n v a r i a b l e s t o b e a c c e s s e d b y th e M a s t e r (th e S N M P m a n a g e r) . Th e A c c e s s C o n t r o l L is t o n th e r o u t e r id e n t if ic a t i o n m a n a g e r s in th e n e t w o r k th a t h a v e r e a d o n ly o r r e a d - w r it e S N M P c r e d e n t i a l s . S e l e c t th e r o u t e r ' s t im e z o n e , r e l a t iv e t o G r e e n w ic h M e a n T im e (G M T) .

D e t e r m in e w h e t h e r t o u s e d e f a u l t o r c u s t o m N e t w o r k T im e P r o t o c o l (N T P) s e r v e r s . A s a n a d m in is t r a t o r y o u c a n m o n it o r th e t y p e o f t r a f f ic th a t g o e s th r o u g h th e r o u t e r a n d a l s o b e n o t if ic e d o f p o t e n t i a l a t t a c k s o r e r r o r s w h e n th e y a r e d e t e c t e d b y th e r o u t e r . Th e fo llo win g s e c t io n s d e s c r ib e th e lo g c o nfig u r a t io n s e t t in g s a n d th e w a y s y o u c a n a c c e s s th e s e lo g s . F o r e a c h f a c i l i t y , th e fo llo win g e v e n t s (in o r d e r o f s e v e r it y) c a n b e lo g g e d : E m e r g e n c y , A l e r t , C r it ic a l , E r r o r , W a r n in g , N o t if ic a t io n , I n f o r m at io n , D e b u g g in g . E M E R G E N C Y : s y s t e m is u n u s a b l e A L E R T : a c t io n m u s t b e t a k e n im m e d i a t e l y C R I T I C A L : c r it ic a l c o n d it io n s E R R O R : e r r o r c o n d it io n s W A R N I N G : w a r n in g c o n d it io n s N O T I F I C A T I O N : n o r m a l b u t s i g n if ic a n t c o n d it io n I N F O R M A T I O N : in f o r m at io n a l D E B U G G I N G : d e b u g - l e v e l m e s s a g e s 1 6 3 U n if i e d S e r v ic e s R o u t e r U s e r M a n u a l F ig u r e 1 1 3 : F a c i l i t y s e t t in g s fo r L o g g in g Th e d is p la y fo r lo g g in g c a n b e c u s t o m iz e d b a s e d o n w h e r e th e lo g s a r e s e n t , e it h e r th e E v e n t L o g v i e w e r in th e G U I (th e E v e n t L o g v i e w e r is in th e S t a t u s > L o g s p a g e) o r a r e m o t e S y s lo g s e r v e r fo r l a t e r r e v i e w .



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)

Denial of service attacks, general attack information, logging attempts, dropped packets, and similar events can be captured for review by the IT administrator. Traffic through each network segment (LAN, WAN, DMZ) can be tracked based on whether the packet was accepted or dropped by the firewall. Accepted packets are those that were successfully transferred through the coresponding network segments. In addition to network segments logging, unicast and multicast traffic can be logged.

165 Unified Services Router User Manual Figure 114: Log configuration options for traffic through route r Tools > Log Settings > IPv6 logging This page allows you to configure the IPv6 logging. 166 Unified Services Router User Manual Figure 115: IPv6 Log configuration options for traffic through route r. For remote logging a key configuration field is the Remote Log Identifier. The SMTP port and return e-mail addresses are required field to allow the router to package the logs and send a valid e-mail that is accepted by one of the configured addresses. Up to three e-mail addresses can be configured as log recipients. In order to establish a connection with the configured SMTP port and server, define the server address as word at a table server. authentication can be disabled if the server does not have the required authentication. In some cases the SMTP server may send out IDENT requests, and this is router can have this response option enabled. On the e-mail server and recipient details are defined you can determine when the router should end output logs. This remote device typically has less memory constraints than the local Event Viewer on the router GUI, and thus can collect a considerable number of logs over a sustained period.

To enable a Syslog server select the checkbox next to an empty Syslog server field and assign the IP address or FQDN to the Name field. The selected facility and severity levels messages will be 168 Unified Services Router User Manual server to the configured (enabled) Syslog server once you save the configuration in page 169. Figure 117: Syslog server configuration for Remote Logging (continued) 9. When ever traffic through the router materializes the settings determined in the Tools > Log Settings > Logs Facility or Tools > Log Settings > Logs Configuration pages, the corresponding log messages will be displayed in this window with a timestamp. 5 Backing up and Restoring Configuration Settings Tools > System You can backup the router GUI configuration settings to a different device or the same router after some other changes. On the LEDs are turned off, wait a few more seconds before doing anything in the router. For backing up configuration or restoring a previous saved configuration, please follow the steps below:

1. To save a copy of your current settings, click the Backup button in the Save Current Settings option. The browser initiates an export of the configuration file and prompts to save the file on your host. 170 Unified Services Router User Manual 2.

To restore your saved settings from a backup file, click Browse then locate the file on the host. After clicking Restore, the router begins importing the file saved configuration settings. After the restore, the router reboots automatically with the restored settings. 3. To erase your current settings and revert to factory default settings, click the Default button.

The router will then restore configuration settings to factory defaults and will reboot automatically. (See Appendix B for the factory default parameters for the router). Figure 119: Restoring configuration from a saved file will result in the current configuration being overwritten and a reboot. However, all user data as well as saved away when users download firmware from 1. 7 Upgrading Router Firmware via USB Tools > Firmware via USB This page allows user to upgrade the firmware, backup and restore the settings using a USB storage key.

Each configured WAN can have a different DDNS service if required. On the configured, the router will update the DDNS services changes in the WAN IP address so that at feature that are dependent on access in the router GUI WAN via FQDN will be directed to the correct IP address. When you save the configuration with a DDNS service, the host and domain name, username, password and wildcard support will be provided by the account provider. 1 Ping This utility can be used to test connectivity between the router and another device on the network or connected to the router. 4 Router Options This static and dynamic routes configured on the router can be shown by clicking Display for the corresponding router in the table. The settings for the wired and wireless interfaces are displayed in the DSR Status page, and the resulting hardware resource and router usage details are summarized on the router GUI Dashboard. The radio band and channel settings are presented below along with all configured and active APs that are enabled on the router. 1 Wired Port Statistics Status > Traffic Monitor > Device Statistics Detailed transmission and receive statistics for each physical port are presented here. each interface (WAN1, WAN2/DMZ, LAN, and VLANs) have port specific packet level information provided for review. Transmission/received packets, port collisions, and the cumulative bytes/seconds for transmission/reception are provided for each interface along with the port uptime.



[You're reading an excerpt. Click here to read official D-LINK DSR-250N user guide](http://yourpdfguides.com/dref/5324200)