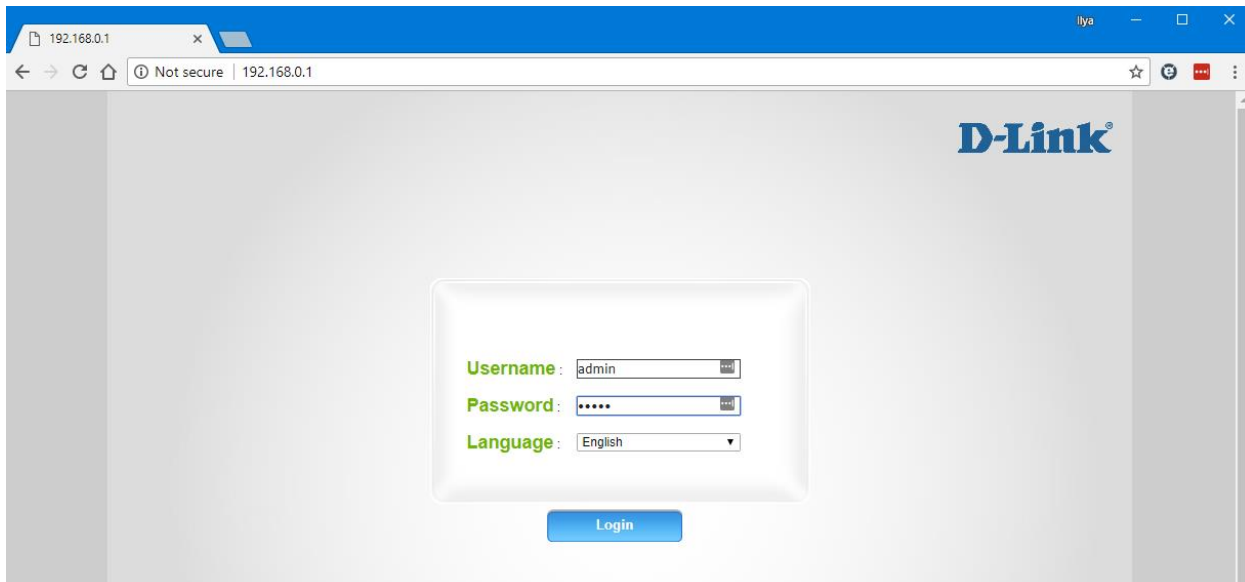


DWM-312

Firmware V01.00.1.019

192.168.0.1 admin/admin



192.168.0.1

Not secure | 192.168.0.1

D-Link

Username : admin

Password :

Language : English

Login



D-Link
DWM-312

Home Internet LAN VPN Advanced System Logout

INTERNET

Connection Time: 00:03:54
IP Address: 10.101.88.25
Subnet Mask: 255.255.255.252
DNS Server 1: 10.4.58.204
DNS Server 2: 10.5.136.242

CELLULAR

SIMA
Service State: 4G
Carrier Name: Telstra Mobile
Disconnect

INFO

System Name: DWM-312
System Uptime: 11:20:14 up 7 min
HW Version: A1
SW Version: V01.00.1.019
Device Mode: Router Mode

LAN

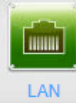
Subnet Mask: 255.255.255.0
DHCP Pool: 10 ~ 20



Home



Internet



LAN



VPN



Advanced



System

Logout

■ **WAN Service**

- SIMA
- SIMB
- Device Mode
- Router Mode

Preferred SIM Card

Preferred SIM Card

SIMA First;SIMB Backup ▾

Switch Time : 5 (5~1440 minutes)

Apply

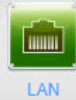
Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

■ **WAN Service**

- SIMA
- SIMB
- Device Mode
- Router Mode

Preferred SIM Card

Preferred SIM Card

SIMA First;SIMB Backup ▾
SIMA First;SIMB Backup
SIMB First;SIMA Backup
SIMA Only
SIMB Only

(5~1440 minutes)

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

Network Status

Network Provider	Telstra Mobile
Network Type	LTE
Connection Time	00:04:52
Signal Strength	100 %
IP Type	IPv4
Total DL	28711 (Bytes)
Total UL	37748 (Bytes)
Profile Name	telstra.internet

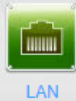
Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

SIMA

APN Settings

Dial-Up Profile	☐ Auto-Detection ☒ Manual ☐ Selection
Country	Australia
Telecom	Telstra
Username	(optional)
Password	(optional)
Dialed Number	*99#
Authentication	Auto
APN	telstra.internet (optional)
PIN Code	(optional)
Primary DNS Server	
Secondary DNS Server	

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

SIMA

APN Settings

Dial-Up Profile

☐ Auto-Detection ☒ Manual ☐ Selection

Country

Australia

Telecom

Telstra

Username

3 AU

(optional)

AAPT

Amaysim

(optional)

Bigpond

BLINK

Crazy Johns

Dodo

Exetel

(optional)

iiNet

(optional)

Internode

iPrimus

Telstra

TPG Mobile

VirginBroadband

Vodafone AU

YesOptus

Others

Dialed Number

Authentication

APN

PIN Code

Primary DNS Server

Secondary DNS Server

Apply

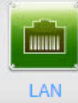
Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

SIMA

APN Settings

Dial-Up Profile	☐ Auto-Detection ☒ Manual ☐ Selection	
Country	New Zealand ▼	
Telecom	2 Degrees ▼	
Username	2 Degrees	(optional)
Password	Call Plus	(optional)
Dialed Number	Orcon	
Authentication	Spark Mobile	
APN	Vodafone NZ	
PIN Code	Others	
Primary DNS Server	internet	(optional)
Secondary DNS Server		(optional)

Apply

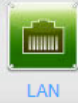
Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

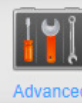
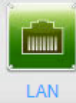
SIMA

APN Settings

Dial-Up Profile	☒ Auto-Detection ☐ Manual ☐ Selection	
Authentication	Auto ▼	
PIN Code	Auto	(optional)
Primary DNS Server	PAP	
Secondary DNS Server	CHAP	

Apply

Refresh



- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

SIMA

APN Settings

Dial-Up Profile

☐ Auto-Detection ☐ Manual ☒ Selection

Apply

Refresh



- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

APN Configuration

SIMA APN Profile List

Item	Profile Name	APN	Priority	Actions
------	--------------	-----	----------	---------

Add New APN

Delete

APN Configuration



Profile Name	Profile-1	
APN		
PIN Code		(Optional)
User Name		(Optional)
Password		(Optional)
Priority		
Authentication	Auto Auto PAP CHAP	

Save

Undo

D-Link®
DWM-312



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings**
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

Connection Settings

Prefer Service Type	Auto Mode
Allow Data Roaming	☐ Enable
Reconnect Mode	☒ Always ☐ Manual ☐ Connect-on-demand
Maximum Idle Time	600 seconds
IP Type	IPv4

Apply

Refresh

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

Connection Settings

Prefer Service Type Auto Mode ▾
Allow Data Roaming ☐ ☒ Connect-on-demand
Reconnect Mode ☐ ☒ ☐ ☐
Maximum Idle Time 0000 seconds
IP Type IPv4 ▾

Apply

Refresh

D-Link®
DWM-312



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- SIMB
- Device Mode
- Router Mode

SIM Card Settings

PIN Code Request function

SIM Status

PIN Code Request function

Input SIM PIN Code

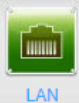
SIMA

☒ Disable ☐ Enable

Apply

Refresh

Warning : 3 more tries allowed.



- WAN Service
- SIMA
 - Network Status
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info**
- SIMB
- Device Mode
- Router Mode

WAN IPv4 And IPv6 Address Info

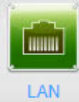
IPv4

IP Address	10.100.51.213
Subnet Mask	255.255.255.252
Gateway	10.100.51.214
DNS Server1	10.4.58.204
DNS Server2	10.5.136.242

IPv6

IP Address	13
Gateway	0000:0000:0000:0000:0000:0000:0000:0000
DNS Server1	0000:0000:0000:0000:0000:0000:0000:0000
DNS Server2	0000:0000:0000:0000:0000:0000:0000:0000

Refresh



- WAN Service
- SIMA
- SIMB
 - Network Status**
 - APN Settings
 - APN Configuration
 - Connection Settings
 - SIM Card Settings
 - IPv4 and IPv6 info
- Device Mode
- Router Mode

Network Status

Network Provider	N/A
Network Type	N/A
Connection Time	N/A
Signal Strength	N/A
IP Type	N/A
Total DL	N/A
Total UL	N/A
Profile Name	N/A

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
- SIMB
- **Device Mode**
- Router Mode

Device Mode

Device Mode

☒ Router Mode ☐ Bridge Mode

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- WAN Service
- SIMA
- SIMB
- Device Mode
- **Router Mode**

Router Mode

NAT

☒ NAT ☐ Classical

Keep Alive for WAN Access

☒ Enable

☐ DNS Query ☒ ICMP Checking

☐ Check Incoming / Outgoing Packet

Check Interval

Fail Threshold

Target1

Target2

Apply

Refresh

- WAN Service
- SIMA
- SIMB
- Device Mode
- Router Mode

Router Mode

NAT

☒ NAT ☐ Classical

Keep Alive for WAN Access

☒ Enable

☐ DNS Query

☒ ICMP Checking

☐ Check Incoming / Outgoing Packet

Check Interval

60 seconds

Fail Threshold

60 seconds

Target1

DNS1

Target2

None

Apply

Refresh

- WAN Service
- SIMA
- SIMB
- Device Mode
- Router Mode

Router Mode

NAT

☒ NAT ☐ Classical

Keep Alive for WAN Access

☒ Enable

☐ DNS Query

☒ ICMP Checking

☐ Check Incoming / Outgoing Packet

Check Interval

60 seconds

Fail Threshold

5 times

Target1

5 times

Target2

10 times

Apply

Refresh

- WAN Service
- SIMA
- SIMB
- Device Mode
- Router Mode

Router Mode

NAT

☒ NAT ☐ Classical

Keep Alive for WAN Access

☒ Enable

☐ DNS Query ☒ ICMP Checking

☐ Check Incoming / Outgoing Packet

Check Interval

Fail Threshold

Target1

Target2

DNS2

Other Host

NTP Server

Apply

Refresh

D-Link®
DWM-312



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPv4
 - LAN Settings
 - DHCP
- IPv6

LAN Settings

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

IP Interface Configuration

Router IP Address

Default Subnet Mask

Local Domain Name

Dynamic Route

LAN Snooping

Apply

Refresh

Dynamic Route

RIP : ☐ Enable ☐ RIP1 ☐ RIP2

Save

to change any of the settings here to get your network up

LAN Snooping

LAN Snooping :

☐ Enable

Save

D-Link®

DWM-312

Home

Internet

LAN

VPN

Advanced

System

Logout

■ IPv4

-LAN Settings

-DHCP

■ IPv6

DHCP

DHCP Server Configuration

Enable DHCP Server :☒

DHCP IP Address Range

10

to

20

(addresses within the LAN subnet)

DHCP Lease Time :

604800

(seconds)

Primary DNS IP Address

Secondary DNS IP Address

Static IP setting

ApplyRefresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPv4
 - LAN Settings
 - DHCP
- IPv6

Static IP Setting

DHCP clients -- Select one --

Copy to

ID -- ▾

ID	MAC Address	IP Address	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐

Previous page

Next page

Back

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPv4
- IPv6
 - IPv6 Config
 - Internet Connection type

IPv6 Config

IPv6 :

☐ Disabled ☒ Enable

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPv4
- IPv6
 - IPv6 Config

[-Internet Connection type](#)

Internet Connection Type

LAN Assigned Type :

SLAAC+RDNSS
DHCPv6
SLAAC+Stateless DHCP
SLAAC+RDNSS

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPsec
 - VPN Settings
 - XAUTH Account
- PPTP
- L2TP
- GRE

VPN Settings

VPN Settings

VPN-IPSEC : ☐ Enabled

Netbios over IPSEC : ☐ Enabled

NAT Traversal : ☒ Enabled

Dynamic VPN Setting

VPN Dynamic IP Setting : ☐ Enable [More](#)

Tunnel Settings

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1					More	☐
2					More	☐
3					More	☐
4					More	☐
5					More	☐

Apply

Refresh

■ IPsec

-VPN Settings

-XAUTH Account

■ PPTP

■ L2TP

■ GRE

VPN Dynamic IP Setting

☐ Enabled

Tunnel Name :

Local Subnet :

Local Netmask :

Phase1 Key Life Time : seconds

Phase2 Key Life Time : seconds

Encapsulation Protocol :

PFS Group :

Aggressive Mode : ☐ Enable

Preshare Key :

Local ID : Type: ID:

Dead Peer Detection (DPD) : ☐ Enable

▶ Timeout : Second(s)

▶ Delay : Second(s)

XAUTH : ☒ None ☐ Server

Set IKE Proposal : ☐ Enable

Set IPSEC Proposal : ☐ Enable

IKE Proposal Settings

ID	Encryption	Authentication	DH Group	Enable
1	DES	SHA1	Group1	☐
2	DES	SHA1	Group1	☐

IPSEC Proposal Settings

ID	Encryption	Authentication	Enable
1	DES	SHA1	☐
2	DES	SHA1	☐

Apply

Refresh

Back

- IPsec
 - VPN Settings
 - XAUTH Account
- PPTP
- L2TP
- GRE

VPN Settings

VPN Settings - Tunnel 1

☐ Enabled

Tunnel Name :

Method :

IKE ▾

Local Subnet :

Local Netmask :

Remote Subnet :

Remote Netmask :

Remote Gateway :

Phase1 Key Life Time :

seconds

Phase2 Key Life Time :

seconds

Encapsulation Protocol :

ESP ▾

PFS Group :

Disable ▾

Aggressive Mode :

☐ Enable

Preshare Key :

Connecting Type :

Always on ▾

Remote ID :

Type: Username ▾
ID:

Local ID :

Type: Username ▾
ID:

Dead Peer Detection (DPD) :

☐ Enable

▶ Timeout :

180

Second(s)

▶ Delay :

30

Second(s)

XAUTH :

☒ None

☐ Server

☐ Client

▶ Username :

▶ Password :

Set IKE Proposal :

☐ Enable

Set IPSEC Proposal :

☐ Enable

IKE Proposal Settings

ID	Encryption	Authentication	DH Group	Enable
1	DES ▾	SHA1 ▾	Group1 ▾	☐
2	DES ▾	SHA1 ▾	Group1 ▾	☐



Home



Internet



LAN



VPN



Advanced



System

Logout

■ IPsec

-VPN Settings

-XAUTH Account

■ PPTP

■ L2TP

■ GRE

XAUTH Account

No.	Username	Password
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Apply

Refresh



- IPsec
- PPTP
 - PPTP Server
 - PPTP Client
- L2TP
- GRE

PPTP Server

Server Setup

Server Setup : ☒ Enable

Server Configuration

Authentication Type : ☐ PAP ☐ CHAP ☐ MS_CHAP ☐ MS_CHAPv2

Server virtual IP :

IP Pool Start Address :

IP Pool End Address :

Encryption : ☐ Enable

Encryption Length : ☐ 40 bits ☐ 56 bits ☐ 128 bits

User Account Setting

ID	User Name	Password
1		
2		
3		
4		
5		

Connection Status

User Name	Peer IP	Virtual IP	Peer Call ID	Operation
-----------	---------	------------	--------------	-----------

No connection from remote

Apply

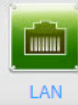
Refresh



Home



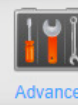
Internet



LAN



VPN



Advanced



System

Logout

- IPsec
- PPTP
 - PPTP Server
 - PPTP Client
- L2TP
- GRE

PPTP Client

Client Setup

VPN-PPTP Client : ☒ Enable

User Account Setting

ID	Name	Peer IP/Domain	User Name	Password	Route	Connect	Option	Enable
1						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
2						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
3						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
4						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
5						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐

Connection Status

ID	Tunnel Name	Virtual IP	Remote IP	Status
----	-------------	------------	-----------	--------



- IPsec
- PPTP
- L2TP
 - L2TP Server
 - L2TP Client
- GRE

L2TP Server

Server Setup

VPN-L2TP Server :

☒ Enable

Server Configuration

Authentication Type :

☐ PAP ☐ CHAP ☐ MS_CHAP ☐ MS_CHAPv2

Server virtual IP :

192.168.10.1

IP Pool Start Address :

10

IP Pool End Address :

17

Encryption :

☐ Enable

Encryption Length :

☐ 40 bits ☐ 56 bits ☐ 128 bits

User Account Setting

ID	User Name	Password
1		
2		
3		
4		
5		

Connection Status

User Name	Peer IP	Virtual IP	Peer Call ID	Operation
-----------	---------	------------	--------------	-----------

No connection from remote



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPsec
- PPTP
- L2TP
 - L2TP Server
 - L2TP Client
- GRE

L2TP Client

Client Setup

VPN-L2TP Client :

☒ Enable

User Account Setting

ID	Name	Peer IP/Domain	User Name	Password	Route	Connect	Option	Enable
1						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
2						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
3						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
4						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐
5						☒ On demand ☐ Auto ☐ Manual	☐ MPPE ☐ NAT	☐

Connection Status

ID	Tunnel Name	Virtual IP	Remote IP	Status
----	-------------	------------	-----------	--------



Home



Internet



LAN



VPN



Advanced



System

Logout

- IPsec
- PPTP
- L2TP
- **GRE**

GRE Tunnel

ID	Name	Tunnel IP	Peer IP	Key	TTL	Subnet	Enable
1							☐
2							☐
3							☐
4							☐
5							☐
6							☐
7							☐
8							☐

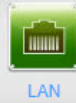
Default Gateway None ▼

Tunnels information

ID	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Apply

Refresh



■ DNS

-DNS

-DNS Redirect

■ Firewall

■ DMZ

■ QoS

■ SNMP

■ TR-069

■ Virtual Server

■ UPnP

■ Network Scan

■ Email Settings

DNS

The resolving of IP address to host names/domains and voice versa is managed by the DNS. The required information(IP address of at least one DNS server) is normally provided by your ISP. But this device is also able to detect the DNS servers available automatically.

DDNS



Provider

DynDNS.org(Dynamic) ▼

Host Name

DynDNS.org(Dynamic)

Username / E-mail

DynDNS.org(Custom)

Password / Key

No-IP.com

TZO.com

dns.org

Apply

Refresh



■ DNS

-DNS

-DNS Redirect

■ Firewall

■ DMZ

■ QoS

■ SNMP

■ TR-069

■ Virtual Server

■ UPnP

■ Network Scan

■ Email Settings

DNS Redirect

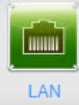
Enable DNS Redirect



DNS Redirect IP Address

Apply

Refresh



- DNS
- Firewall
 - Outbound Filter
 - Inbound Filter
 - URL Filter
 - MAC Address Filter
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

Outbound Filter

Outbound Filter Setting

Outbound Filter

☐ Enable

Use schedule rule ---ALWAYS ON---

[Copy to](#)

ID --

Outbound Filter Rules List

- ☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1	192.168.1.1 80	192.168.1.1 80	☐	1 Add New Rule...
2	192.168.1.1 80	192.168.1.1 80	☐	1 Add New Rule...



- DNS
- Firewall
 - Outbound Filter
 - Inbound Filter
 - URL Filter
 - MAC Address Filter
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

Inbound Filter

Inbound Filter Setting

Inbound Filter

☐ Enable

Use schedule rule ---ALWAYS ON---

Copy to

ID --

Inbound Filter Rules List

- ☒ Allow all to pass except those match the following rules.
☐ Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1	:	:	☐	 Add New Rule...
2	:	:	☐	 Add New Rule...



- DNS
- Firewall
 - Outbound Filter
 - Inbound Filter
 - URL Filter**
 - MAC Address Filter
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

URL Filter

URL Filter provides the useful tools for restricting Internet access.
Website URL Blocking allows you to quickly create a list of all web sites that you wish to allow or deny users from accessing.

URL Filtering Setting

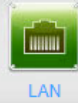
URL Filtering ☐ Enable

URL Filtering Rules

ID	URL	Enable
1		☐
2		☐
3		☐
4		☐
5		☐

Apply

Refresh



- DNS
- Firewall
 - Outbound Filter
 - Inbound Filter
 - URL Filter
 - MAC Address Filter**
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

MAC Address Filter

MAC Filtering Settings

MAC Address Control

☐ Enable

☐ Connection control

Wired clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.

DHCP clients -- Select one --
-- Select one --
 192.168.0.10 (ProBook-1242)

Copy to

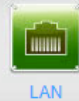
ID --

MAC Filtering Rules

ID	MAC Address	C
1		☐
2		☐
3		☐
4		☐
5		☐

Previous page

Next page



- DNS
- Firewall
- **DMZ**
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

DMZ

Firewall Settings

Enable SPI

☐

DMZ Host

Enable DMZ

☐

DMZ IP Address

<<

Computer Name
 Computer Name
 ProBook-1242(192.168.0.10)

Apply

Refresh



- DNS
- Firewall
- DMZ
- **QoS**
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

QoS

QoS Engine Setup

Enable QoS Packet Filter : ☐

Upstream bandwidth :

kbps

Use schedule rule ---ALWAYS ON---

Copy to

ID -- ▾

QoS Rules

ID	Local IP : Ports	Remote IP : Ports	QoS Priority	Enable	Use Rule#
1	:	:	High ▾	☐	 Add New Rule...
2	:	:	High ▾	☐	 Add New Rule...



Home



Internet



LAN



VPN



Advanced



System

Logout

- DNS
- Firewall
- DMZ
- QoS
- **SNMP**
- TR-069
- Virtual Server
- UPnP
- Network Scan
- Email Settings

SNMP

SNMP

SNMP Local ☐ Enable ☒ Disable

SNMP Remote ☐ Enable ☒ Disable

Get Community

Set Community

IP 1

IP 2

IP 3

IP 4

SNMP Version ☒ V1 ☐ V2c ☐ v3

WAN Access IP Address

System Contact

System Name

System Location

User Privacy Definition

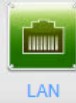
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Actions
1			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
2			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
3			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
4			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
5			MD5	Disable	authNoPriv	Disable	Read	☐	Edit



Home



Internet



LAN



VPN



Advanced



System

Logout

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- **TR-069**
- Virtual Server
- UPnP
- Network Scan
- Email Settings

TR-069

TR-069

☐ Enable

Apply

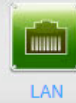
Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- TR-069
- **Virtual Server**
- UPnP
- Network Scan
- Email Settings

Virtual Server

The Externally acts as server. It receives the requests of remote users under its public IP address and forwards them automatically to the Virtual Server. So a client in your network behind NAT or firewall can provide services as a Virtual Server. You just have to enable specific ports or port ranges and protocols (UDP/TCP). File sharing or web services for e.g. HTTP, FTP or POP3 are possible. The private IP addresses of the servers in the local network remain safe. If you have a dynamic IP address, you may want to enable DynDNS additionally.

Well known services

Copy to

ID

Use schedule rule

Virtual Servers List

ID	Service Ports	Server IP : Port	Enable	Schedule Rule#
1		:	☐	 Add New Rule...
2		:	☐	 Add New Rule...

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- TR-069

■ Virtual Server

- UPnP
- Network Scan
- Email Settings

Virtual Server

The Externally acts as server. It receives the requests of remote users under its public IP address and forwards them automatically to the Virtual Server. So a client in your network behind NAT or firewall can provide services as a Virtual Server. You just have to enable specific ports or port ranges and protocols (UDP/TCP). File sharing or web services for e.g. HTTP, FTP or POP3 are possible. The private IP addresses of the servers in the local network remain safe. If you have a dynamic IP address, you may want to enable DynDNS additionally.

Well known services -- Select one -- Copy to ID --

-- Select one --

AUTH (113)
DNS (53)
FTP (21)
ISAKMP (500)
POP3 (110)
PPTP (1723)
SMTP (25)
TELNET (23)
WEB (80)

Virtual Servers List

ID	Service Ports	Enable	Schedule Rule#
1			

Add New Rule...

D-Link®
DWM-312



Home



Internet



LAN



VPN



Advanced



System

Logout

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server

■ UPnP

- Network Scan
- Email Settings

UPnP

Enable UPnP

☐

Apply

Refresh



Home



Internet



LAN



VPN



Advanced



System

Logout

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- **Network Scan**
- Email Settings

Network Scan

Network Scan

Item	Setting
Physical Interface	SIMA
Scan Approach	Auto ▼ Auto Manually
Apply Refresh	



Home



Internet



LAN



VPN



Advanced



System

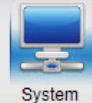
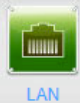
Logout

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- TR-069
- Virtual Server
- UPnP
- Network Scan
- **Email Settings**

Email Settings

Email Settings

Enable Email Notification	☐
SMTP Server IP and Port	:
SMTP Username	
SMTP Password	
Send E-mail alert to	
E-mail Subject	
Email Log Now	



- Administration
 - Password Settings
 - Remote Login Settings
 - Configuration Backup
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Password Settings

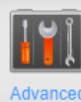
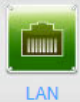
Old Password

New Password

Confirm Password

Apply

Refresh



- Administration
 - Password Settings
 - Remote Login Settings
 - Configuration Backup
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Remote Login Settings

Remote Management (HTTPS)

Enable Remote Management

☐ Enable

IP Allowed to Access

 /

Port

 Manual ▼

Apply

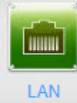
Refresh



Home



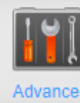
Internet



LAN



VPN



Advanced



System

Logout

- Administration
 - Password Settings
 - Remote Login Settings
 - Configuration Backup**
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Configuration Backup

Save Settings To Local Hard Drive

Save

Load Settings From Local Hard Drive

Choose File

No file chosen

Upload Settings

Restore To Factory Default Settings

Reset to Default

Auto Restore Configuration

☐ Enable

Save Conf.

Clean Conf.

Conf. Info.



Home



Internet



LAN



VPN



Advanced



System

Logout

- Administration
- SMS
 - SMS Inbox
 - Compose SMS
 - Message Settings
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

SMS Inbox

SMS Status

SIM Status	SIMB
Received SMS	1
New SMS	1
Total Capacity	30

Inbox

☐ From	Timestamp ▲	Text
☐ 101	2017/09/28,14:44:54	Call "101".....

SMS

Delete Reply Forward Refresh



- Administration
- SMS
 - SMS Inbox
 - Compose SMS**
 - Message Settings
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Compose SMS

Receiver :

Add '+' for international format of the phone number.

Text message :

Current input text length : 0 .

The max. length of a message is 160 characters for pure alphabetical or numeric.

Send

Refresh

- Administration
- SMS
 - SMS Inbox
 - Compose SMS
 - Message Settings
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Message Settings

Management Settings

Remote Management via SMS	☐ Enable ☒ Disable
Delete SMS for Remote Management	☐ Enable ☒ Disable
Security Key	

Command Settings

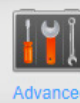
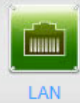
Status	☐ Enable ☒ Disable
Connect	☐ Enable ☒ Disable
Disconnect	☐ Enable ☒ Disable
Reconnect	☐ Enable ☒ Disable
Reboot	☐ Enable ☒ Disable

Notification Settings

WAN Link Up	☐ Enable ☒ Disable
WAN Link Down	☐ Enable ☒ Disable

Access Control List

Access Control	☐ Enable ☒ Disable
Phone 1	
Phone 2	
Phone 3	
Phone 4	
Phone 5	
	☐ Management ☐ Notification
	☐ Management ☐ Notification
	☐ Management ☐ Notification
	☐ Management ☐ Notification
	☐ Management ☐ Notification



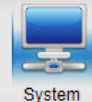
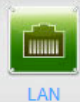
- Administration
- SMS
- **Time Settings**
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Time Settings

The time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time	Fri Sep 29, 2017 11:50:00
Time Zone	(GMT +10:00) Canberra, Melbourne, Sydney ▼
Enable Daylight Saving	☐
	Sync. your computer's time settings
☒ Automatically synchronize with Internet time server	
NTP Server Used	time.nist.gov
	Update Now

Sync. RESULT



- Administration
- SMS
- Time Settings
- Firmware Upgrade
- **-Device Upgrade**
- -Module Upgrade
- System Log
- Schedules
- Reboot & Reset

Device Upgrade

Please use the "Upgrade" button to update firmware version for your device.

Firmware Information

Current Firmware Version	V01.00.1.019	Check File
Current Firmware Date	2017/09/14	

Firmware Update

Select Firmware No file chosen

Accept unofficial firmware. ☐



- Administration
- SMS
- Time Settings
- Firmware Upgrade
 - Device Upgrade
 - Module Upgrade**
- System Log
- Schedules
- Reboot & Reset

Module Upgrade

Please use the "Upgrade" button to update firmware version for your device.

Firmware Information

Current Firmware Version

M18QW_v07.05.164541

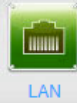
Check File



Home



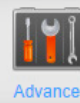
Internet



LAN



VPN



Advanced



System

Logout

- Administration
- SMS
- Time Settings
- Firmware Upgrade
- **System Log**
- Schedules
- Reboot & Reset

System Log

The System Log allows you to configure local, remote and email logging, and to view the logs that have been created.

Enable Logging To Syslog Server ☐

Syslog Server IP Address

Apply

Refresh

View Logs

Time	Message
Sep 29 11:49:57	MultiWanChk2: printnode[114]: ipaddr -> 10.100.83.192
Sep 29 11:49:57	MultiWanChk2: printnode[115]: dns -> 10.4.58.204
Sep 29 11:49:57	MultiWanChk2: printnode[116]: sec dns -> 10.5.136.242
Sep 29 11:49:57	MultiWanChk2: printnode[117]: hostaddr -> 10.4.58.204
Sep 29 11:49:57	MultiWanChk2: printnode[118]: sec_hostaddr->
Sep 29 11:49:57	MultiWanChk2: printnode[119]: interval -> 3
Sep 29 11:49:58	httpd: Create httpd thread fail! Retry.
Sep 29 11:50:02	MultiWanChk2: chkcntstatus[463]: nat is restarting, skip checking
Sep 29 11:50:40	MultiWanChk2: chkDestFunction[933]: usbnet0 Destination 10.4.58.204 is unreachable!

Page: 64/64 (Log Number : 954)

Previous page

Next page

First Page

Last Page

Refresh

Download

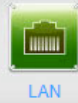
Clear logs



Home



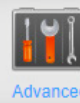
Internet



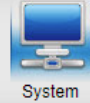
LAN



VPN



Advanced



System

Logout

- Administration
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- **Schedules**
- Reboot & Reset

Schedules

Schedule Rule

Enable Schedule



Rule#	Rule Name	Action
-------	-----------	--------

Previous page

Next page

Add New Rule...

- Administration
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- **Schedules**
- Reboot & Reset

Schedule Rule Setting

Name of Rule 1 :

Policy :

Activate

except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	Every Day		
5	Sunday		
6	Monday		
7	Tuesday		
8	Wednesday		
	Thursday		
	Friday		
	Saturday		

Back

Apply

Refresh



- Administration
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

-Reboot the Device

-Connection Reset

Reboot The Device

Reboot the Device

Reboot



- Administration
- SMS
- Time Settings
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

-Reboot the Device

-Connection Reset

Connection Reset

Auto-Reboot

☒ Disabled ☐ Enabled

Reboot-Schedule

3 : 0

☐ Daily Schedule

☒ Weekly Schedule Day of Week

Monday

☐ Date of Month

1

Apply

Refresh