

Inteno JUCI

User Guide

v3.10.2a

Table of Contents

| | | | |
|--------------------------------------|-----------|---------------------------------------|-----------|
| Introduction | 12 | WIFI | 22 |
| Requirements..... | 12 | WPS settings..... | 22 |
| Access web interface..... | 12 | Edit 5GHz Wireless Interface..... | 22 |
| Login..... | 12 | Edit 2.4GHz Wireless Interface..... | 22 |
| User Roles..... | 12 | LAN | 22 |
| User Modes..... | 12 | Detailed Client Overview..... | 23 |
| Features..... | 12 | Edit LAN Settings..... | 23 |
| Menu..... | 13 | Client..... | 23 |
| Applying changes..... | 13 | Detailed Client Overview | 23 |
| User Modes | 13 | Edit LAN Settings | 24 |
| Basic Mode..... | 13 | Client | 25 |
| Expert Mode..... | 13 | Status..... | 26 |
| Basic Mode | 13 | Port Forwarding..... | 26 |
| Features..... | 13 | Static Leases..... | 26 |
| Expert Mode | 14 | Parental Control..... | 26 |
| Features..... | 14 | Parental Control | 26 |
| User Roles | 14 | Internet Access Scheduling..... | 26 |
| User..... | 14 | WAN | 27 |
| Support..... | 14 | USB | 28 |
| Admin..... | 14 | Voice | 28 |
| Root..... | 14 | Profile | 28 |
| Features | 15 | Voice | 29 |
| Availability | 15 | Call Log..... | 29 |
| Menu | 15 | SIP Accounts..... | 29 |
| Overview..... | 15 | SIP Users..... | 29 |
| Voice..... | 15 | Voice Lines..... | 29 |
| Network..... | 15 | Advanced Settings..... | 29 |
| WIFI..... | 15 | Number Blocking..... | 29 |
| System..... | 16 | Ringing Schedule..... | 29 |
| Status..... | 16 | Speed Dialing..... | 29 |
| Applying changes | 16 | DECT Radio..... | 30 |
| Overview | 16 | Call Log | 30 |
| Parts..... | 17 | SIP Accounts | 30 |
| Device Network Map..... | 17 | Add account..... | 31 |
| Configuration Shortcuts..... | 17 | SIP Users | 31 |
| Status Panels..... | 18 | Add user..... | 31 |
| Device Network Map | 18 | Voice Lines | 32 |
| Colors..... | 18 | Advanced Settings | 32 |
| Details | 18 | SIP..... | 32 |
| Edit Node Settings | 19 | Line..... | 33 |
| Status..... | 19 | Dial Plan..... | 33 |
| Static Leases..... | 19 | SIP | 33 |
| Forwarding..... | 19 | Trusted CA Certificate..... | 34 |
| Parental Control..... | 19 | Line | 34 |
| Configuration Shortcuts | 19 | Dial Plan | 34 |
| Status Panels | 20 | Number Blocking | 34 |
| WIFI..... | 21 | Outgoing..... | 35 |
| LAN..... | 21 | Incoming..... | 35 |
| WAN..... | 21 | Block number..... | 35 |
| USB..... | 21 | Block number range..... | 35 |
| Voice..... | 21 | Ringing Schedule | 36 |
| Profile..... | 22 | | |

| | | | |
|--|-----------|--|-----------|
| Speed Dialing | 36 | 3G..... | 45 |
| DECT Radio | 36 | Point-to-point Tunnel..... | 45 |
| Network | 37 | IPv6 Tunnel in IPv4..... | 45 |
| Devices..... | 37 | IPv6 Tunnel to IPv4..... | 45 |
| XDSL..... | 37 | IPv6 rapid deployment..... | 46 |
| Connections..... | 37 | WWAN (LTE/HSPA+) | 46 |
| Routes..... | 37 | WWAN..... | 46 |
| Firewall..... | 37 | LTE..... | 46 |
| Parental Control..... | 37 | HSPA / HSPA+..... | 46 |
| Quality Of Service..... | 37 | Wizard..... | 46 |
| MultiWAN..... | 37 | Step 1..... | 46 |
| Services..... | 38 | Finalize..... | 46 |
| Devices | 38 | DHCP v6 (Uplink) | 47 |
| Base Device..... | 38 | Wizard..... | 47 |
| Ethernet..... | 38 | Step 1..... | 47 |
| ADSL..... | 38 | Finalize..... | 47 |
| VLAN..... | 38 | DHCP v4 | 47 |
| Base Device | 38 | Wizard..... | 47 |
| Device Status..... | 38 | Step 1..... | 47 |
| Ethernet | 39 | Finalize..... | 47 |
| Port Speed..... | 39 | Point-to-Point Protocol | 49 |
| ADSL | 39 | PPP..... | 49 |
| Service Type..... | 40 | Wizard..... | 49 |
| VDSL | 40 | Step 1..... | 49 |
| Latency Path..... | 40 | Finalize..... | 49 |
| PTM Priority..... | 40 | Point-to-Point Protocol over Ethernet | 49 |
| IP Quality of Service Algorithm..... | 41 | PPPoE..... | 49 |
| Strict Priority Precedence..... | 41 | Wizard..... | 50 |
| Weighted Fair Queuing..... | 41 | Step 1..... | 50 |
| VLAN | 41 | Finalize..... | 50 |
| 802.1q..... | 41 | Point-to-Point Protocol over ATM | 50 |
| 802.1p..... | 41 | PPPoA..... | 50 |
| XDSL | 42 | Wizard..... | 50 |
| Modulation..... | 42 | Step 1..... | 50 |
| VSDL Profile..... | 42 | Finalize..... | 50 |
| Capabilities..... | 42 | 3G | 51 |
| Modulation | 42 | 3G..... | 51 |
| VSDL Profile | 42 | Wizard..... | 51 |
| Capabilities | 43 | Step 1..... | 51 |
| Connections | 43 | Finalize..... | 51 |
| Connect..... | 43 | Point-to-point Tunnel | 51 |
| Disconnect..... | 44 | Point-to-Point Tunneling Protocol..... | 51 |
| Create Interface..... | 44 | Wizard..... | 51 |
| Configure Interface..... | 44 | Step 1..... | 51 |
| Create Interface | 44 | Finalize..... | 52 |
| Connection Types..... | 44 | IPv6 Tunnel in IPv4 | 52 |
| Uplink..... | 44 | 6in4..... | 52 |
| Downlink..... | 44 | Wizard..... | 52 |
| Unmanaged..... | 45 | Step 1..... | 52 |
| Uplink | 45 | Finalize..... | 52 |
| Interfaces..... | 45 | IPv6 Tunnel to IPv4 | 52 |
| DHCP v4..... | 45 | 6to4..... | 53 |
| DHCP v6 (Uplink)..... | 45 | Wizard..... | 53 |
| Point-to-Point Protocol..... | 45 | Step 1..... | 53 |
| Point-to-Point Protocol over Ethernet..... | 45 | Finalize..... | 53 |
| Point-to-Point Protocol over ATM..... | 45 | | |

| | | | |
|--|-----------|--|-----------|
| IPv6 rapid deployment | 53 | Physical Settings..... | 60 |
| 6rd..... | 53 | Advanced..... | 60 |
| Wizard..... | 53 | DHCP..... | 60 |
| Step 1..... | 53 | DHCP v4 | 60 |
| Finalize..... | 54 | General..... | 61 |
| Downlink | 54 | Physical Settings..... | 61 |
| Finalize..... | 54 | Advanced..... | 61 |
| Physical Device..... | 54 | DHCP v6 | 61 |
| Ethernet Adapter..... | 54 | General..... | 61 |
| Add Device..... | 54 | Physical Settings..... | 61 |
| Unmanaged | 55 | Advanced..... | 61 |
| Step 1..... | 55 | Point-to-Point Protocol | 61 |
| Add Device..... | 55 | PPP..... | 62 |
| Finalize..... | 55 | General..... | 62 |
| Configure Interface | 55 | Advanced..... | 62 |
| Edit Connections..... | 55 | Point-to-Point Protocol over Ethernet | 62 |
| Default Connections..... | 56 | PPPoE..... | 62 |
| LAN..... | 56 | General..... | 62 |
| WAN..... | 56 | Physical Settings..... | 62 |
| WAN6..... | 56 | Advanced..... | 62 |
| Connection Types..... | 56 | Point-to-Point Protocol over ATM | 63 |
| Unmanaged..... | 56 | PPPoA..... | 63 |
| Static Address..... | 56 | General..... | 63 |
| DHCP v4..... | 56 | Physical Settings..... | 63 |
| DHCP v6..... | 56 | Advanced..... | 63 |
| Point-to-Point Protocol..... | 56 | 3G | 63 |
| Point-to-Point Protocol over Ethernet..... | 57 | 3G..... | 63 |
| Point-to-Point Protocol over ATM..... | 57 | General..... | 63 |
| 3G..... | 57 | Advanced..... | 64 |
| 4G..... | 57 | WWAN (LTE/HSPA+) | 64 |
| Point-to-point Tunnel..... | 57 | WWAN..... | 64 |
| IPv6 Tunnel in IPv4..... | 57 | LTE..... | 64 |
| IPv6 Tunnel to IPv4..... | 57 | HSPA / HSPA+..... | 64 |
| IPv6 rapid deployment..... | 57 | General..... | 64 |
| Dual-Stack Lite..... | 57 | Advanced..... | 64 |
| Point-to-Point Protocol over L2TP..... | 57 | 4G | 64 |
| LAN | 57 | 4G..... | 65 |
| General..... | 58 | General..... | 65 |
| Physical Settings..... | 58 | Advanced..... | 65 |
| Advanced..... | 58 | Point-to-point Tunnel | 65 |
| DHCP..... | 58 | Point-to-Point Tunneling Protocol..... | 65 |
| WAN | 58 | General..... | 65 |
| General..... | 58 | Advanced..... | 65 |
| Physical Settings..... | 58 | IPv6 Tunnel in IPv4 | 65 |
| Advanced..... | 58 | 6in4..... | 66 |
| WAN6 | 59 | General..... | 66 |
| General..... | 59 | Advanced..... | 66 |
| Physical Settings..... | 59 | IPv6 Tunnel to IPv4 | 66 |
| Advanced..... | 59 | 6to4..... | 66 |
| Unmanaged | 59 | General..... | 66 |
| Unmanaged..... | 59 | Advanced..... | 66 |
| General..... | 59 | IPv6 rapid deployment | 66 |
| Physical Settings..... | 59 | 6rd..... | 67 |
| Advanced..... | 60 | General..... | 67 |
| Static Address | 60 | Advanced..... | 67 |
| Static address..... | 60 | Dual-Stack Lite | 67 |
| General..... | 60 | | |

| | | | |
|---|-----------|---------------------------------------|-----------|
| DS-Lite..... | 67 | Overview..... | 77 |
| General..... | 67 | Add Interface..... | 77 |
| Advanced..... | 67 | Class..... | 78 |
| Point-to-Point Protocol over L2TP..... | 67 | Overview..... | 78 |
| PPP..... | 68 | Add Class..... | 78 |
| L2TP..... | 68 | Classification Group..... | 79 |
| General..... | 68 | Overview..... | 79 |
| Advanced..... | 68 | Add Classification Group..... | 79 |
| Routes..... | 68 | Classify..... | 79 |
| IPv4 Routes..... | 68 | Overview..... | 79 |
| IPv6 Routes..... | 68 | Add Filter..... | 80 |
| Add Static Route..... | 68 | Reorder..... | 80 |
| IPv4 Routes..... | 69 | Workflow..... | 80 |
| IPv6 Routes..... | 69 | Process..... | 81 |
| Firewall..... | 69 | Configuration steps..... | 81 |
| General Settings..... | 69 | 1: Class..... | 81 |
| Zones..... | 69 | 2: Classify..... | 81 |
| Rules..... | 70 | 3: Group..... | 81 |
| Forwarding..... | 70 | 4: Enable..... | 81 |
| DMZ / Exposed Host..... | 70 | MultiWAN..... | 81 |
| General Settings..... | 70 | MultiWAN Settings..... | 81 |
| Firewall Settings..... | 70 | Traffic Rules..... | 81 |
| Zones..... | 70 | MultiWAN Options..... | 82 |
| Zone configuration..... | 70 | MultiWAN Settings..... | 82 |
| Default Policy..... | 71 | Add WAN..... | 82 |
| Firewall Action..... | 71 | Add Custom DNS Servers..... | 82 |
| Add Firewall Zone..... | 71 | Traffic Rules..... | 83 |
| Add Zone Members..... | 71 | Add Rule..... | 83 |
| Rules..... | 72 | MultiWAN Options..... | 83 |
| Add Firewall Rule..... | 72 | Sample Configurations..... | 84 |
| Reorder Firewall Rules..... | 72 | Load Balancer Weights..... | 84 |
| Forwarding..... | 73 | Load Balancing Interfaces..... | 84 |
| Port Mapping Settings..... | 73 | Interface Selection..... | 84 |
| Add or Edit Port Mapping..... | 74 | Health Monitor Ping / Statistics..... | 84 |
| Protocol..... | 74 | Failover Traffic Destination..... | 84 |
| Add or Edit Port Mapping..... | 74 | Services..... | 85 |
| Protocol..... | 75 | Printer Server..... | 85 |
| DMZ / Exposed Host..... | 75 | MiniDLNA..... | 85 |
| Add Exposed Host..... | 75 | UPnP..... | 85 |
| Parental Control..... | 75 | DDNS..... | 85 |
| Internet Access Scheduling..... | 75 | IPTV..... | 85 |
| Start and Stop Times..... | 76 | DHCP..... | 85 |
| Quality Of Service..... | 76 | SNMP..... | 85 |
| Interface views..... | 76 | Samba..... | 85 |
| Interface..... | 76 | Printer Server..... | 85 |
| Class..... | 76 | MiniDLNA..... | 86 |
| Classification Group..... | 76 | Status..... | 86 |
| Classify..... | 76 | General..... | 86 |
| Workflow..... | 76 | Advanced..... | 86 |
| Workflow..... | 76 | UPnP..... | 86 |
| 1: Class..... | 77 | General..... | 86 |
| 2: Classify..... | 77 | Advanced..... | 87 |
| 3: Group..... | 77 | ACL..... | 87 |
| 4: Enable..... | 77 | DDNS..... | 87 |
| Interface..... | 77 | DDNS Services..... | 87 |

| | | | |
|---|-----------|---|------------|
| IPTV | 88 | Services..... | 96 |
| DHCP | 88 | Restart..... | 96 |
| General..... | 88 | General Settings | 96 |
| Advanced..... | 88 | Time Servers | 97 |
| Hostnames..... | 88 | Add Server..... | 97 |
| SNMP | 89 | Log Settings | 97 |
| System..... | 89 | Current Firmware..... | 97 |
| Agent..... | 89 | Connectivity Test | 98 |
| Com2Sec..... | 89 | Current Firmware..... | 98 |
| Group..... | 89 | Menu Access | 98 |
| View..... | 89 | Passwords | 98 |
| Access..... | 89 | Change Password Dialog..... | 98 |
| Pass..... | 89 | Change password..... | 98 |
| Samba | 89 | Firmware Upgrade | 99 |
| General..... | 90 | Current Firmware..... | 99 |
| Samba Users..... | 90 | USB Firmware Upgrade..... | 99 |
| Samba Shares..... | 90 | Manual Firmware Upgrade..... | 99 |
| WIFI | 90 | Upgrade Options | 99 |
| General..... | 90 | Firmware image extensions..... | 99 |
| Band Steering..... | 90 | Online Upgrade..... | 100 |
| WPS Settings..... | 90 | Backup/Restore | 100 |
| MAC Filter..... | 90 | Backup Settings..... | 100 |
| General | 90 | Save Backup..... | 100 |
| Radios..... | 91 | Load Backup..... | 100 |
| Wireless..... | 91 | Factory Settings..... | 101 |
| Radios | 91 | Backup Settings | 101 |
| Wireless | 91 | IUP | 101 |
| Add Wireless Interface..... | 92 | General..... | 101 |
| Band Steering | 92 | Main Provisioning Server..... | 102 |
| Enable Band Steering..... | 92 | DHCP Discover Provisioning Server..... | 102 |
| WPS Settings | 92 | Software Update Config..... | 102 |
| General WPS Settings..... | 93 | Sub Configs..... | 102 |
| WPS-PBC: Push Button on Device..... | 93 | Add Sub Config..... | 103 |
| WPS/REG: Device provides PIN..... | 93 | TR69 | 103 |
| WPS-PIN: Another Device provides PIN..... | 93 | Configure ACS Specific Settings..... | 103 |
| WPS-PIN: Another Device provides PIN | 93 | Configure CPE Specific Settings..... | 103 |
| | 93 | Management | 104 |
| WPS/REG: Device provides PIN | 93 | SSH..... | 104 |
| Generating a PIN..... | 94 | Services..... | 104 |
| General WPS Settings | 94 | OWSD | 104 |
| WPS-PBC: Push Button on Device | 94 | Configuration..... | 104 |
| Pairing Your Device..... | 94 | Add Listen Interface..... | 104 |
| MAC Filter | 94 | Add Origin..... | 105 |
| Enable MAC Filter..... | 95 | SSH | 105 |
| System | 95 | General Settings..... | 105 |
| General Settings..... | 95 | Dropbear Instances..... | 105 |
| Menu Access..... | 95 | Add SSH Server instance:..... | 105 |
| Passwords..... | 96 | Accepted SSH Keys..... | 106 |
| Firmware Upgrade..... | 96 | Services | 106 |
| Backup/Restore..... | 96 | Allow WAN Access To Running Services..... | 106 |
| IUP..... | 96 | Configure firewall rule for this service..... | 106 |
| TR69..... | 96 | Add Firewall Rule..... | 107 |
| Management..... | 96 | Hardware | 107 |
| Hardware..... | 96 | Configure Buttons..... | 107 |
| Power Management..... | 96 | | |

| | | | |
|-------------------------------|------------|-----------------------------|------------|
| LEDs..... | 107 | WiFi Status..... | 115 |
| Configure Buttons..... | 107 | WiFi Scan..... | 115 |
| Examples..... | 107 | WiFi Status..... | 115 |
| Toggle Button..... | 108 | Configuration..... | 116 |
| LEDs..... | 108 | Client..... | 116 |
| Displayed Leds..... | 108 | WiFi Scan..... | 116 |
| Examples..... | 108 | Chart..... | 116 |
| Toggle LED..... | 108 | Axes..... | 117 |
| Power Management..... | 109 | Table..... | 117 |
| Services..... | 109 | Scan WiFi..... | 117 |
| Restart..... | 109 | Band Steering..... | 117 |
| Restart device..... | 109 | Status..... | 117 |
| Status..... | 110 | Log..... | 118 |
| System..... | 110 | DSL Status..... | 118 |
| IGPM TV Status..... | 110 | DSL Status Information..... | 118 |
| WiFi Status..... | 110 | Line Status..... | 118 |
| DSL Status..... | 110 | DSL Mode..... | 118 |
| USB Status..... | 110 | Bit Rate..... | 118 |
| Network Status..... | 110 | Actual Data Rate..... | 119 |
| Diagnostics..... | 110 | Operating Data..... | 119 |
| Voice Status..... | 110 | SNR margin..... | 119 |
| System..... | 111 | Loop Attenuation..... | 119 |
| System Status..... | 111 | Error Counter..... | 119 |
| Processes..... | 111 | FEC Corrections..... | 119 |
| System Status..... | 111 | CRC Corrections..... | 119 |
| Configuration..... | 111 | Cell Statistics..... | 119 |
| Processes..... | 111 | IGPM TV Status..... | 120 |
| Overview..... | 112 | Configuration..... | 120 |
| Process Detail Toggle..... | 112 | USB Status..... | 120 |
| Network Status..... | 112 | Table..... | 120 |
| Status..... | 112 | CATV..... | 120 |
| Clients..... | 112 | SFP..... | 121 |
| Routing..... | 112 | Configuration..... | 121 |
| UPnP..... | 112 | DDM..... | 121 |
| DHCP..... | 112 | ROM..... | 121 |
| NAT..... | 113 | Diagnostics..... | 122 |
| Status..... | 113 | Ping..... | 122 |
| WAN6..... | 113 | Trace..... | 122 |
| LAN..... | 113 | Speed Test..... | 122 |
| WAN..... | 113 | Ping..... | 122 |
| Clients..... | 113 | Ping Test..... | 122 |
| Table..... | 113 | Example..... | 122 |
| Routing..... | 114 | Trace..... | 123 |
| ARP..... | 114 | Traceroute Test..... | 123 |
| IPv4..... | 114 | Example..... | 123 |
| IPv6..... | 114 | Speed Test..... | 123 |
| IPv6 Neighbors..... | 114 | Configuration..... | 123 |
| UPnP..... | 114 | Perform Speed Test..... | 123 |
| DHCP..... | 114 | Example..... | 123 |
| DHCPv4 Leases..... | 114 | Add test server..... | 123 |
| DHCPv6 Leases..... | 114 | Remove test server..... | 124 |
| NAT..... | 115 | Voice Status..... | 124 |
| Connections..... | 115 | Configuration..... | 124 |
| NAT Connection Table..... | 115 | Your phone numbers..... | 124 |
| WiFi Status..... | 115 | Voice lines..... | 125 |
| | | Event Log..... | 125 |
| | | Log..... | 125 |

| | | | |
|--|-----|-------------------------------------|-----|
| ACS..... | 125 | Domain Name..... | 132 |
| ARP..... | 125 | Delay..... | 132 |
| ATM - Asynchronous Data Transfer Mode | | Dwell Time..... | 132 |
| | 125 | DLNA..... | 132 |
| Assured Forwarding..... | 125 | DNS..... | 132 |
| Auto-Negotiation..... | 126 | DHCP..... | 132 |
| Access Control List..... | 126 | DHCP lease..... | 132 |
| APN..... | 126 | DHCP Pool..... | 132 |
| Ad SPECification..... | 126 | DHCP Options..... | 133 |
| AMPDU..... | 126 | Downlink..... | 136 |
| Asterisk..... | 126 | DMZ..... | 136 |
| AMSDU..... | 126 | DSL..... | 136 |
| ADPCM..... | 127 | Discrete MultiTone Modulation..... | 136 |
| ADSL..... | 127 | DNS Server..... | 137 |
| Access point..... | 127 | Dynamic DNS (DDNS or DynDNS)..... | 137 |
| ABR..... | 127 | DTMF..... | 137 |
| AFTR..... | 127 | DSL Mode..... | 137 |
| Band Steering..... | 127 | DNS Server..... | 137 |
| Bit Error Rate..... | 127 | DSCP..... | 137 |
| Bitswap..... | 127 | Differentiated Services..... | 138 |
| Beamforming..... | 128 | Classification Process..... | 138 |
| Back-Off..... | 128 | Duplex..... | 138 |
| Bandwidth..... | 128 | DFS..... | 139 |
| Bit Rate..... | 128 | DUID..... | 139 |
| BSS..... | 128 | Data Package..... | 139 |
| Companing..... | 128 | DECT..... | 139 |
| CRC..... | 128 | DCPM..... | 139 |
| CA..... | 128 | Dropping..... | 139 |
| CPE..... | 129 | DDM..... | 139 |
| Cell (DSL)..... | 129 | DTMF Mode..... | 139 |
| Congestion..... | 129 | Ethernet Auto Power Down..... | 140 |
| CLR..... | 129 | EEE..... | 140 |
| Connection Bytes..... | 129 | EoA..... | 140 |
| Classful QDisc / Packet Scheduler..... | 129 | ESP..... | 140 |
| Class Selector..... | 129 | Ethernet..... | 140 |
| %CPU..... | 130 | EVDO..... | 140 |
| Checksum..... | 130 | Firewall Zone..... | 140 |
| CCMP..... | 130 | Failover..... | 140 |
| CDMA..... | 130 | Firewall group..... | 140 |
| CATV..... | 130 | Firewall Action..... | 141 |
| CBR..... | 130 | Flow Specification..... | 141 |
| Cipher..... | 130 | Frame..... | 141 |
| Codec..... | 131 | FEC - Forward error correction..... | 141 |
| CPU..... | 131 | GSM..... | 141 |
| Com2Sec..... | 131 | GRE..... | 141 |
| Cron Log Level..... | 131 | Genmask..... | 141 |
| CHAP..... | 131 | Gateway..... | 141 |
| DS-Lite..... | 131 | GPRS..... | 142 |
| Dial Plan..... | 131 | Gateway metric..... | 142 |
| Device Flags..... | 132 | Host ID..... | 142 |

| | | | |
|--------------------------------------|-----|--|-----|
| Hostname..... | 142 | Link Speed..... | 150 |
| HT Capabilities..... | 142 | MCR..... | 150 |
| HSPA / HSPA+..... | 142 | Multicast..... | 151 |
| IUP..... | 142 | MPDU..... | 151 |
| ICMP..... | 142 | MIB..... | 151 |
| IP Datagram..... | 143 | Masquerading..... | 151 |
| IGMP Snooping..... | 144 | MiniDLNA..... | 151 |
| IP Route..... | 144 | MTU..... | 151 |
| IP in IP..... | 144 | MAC..... | 151 |
| IPUI..... | 144 | MSS Clamping..... | 152 |
| IP ECN..... | 144 | MSDU..... | 152 |
| IP Address..... | 144 | MBS..... | 152 |
| IP Quality of Service Algorithm..... | 145 | MSS..... | 152 |
| Strict Priority Precedence..... | 145 | NIC..... | 152 |
| Weighted Fair Queuing..... | 145 | Netmask..... | 152 |
| Interface Protocol Type..... | 145 | NTP - Network Time Protocol..... | 152 |
| Uplink..... | 145 | Network interface..... | 152 |
| Downlink..... | 145 | NAT Loopback..... | 152 |
| Unmanaged..... | 145 | Network Profile..... | 153 |
| IPoE..... | 145 | NAT..... | 153 |
| IGMP..... | 145 | Next Hop..... | 153 |
| IPv4 Broadcast Address..... | 145 | NTP Mode..... | 153 |
| IPv4..... | 146 | NAT-PMP..... | 153 |
| Inotify..... | 146 | Noise level..... | 153 |
| Interface Protocol..... | 146 | Network bridge..... | 154 |
| Interface Type..... | 146 | OBSS Coexistence..... | 154 |
| lophys..... | 147 | OpenWRT..... | 154 |
| IP Precedence..... | 147 | More information:..... | 154 |
| IP..... | 147 | OSWD..... | 154 |
| IntServ..... | 147 | Overhead..... | 154 |
| IPTV..... | 147 | OUI..... | 154 |
| IPv6 Address..... | 147 | Port..... | 154 |
| IAID..... | 148 | Packet Scheduler / Queueing Discipline | |
| IGMP Proxy..... | 148 | | 155 |
| IP TOS..... | 148 | Port Forwarding..... | 155 |
| IPtables..... | 148 | PTM Priority..... | 155 |
| Jitter..... | 148 | Packet Loss..... | 155 |
| Jitter Buffer..... | 148 | Precedence..... | 155 |
| JUCI..... | 149 | Proxy..... | 156 |
| LTE..... | 149 | Periodic Inform..... | 156 |
| LCP..... | 149 | PTM - Pulse-Time Modulation..... | 156 |
| LLC..... | 149 | Traffic Policing..... | 156 |
| Lease Time..... | 149 | Packet Aggregation..... | 156 |
| Logging Level..... | 149 | Pairing..... | 156 |
| LSAP..... | 149 | PLC..... | 156 |
| L2TP..... | 150 | PCR..... | 156 |
| Latency..... | 150 | Point-to-Point Tunneling Protocol..... | 157 |
| LAN..... | 150 | Port Speed..... | 157 |
| Loop Attenuation..... | 150 | PoP..... | 157 |
| Latency Path..... | 150 | Ping..... | 157 |
| Load Balancing..... | 150 | | |

| | | | |
|--|-----|---------------------------------|-----|
| PPP..... | 157 | | 165 |
| PSK..... | 157 | SNAP..... | 166 |
| PPPoA..... | 157 | SSID..... | 166 |
| Protocol..... | 157 | SIP Realm..... | 166 |
| PAP..... | 158 | SNR Margin..... | 166 |
| PPID..... | 158 | STUN..... | 166 |
| Prefix delegation..... | 158 | SIP Reg Interval..... | 166 |
| PSDN..... | 158 | Samba..... | 166 |
| PPPoE..... | 158 | SSDP..... | 167 |
| PSTN..... | 158 | SIP..... | 167 |
| Packetization..... | 158 | State Code..... | 167 |
| PCM..... | 158 | Source-Specific Multicast..... | 167 |
| PBX..... | 159 | SIP Server/Registrar..... | 167 |
| PID..... | 159 | Service Type..... | 168 |
| Packet..... | 159 | SRTP..... | 168 |
| Quantization..... | 159 | SIP Account..... | 168 |
| QoS Mark..... | 159 | SSH..... | 168 |
| QoS..... | 159 | SIP Domain..... | 168 |
| QoS Filter..... | 159 | SIP User..... | 168 |
| Scheduling..... | 160 | SIP Address..... | 168 |
| QoS Class..... | 160 | SIP Codec..... | 168 |
| QoS Classification Group..... | 160 | G.711ALaw..... | 169 |
| Queueing Discipline / Packet Scheduler | | G.711MuLaw..... | 169 |
| | 160 | G.729a..... | 169 |
| Routing..... | 160 | G.726..... | 169 |
| RTSP..... | 160 | SFP..... | 169 |
| Route..... | 161 | More information:..... | 169 |
| RX Chain Power Save Quiet Time..... | 161 | SCR..... | 169 |
| Root QDisc..... | 161 | Strict Priority Precedence..... | 169 |
| Routing Table..... | 161 | SSL..... | 169 |
| Types of routes..... | 161 | SIP Authentication Name..... | 170 |
| Route metric..... | 161 | SNMP Agents..... | 170 |
| RX Chain Power Save..... | 161 | TR069..... | 170 |
| Request SPECification..... | 161 | Traceroute..... | 170 |
| RFC2275..... | 163 | TPtest..... | 170 |
| ROM..... | 163 | More information:..... | 170 |
| RFC1918..... | 163 | TLS..... | 170 |
| RXC..... | 163 | TD-SCDMA..... | 170 |
| RSSI..... | 163 | TCP..... | 171 |
| RSVP..... | 163 | TTL..... | 171 |
| RSS (Memory)..... | 164 | Token Bucket..... | 171 |
| RX Chain Power Save PPS..... | 164 | TCP Flags..... | 171 |
| RTP..... | 164 | TPC..... | 171 |
| Shaping..... | 164 | TKIP..... | 172 |
| Static Route..... | 164 | Traffic SPECification..... | 172 |
| Static address..... | 164 | UDP..... | 172 |
| SNR - Signal to Noise Ratio..... | 165 | Unicast..... | 172 |
| Seamless Rate Adaptation..... | 165 | UBIFS..... | 172 |
| SRV..... | 165 | UAPSD..... | 172 |
| Simple Network Management Protocol | | UPnP..... | 172 |
| | | USB..... | 173 |

| | | | |
|--|------------|----------------------------------|------------|
| UBR | 173 | WMM | 177 |
| UMTS | 173 | WPA personal | 177 |
| Uplink | 173 | WCDMA | 178 |
| UUID | 173 | WiFi encryption | 178 |
| Unmanaged | 173 | WPA2 Enterprise | 178 |
| VOIP | 173 | WiFi channel | 178 |
| VC-MUX | 173 | WPA Enterprise | 178 |
| VCI | 174 | WMM Power Save | 179 |
| %VSZ | 174 | WiFi band | 179 |
| VPI | 174 | WiFi | 179 |
| VLAN | 174 | WMM Acknowledgement | 179 |
| VDSL | 174 | WAN | 179 |
| VPN | 174 | WPS | 179 |
| VBR | 175 | LAN | 180 |
| Non-Realtime VBR | 175 | WiFi interface | 180 |
| Realtime VBR | 175 | WWAN | 180 |
| VSZ | 175 | 6to4 | 180 |
| Virtual Network Interface | 175 | 6rd | 180 |
| Types of Virtual Network Interfaces..... | 175 | 802.11g | 180 |
| Weighted Fair Queuing | 176 | 802.11n | 180 |
| WEP | 176 | 3G | 180 |
| WiFi Mode | 176 | 802.11ac | 180 |
| Auto..... | 176 | 6in4 | 181 |
| 802.11a..... | 176 | 802.11a | 181 |
| 802.11ac..... | 176 | 802.11b/g | 181 |
| 802.11b..... | 176 | 802.1q | 181 |
| 802.11b/g..... | 176 | 802.1p | 181 |
| 802.11g..... | 176 | 802.11b | 181 |
| 802.11n..... | 177 | 2G | 182 |
| WPA2 PSK | 177 | 4G | 182 |
| WiFi Key | 177 | | |
| Wireless radio | 177 | | |

Introduction

Administration of the gateway is done through a web interface. All settings are accessible through an address on your local network.

Requirements

To access the web interface, you need the following:

An installed gateway device.

A computer connected to the LAN or WLAN port on the device.

A web browser installed on the computer.

The default address for the web interface is <http://192.168.1.1>.

Access web interface

To access the web interface you need to use your web browser. There are multiple ways of accessing the interface.

Login

To login to the web interface, you use a user name and a password.

User Roles

The web interface uses *Roles* to provide and restrict access to the various features in the device.

There are four pre-defined roles: **User**, **Support**, **Admin**, and **Root**.

User Modes

In addition to *User Roles*, the *User Modes* may provide further constraints on what settings and features are displayed in the web interface.

Note: The mode affects display only, the features are still available and operational.

Features

Depending on your device and/or geographical region, certain features may be unavailable

in the interface.

Menu

The menu contains a number of items, which provide access to various parts of the web interface.

Applying changes

When you change a setting or a value in the interface, it gets added to a list of changes. The changes will not take effect until you click **apply**.

User Modes

In addition to *User Roles*, the *User Modes* may provide further constraints on what settings and features are displayed in the web interface.

Note: The mode affects display only, the features are still available and operational.

Basic Mode

Basic mode provides access to a selected set of settings and aspects of features, displaying a reduced set of options. This mode is suitable for the most common tasks and configurations.

Expert Mode

Expert mode provides access to a larger number of settings and aspects of features. This mode is suitable when you have deeper technical knowledge and want to do specific customizations or troubleshooting.

Basic Mode

Basic mode provides access to a selected set of settings and aspects of features, displaying a reduced set of options. This mode is suitable for the most common tasks and configurations.

Features

In basic mode, all Expert mode settings and views are hidden from the interface. However, if you select a particular task in basic mode that requires expert mode settings, they will automatically be displayed.

Expert Mode

Expert mode provides access to a larger number of settings and aspects of features. This mode is suitable when you have deeper technical knowledge and want to do specific customizations or troubleshooting.

Features

In expert mode, all Basic mode settings and views are also shown.

User Roles

The web interface uses *Roles* to provide and restrict access to the various features in the device.

There are four pre-defined roles: **User**, **Support**, **Admin**, and **Root**.

User

The User role has restricted access to basic set of features.

login: user

password: user

Support

The Support role has elevated access to basic and a set of advanced features.

login: support

password:support

Admin

The Admin role has unrestricted access to all basic and advanced features.

login: admin

password:admin

Root

The Root role has unrestricted to the device, and can be used for command line access to the device via .

login: root

password:root

Features

Depending on your device and/or geographical region, certain features may be unavailable in the interface.

Availability

Certain features may not be available in your interface, depending on several factors:

Device - Your device may be limited in which ports are available.

Geographical region - Features might not be offered in some regions or countries.

Operator Settings - Your operator may have restricted, altered or added features in the software.

Menu

The menu contains a number of items, which provide access to various parts of the web interface.



Overview

The **Overview** page shows the most important statuses and settings for your device.

Voice

The **Voice** provides access to settings relating to voice communications through the device.

Network

The **Network** view provides access to the devices, connections and available configurations in the network.

WIFI

The **WiFi view** shows you information about your wireless network.

System

The **System** view provides access to device information, management, provisioning and settings.

Status

The Status area provides an overview of the current situation for your device, network and services, and also contains diagnostic tools.

Applying changes

When you change a setting or a value in the interface, it gets added to a list of changes. The changes will not take effect until you click **apply**.

The **unapplied changes** and **apply** button are shown at the bottom of the window.



changes

To make the changes take effect click **Apply**.

To keep the current state without any changes click **Cancel**.

Overview

The **Overview** page shows the most important statuses and settings for your device.

Parts



WIFI

WPS Pair

WPS pin: 10311615

- Inteno-88C4 (5GHz)
- Inteno-88C4 (2.4GHz)

LAN

192.168.1.1 LAN

- Inteno_D8C0 192.168.1.233 1000M FD
- Inteno_88F0 192.168.1.241 1000M FD
- alex-hp 192.168.1.106 1000M FD
- iao6s-iPhone 192.168.1.234 5GHz
- android-8b631a5346ca0481 192.168.1.131 5GHz

WAN

Internet ONLINE

WAN IP(s) 10.10.1.181

Gateway(s) 10.10.1.254

Link Type Ethernet

Link Speed Auto-negotiated 1000 Mbps Full Duplex

DNS-Servers 10.10.1.2, 10.10.1.202

WAN Uptime 16m 38s

USB

VOICE

Schedule off

S0: Account 1

PROFILE

Fully Routed (NA) Change Profile

ain image

The overview has three parts: a , , and .

Device Network Map

The device map shows how your device is connected to the LAN and the WAN, as well as other devices in the local network.

Configuration Shortcuts

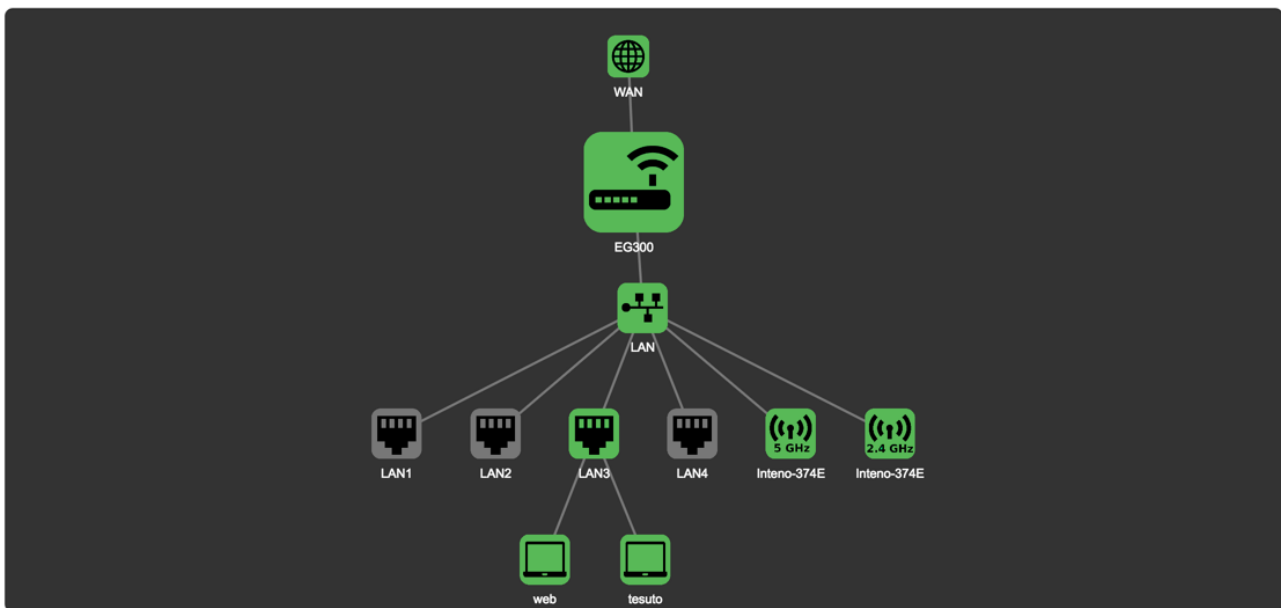
The shortcuts show you the main wireless, Ethernet, LAN, WAN, USB, voice and profile configurations.

Status Panels

The status panels display status information about selected features. They also allow you quick access to configuration of the most common features.

Device Network Map

The device map shows how your device is connected to the LAN and the WAN, as well as other devices in the local network.



ap

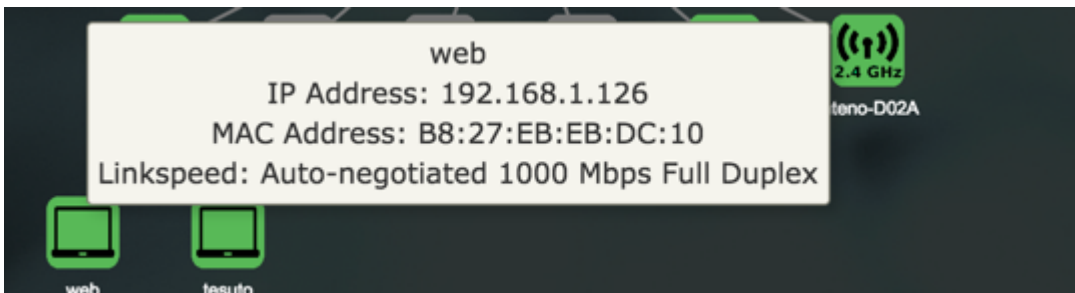
Colors

The status of a device is indicated by the color of the icon.

| Color | Status |
|--------|-------------------------|
| Green | Enabled and active |
| Black | Enabled, not active |
| Yellow | Active, with warnings. |
| Red | Active, not functional. |

Details

More detailed information about the status of an item in the map is available by pointing the cursor at an icon in the map.



etails

Edit Node Settings

You can edit the settings for a node directly from the Device Network Map.

To edit a settings for a node:

- Click the node in the map

A window containing settings tabs opens.

Status

The **Status** tab shows information about the client and the connection.

Static Leases

The **Static Leases** tab allows you to assign a static to the client.

Forwarding

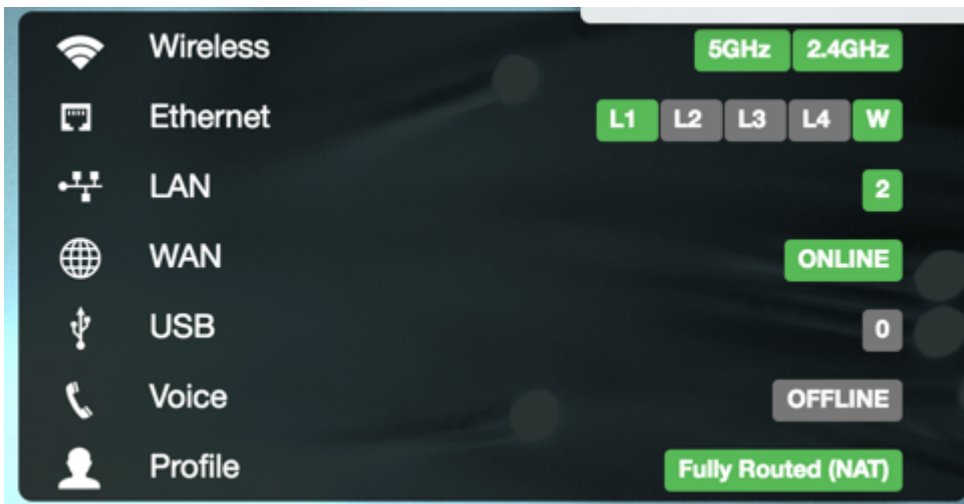
allows remote computers to connect to a specific device within your private network.

Parental Control

Parental control is used to restrict access to the network for particular devices.

Configuration Shortcuts

The shortcuts show you the main wireless, Ethernet, LAN, WAN, USB, voice and profile configurations.

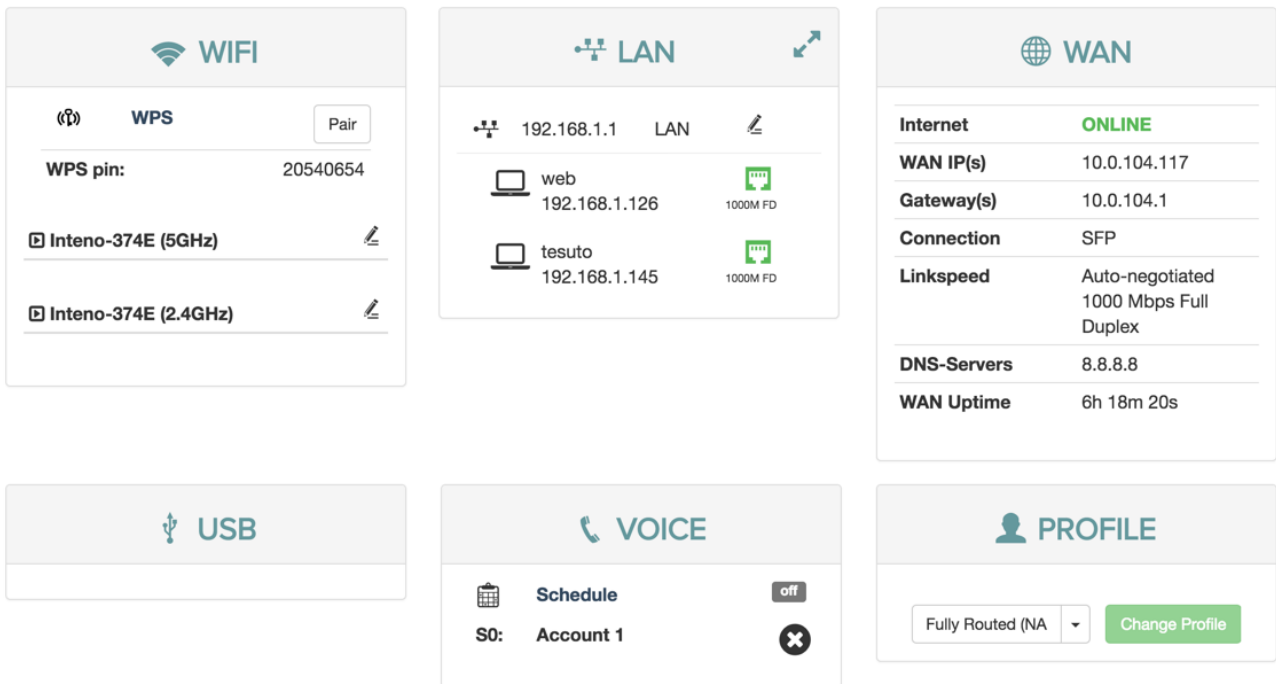


shortcuts

| Option | |
|----------|-----------------------|
| Wireless | Active . |
| Ethernet | in use on the device. |
| LAN | Active |
| WAN | Status of . |
| USB | Connected , if any. |
| Voice | , if any. |
| Profile | Selected , if any. |

Status Panels

The status panels display status information about selected features. They also allow you quick access to configuration of the most common features.



anel's

WiFi

The **WiFi status panel** lets you change the default wireless security settings () to make your network more secure. You can also view the wifi status and edit the .

LAN

The **LAN** panel shows basic information about the device and connected clients IP addresses.

From the status panel you can configure the settings for the device.

WAN

The **WAN** panel displays the status of your . It also lets you configure servers.

USB

The **USB** panel displays the status of any connected devices.

Voice

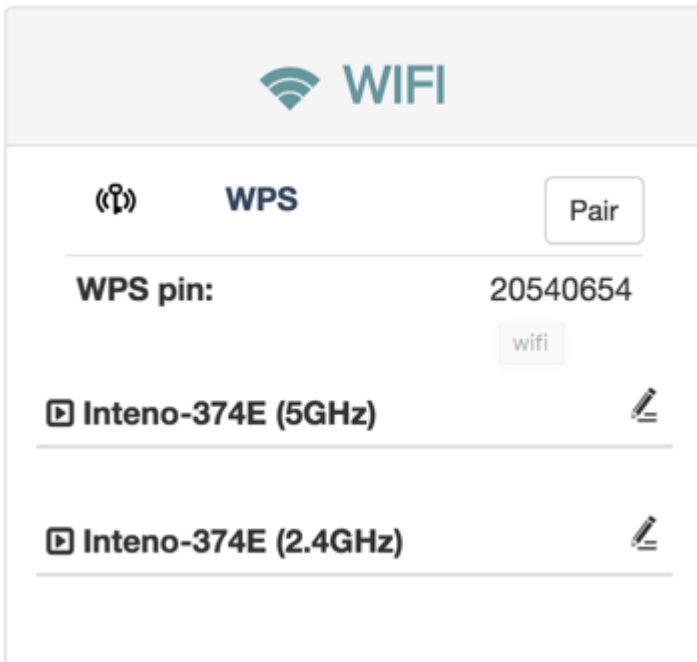
The **Voice** panel shows the status of the ringing schedule connected phone lines.

Profile

The **Profile** panel shows the configured on your device, if any.

WIFI

The **WiFi status panel** lets you change the default wireless security settings () to make your network more secure. You can also view the wifi status and edit the .



iFi panel

WPS settings

WPS makes it easier to connect other wireless devices to your device on an encrypted channel.

Edit 5GHz Wireless Interface

In the **edit wireless interface** view you can change different aspects of your interface.

Edit 2.4GHz Wireless Interface

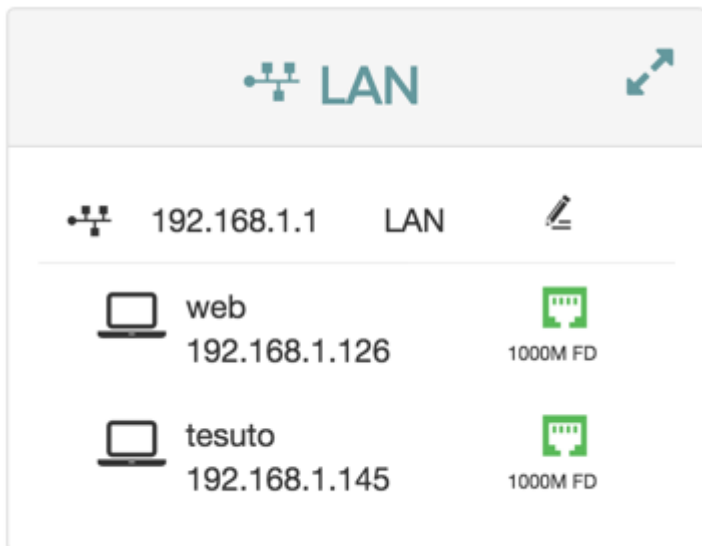
In the **edit wireless interface** view you can change different aspects of your interface.

LAN

The **LAN** panel shows basic information about the device and connected clients IP


addresses.

From the status panel you can configure the settings for the device.



AN panel

To open the **Edit LAN Settings** dialog, click the  **edit** button.

To view a more detailed overview of the clients, click the  **expand** button

To view details about a client click the client in the list.

Detailed Client Overview

In The **Detailed Client Overview**, information about the clients in the lan is displayed.

Edit LAN Settings

In The **Edit LAN settings** view you can change different features about your network.

Client

The **Client** dialog displays information about the connected clients and allows you to edit their configuration.

Detailed Client Overview

In The **Detailed Client Overview**, information about the clients in the lan is displayed.

Ethernet

| Hostname | IP Address | MAC Address | Port | Network | Linkspeed |
|----------|---------------|-------------------|------|---------|-----------------------|
| tesuto | 192.168.1.145 | 34:17:EB:EC:5D:DB | LAN3 | LAN | Auto-negotiated 10... |
| web | 192.168.1.126 | B8:27:EB:EB:DC:10 | LAN3 | LAN | Auto-negotiated 10... |

verview

| Item | Description |
|--------------|-----------------------------------|
| Hostname | Client . |
| IPv4 Address | Client . |
| MAC Address | Client . |
| Port | Device . |
| Network | Network interface for the client. |
| Link Speed | Type of , and for the connection. |

Edit LAN Settings

In The **Edit LAN settings** view you can change different features about your network.

Edit LAN Settings

IPv4 Address . . .

IPv4 Subnet Mask . . .

IPv4 Broadcast . . .

DHCP Server

DHCP Pool Start

DHCP Pool Size

DHCP Lease Time ▾

Static DHCP

▾

AN Settings

| Item | Description |
|---------------------|---|
| IPv4 Address | Device address |
| IPv4 Subnet Mask | IPv4 |
| IPv4 Broadcast Mask | IPv4 |
| DHCP Server | Turn on or off. |
| DHCP Pool Start | Start IP number for the start number |
| DHCP Pool Size | Number of IP addresses in the |
| DHCP Lease Time | DHCP for the LAN. |
| Static DHCP | Reserve an IP address for a connected device. |

Client

The **Client** dialog displays information about the connected clients and allows you to edit their configuration.

Information about the client is divided into several tabs.

| Status | Port Forwarding | Static Leases | Parental Control |
|------------------------|---------------------------------------|---------------|------------------|
| <h2>Client Status</h2> | | | |
| Hostname | web | | |
| IP Address | 192.168.1.126 | | |
| MAC Address | B8:27:EB:EB:DC:10 | | |
| DHCP | True | | |
| Connected | True | | |
| Link Speed | Auto-negotiated 1000 Mbps Full Duplex | | |

lient

Status

The **Status** tab shows information about the client and the connection.

Port Forwarding

In the **Port Forwarding** tab you can map incoming connections on different to ports on the client.

Static Leases

The **Static Leases** tab allows you to assign a static to the client.

Parental Control



Parental control is used to restrict access to the network for particular devices.

Parental Control

Parental control is used to restrict access to the network for particular devices.

Internet Access Scheduling

Parental control is handled by setting schedules where access is restricted to explicitly named addresses.

| Item | Description |
|---|----------------------------------|
| Weekdays | List of days the filter applies. |
| Start Time | Time of day to start filtering. |
| Stop Time | Time of day to stop filtering. |
|  | Edit filtering rule. |
|  | Delete filtering rule. |

WAN

The **WAN** panel displays the status of your . It also lets you configure servers.



The screenshot shows the WAN panel with a header containing a globe icon and the text 'WAN'. Below the header is a table with the following data:

| | |
|--------------------|---|
| Internet | ONLINE |
| WAN IP(s) | 10.0.104.117 |
| Gateway(s) | 10.0.104.1 |
| Connection | SFP |
| Linkspeed | Auto-negotiated 1000 Mbps Full Duplex |
| DNS-Servers | 8.8.8.8 |
| WAN Uptime | 6h 6m 56s |

WAN panel

| Item | Description |
|-------------|--|
| Internet | Status of Internet connection. |
| WAN IP(s) | IPv4 and address to the device. |
| Gateway(s) | IPv4 and address to . |
| Connection | Type of WAN connection. |
| DNS-Servers | IPv4 and IPV6 addresses to . |
| WAN uptime | Time since last disconnect for IPv4 and IPV6 WAN connection. |

USB

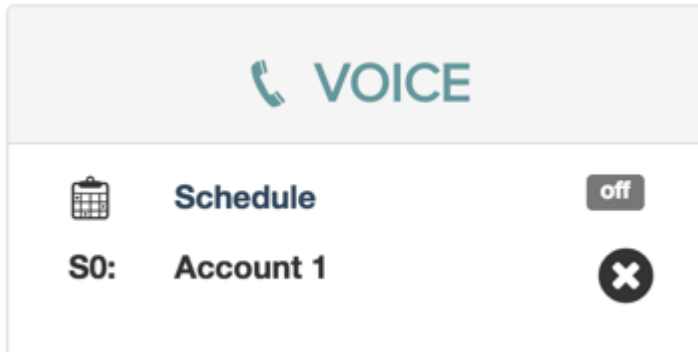
The **USB** panel displays the status of any connected devices.



SB panel

Voice

The **Voice** panel shows the status of the ringing schedule connected phone lines.



oice panel

The Voice panel is in certain regions.

Profile

The **Profile** panel shows the configured on your device, if any.

The network profiles are configured by the manufacturer for each device type.

Depending on the network profile selected, additional panels may be displayed in the

overview.

Voice

The **Voice** provides access to settings relating to voice communications through the device.

Call Log

The **Call Log** view shows a list of the recent calls handled through the device.

SIP Accounts

The **SIP Accounts** view shows information about configured for the device.

SIP Users

The **SIP Users** view shows information about configured for the device.

Voice Lines

The **Voice Lines** view shows a list of available voice lines for the device and allows you to configure them.

Advanced Settings

The **Advanced Settings** view contains advanced settings for SIP , voice lines and dial plans.

Number Blocking

The **Number Blocking** view allows you to block outgoing calls to specific numbers or or number ranges.

Ringling Schedule

The **Ringling Schedule** view lets you define when telephones should be allowed to ring.

Speed Dialing

The **Speed Dialing** view lets you configure a set of shortcode numbers that convert to the specified numbers when dialled.

DECT Radio

The **Dect Radio** view allows you to configure radio settings.

Call Log

The **Call Log** view shows a list of the recent calls handled through the device.

| Item | Description |
|-----------------|-----------------------|
| Date | Date for the call. |
| Time | Time for the call. |
| External Number | Calling number. |
| Internal Number | Receiving number. |
| Duration | Duration of the call. |

SIP Accounts

The **SIP Accounts** view shows information about configured for the device.

At the top of the page is a list of selectable accounts.

When a particular account is selected, details about it is shown in the configuration section.

| Item | Description |
|---------------------------|---|
| Enabled | Turn account on or off. |
| Account Name | Name of . |
| SIP domain name | Name of . |
| SIP Username | The for the account. |
| SIP Authentication Name | used with password to register with SIP server. |
| SIP Password | Enter new password to change. |
| Show Key Text | Display the password. |
| Display Name | Display name used in Caller ID. |
| SIP Server/Registrar | Address for . |
| SIP Server/Registrar Port | for . |
| SIP Outbound Proxy | Address for outbound . |
| SIP Outbound Proxy Port | for outbound . |
| Incoming Phone Lines | Check boxes for connected phone line ports. |
| Preferred codecs | Order of preference for . |
| G.711MuLaw Packetization | setting for . |
| G.726 Packetization | setting for . |
| G.729a Packetization | setting for . |
| G.G.729a Packetization | setting for . |

| | |
|---------------|---|
| Autoframing | Negotiate when call is established. |
| SIP Transport | // |
| Encryption | Use . |
| Use as Fax | Indicate that this SIP account will be used for a fax machine. This will force some settings. |
| Mailbox | Voicemail inbox. |

Add account

You can add as many accounts as you needed.

To add a account:

- Click the **Add** button
- Enter a **Name** for the account
- Enter values as needed.
- Click **Apply**

SIP Users

The **SIP Users** view shows information about configured for the device.

At the top of the page is a list of selectable accounts.

When a particular account is selected, details about it is shown in the configuration section.

| Item | Description |
|-----------------------------|-----------------------------------|
| Enabled | Turn user on or off. |
| Name | Display name used in Caller ID. |
| Extension | Extension for this user. |
| User Name | . |
| User Password | Enter new password to change. |
| Show Key Text | Display the password. |
| Call out using SIP provider | for outbound calls. |
| Mailbox | Voicemail inbox. |
| Preferred codecs | Order of preference for . |
| Host | Specific host for this user. |
| Qualify | Check that the user is reachable. |

Add user

You can add as many users as you needed.

To add a user:

- Click the **Add** button
- Enter a **Name** for the user
- Enter values as needed.
- Click **Apply**

Voice Lines

The **Voice Lines** view shows a list of available voice lines for the device and allows you to configure them.

Each available voice line has its own panel. Detailed information about each line is shown when you expand the panel.

The panels allow you to configure individual voice lines.

| Item | Description |
|--------------------------|---|
| Name | Identifier for the DECT line. |
| Internal Number | Direct call number. |
| Outgoing Calls Number | for external calls. |
| Call Waiting | Enable call waiting notification. |
| Call ID Restriction | Hide caller ID. |
| Voice Activity Detection | Detect voice (Transparent / Aggressive / Conservative). |
| Comfort Noise Generation | Generated noise (White / Hot / Spectrum estimate). |
| Echo cancellation | Remove echoes. |
| Transmit gain | Increase transmitted signal. |
| Receive gain | Increase received signal. |

Advanced Settings

The **Advanced Settings** view contains advanced settings for SIP , voice lines and dial plans.

SIP

The **Advanced SIP Settings** view lets you configure detailed parameters for your services.

Line

The **Advanced Line Settings** view lets you configure detailed parameters for your voice lines .

Dial Plan

The **Custom Dial plan** view allows you to configure dialling digits for various services and networks.

SIP

The **Advanced SIP Settings** view lets you configure detailed parameters for your services.

| Item | Description |
|-------------------------------|---|
| Sip Proxy servers | to allow incoming calls from. |
| Bind Interface | Restrict listening to particular WAN interface. |
| Bindport | to use for listening. |
| User Agent | Custom User - Agent information in the SIP header. |
| RTP Port Range | to use for |
| DTMF Mode | Mode for (Compatibility / RFC 2833 / SIP INFO / Inband). |
| Register Interval | Time in seconds between registration attempts. |
| Realm | for digest authentication. |
| Localnet | Network addresses that are considered inside of the network. |
| Register Attempts | Number of registration attempts before giving up. |
| Register Timeout | Time before giving up a registration attempt. |
| Register Back-off Attempts | Number of attempts before . |
| Register Back-off Timeout | Time in before giving up attempt to register. |
| Remote Hold | Send hold events to proxy (Let network handle music on hold). |
| SRV Lookup | Enable DNS lookup. |
| DNS Manager | Enable DNS manager. |
| DNS Manager Refresh Interval | Refresh interval for the DNS manager. |
| Line suffix in contact header | Add suffix to SIP contact header with information about called lines. |
| SIP DiffServ | type of service for SIP data. |
| Audio DiffServ | type of service for audio data. |
| Congestion tone | Tone to play on congestion. (Congestion / Info) |
| STUN server | service provider. |
| TLS/SSL Version | // . |
| Cipher string | identifier string. |
| Trusted CA | Public key for a trusted . |

Trusted CA Certificate

To add a Trusted CA Certificate key:

- Click **Add**
- Copy the public key
- Paste the key into the window
- Click **Save**
- Click **Apply**

Line

The **Advanced Line Settings** view lets you configure detailed parameters for your voice lines .

| Item | Description |
|--------------------------------|---|
| Locale selection | Country for device location. |
| Enable Jitter Buffer | Turn jitter prevention buffer on or off. |
| Force Jitter Buffer | Forces the receiver to use a . |
| Jitter Buffer implementation | The type of Fixed / Adaptive. |
| Maximum Jitter Buffer size | Size of (ms). |
| Enable Packet Loss Concealment | Turn on or off. |
| Inter-digit timeout | Time between dialled digits before timing out (ms). |

Dial Plan

The **Custom Dial plan** view allows you to configure dialling digits for various services and networks.

| Item | Description |
|----------------------|---|
| Enable incoming | Turn dial plan on or off for incoming calls. |
| Enable outgoing | Turn dial plan on or off for outgoing calls. |
| Enable custom hangup | Turn custom hang up on or off. |
| All Ports Extension | Port test extension. |
| Test Audio Extension | Audio tests the audio quality. |
| Test Echo Extension | Echo returns the outgoing audio from a channel back to the channel. |

Number Blocking

The **Number Blocking** view allows you to block outgoing calls to specific numbers or or

number ranges.

Outgoing


| Item | Description |
|---|--|
| Outgoing Number Blocking | Turn blocking on or off for outgoing calls. |
| Do not allow connections to these numbers | List of blocked numbers. |
| Block connections to all foreign numbers | Block calls to different locales. |
| Block connections to all special rate numbers | Block calls to premium rate or pay services. |

Incoming

| Item | Description |
|---|---|
| Incoming Number Blocking | Turn blocking on or off for incoming calls. |
| Do not allow connections from these numbers | List of blocked numbers. |

Block number


To block a number:

- Click the  **add** button
- Click in the **Phone extension** box
- Enter the number
- Click outside of the **Phone extension** box
- Click **Apply**

Block number range

You can use # as wildcard to define number ranges. For example “0160#” blocks all numbers starting with “0160”.

To block a sequence of numbers:

- Click the  **add** button
- Enter digits
- Add '#' as wildcard
- Enter the number
- Click outside of the **Phone extension** box
- Click **Apply**

Ringling Schedule

The **Ringling Schedule** view lets you define when telephones should be allowed to ring.

| Item | Description |
|------------------------------------|---|
| Ringling Schedule | Turn the schedule on or off. |
| During the times below ringling is | Enabled / Disabled. |
| Day | List of days when status applies. |
| Time | Time interval when status applies. |
| Status | Enabled / Disabled. |

Speed Dialing

The **Speed Dialing** view lets you configure a set of shortcode numbers that convert to the specified numbers when dialled.

The speed dialling list consists of the numbers 0 to 9. For each of these, you can add a number or extension that will be called when somebody dials the number.

| Item | Description |
|---|--------------------------------|
| Speed Dialing | Turn speed dialling on or off. |
| Remove all entries from speed dial list | Clears the list |

DECT Radio

The **Dect Radio** view allows you to configure radio settings.

| Item | Description |
|------------------|------------------------------------|
| DECT Radio | Auto / On / Off. |
| Radio Status | Current status for the DECT Radio. |
| Pair DECT Device | Button to start for a DECT device. |
| Codecs | DECT available for the device. |

At the bottom of the page is a list of currently devices.

| Item | Description |
|--------|--------------------------------|
| ID | Pairing ID. |
| IPUI | number. |
| Codecs | DECT available for the device. |

Network

The **Network** view provides access to the devices, connections and available configurations in the network.

Devices

The **Devices** view allows you to configure settings for various network types.

XDSL

The **xDSL** view allows you to configure line settings and profiles.

Connections

The **Connections** view allows you configure various connection interfaces to use in your device.

Routes

Static routes are useful if you have several networks accessible from your router and you want to correctly route packets between them.

Firewall

The firewall lets you filter traffic, set up port forwarding or expose particular services to the outside world.

Parental Control

Parental control is used to restrict access to the network for particular devices.

Quality Of Service

The **Quality Of Service** view allows you to configure parameters for through applying of to interfaces.

MultiWAN

The **MultiWAN** view allows you to create and configure WAN traffic divisions for and and apply traffic rules.

Services

The **Services** view allows you to configure the services connected device.

Devices

The **Devices** view allows you to configure settings for various network types.

Base Device

The **Base Device** view shows you a list of devices that are used to access the network.

Ethernet

The **Ethernet** view allows you to configure the physical ethernet interfaces of your device.

ADSL

The **ADSL** view allows you to configure devices.

VLAN

The **VLAN** view allows you to configure devices.

Base Device

The **Base Device** view shows you a list of devices that are used to access the network.

| Option | Description |
|---------|-----------------|
| Type | Type of device |
| Name | Name of device |
| Adapter | Adapter name |
| MAC | address |
| MTU | Number of bytes |
| Status | Device Status |

Device Status

The status of a device is indicated by the color of the icon.

| Color | Status |
|-------|--------|
|-------|--------|

| | |
|-------|---------------------|
| Green | Enabled and active |
| Black | Enabled, not active |

Note: These are the default colors. Your operator may use a different coloring scheme.

Ethernet

The **Ethernet** view allows you to configure the physical ethernet interfaces of your device.

The configuration is divided into multiple sections.

| Section | Description |
|----------------|---|
| Interface List | List of selectable the connected ethernet port devices. |
| Port Speed | Configuration of transmission speed, setting and . |
| Internet Port | Hardware to use for Internet traffic. |
| Bridge | Setting to enable use. |

Port Speed

Port speed settings affect how a LAN or WAN port negotiates the speed setting.

Negotiation can be turned off (speed setting: **only**) or use (speed setting **max**) to determine actual speed.

Communication on a port can be either half or full .

A port that is set to **disabled** does not handle any traffic.

ADSL

The **ADSL** view allows you to configure devices.

At the top of the page is a list of selectable devices.

When a particular device is selected, details about it is shown in the configuration section.

| Section | Description |
|--------------------|---------------------|
| Name | Name of the device. |
| VPI | ATM . |
| VCI | ATM . |
| DSL Link Type | // . |
| Encapsulation Mode | LLC / . |

| | |
|--------------|------------------------|
| Service Type | . |
| Bridge | Setting to enable use. |

Service Type

Service types define the guaranteed level of service in a network. This involves such things as the timing between the source and destination, the guaranteed bandwidth and how many cells get lost in transmission.

| Setting | Description |
|------------------|---------------------|
| UBR without PCR | Use without . |
| UBR with PCR | Use with . |
| CBR | Use . |
| Non-Realtime VBR | Use Non-Real-Time . |
| Realtime VBR | Use Real-Time . |

VDSL

The **VSDL** view allows you to configure devices.

At the top of the page is a list of selectable devices.

When a particular device is selected, details about it is shown in the configuration section.

| Section | Description |
|---------------------------|-------------------------|
| Name | Name of the device. |
| DSL Latency Path | DSL 1, 2 or both 1 & 2. |
| PTM Priority | Normal or High . |
| IP QoS Schedule Algorithm | / . |
| Bridge | Setting to enable use. |

Latency Path

The DSL Latency Path comes in three modes: *Path 1* (Fast), *Path 2* (Interleaved) and *Both 1 & 2*. Fast is used for applications sensitive to delay. Interleaved suits applications sensitive to errors.

PTM Priority

The PTM Propriety defines how traffic packets should be handled.

| Priority | Description |
|-----------------|--|
| Normal Priority | Sen packets according to their priority. |
| High Priority | Use preemption; lower-priority packets are paused when higher-priority packets are sent. |

IP Quality of Service Algorithm

The IP Quality of Service Algorithm determines which type of QoS to provide; or .

Strict Priority Precedence

Strict Priority Precedence means that where the the packets with the highest priority always are sent first.

Weighted Fair Queuing

Weighted Fair Queuing means that bandwidth is adjusted automatically according to traffic priority and weight value.

VLAN

The **VLAN** view allows you to configure devices.

At the top of the page is a list of selectable devices.

When a particular device is selected, details about it is shown in the configuration section.

| Section | Description |
|-------------|--------------------------|
| Name | Name of the device. |
| Base Device | to create interface for. |
| 802.1q | tag. |
| 802.1p | priority. |
| Bridge | Setting to enable use. |

802.1q

IEEE 802.1Q is a standard for Ethernet where VLANs are given a numeric tag. The tag is used to identify traffic in networks, and decide how to handle it.

This allows multiple bridged networks to share the same physical link without leaking information to each other networks.

802.1p

802.1p is a standard for priority levels, identifying the class of service a is to be used for. There are 8 different levels, numbered from 0 to 7.

| Priority | Acronym | Traffic types | Comment |
|----------|---------|------------------|---------|
| 0 | BK | Background | Lowest |
| 1 | BE | Best Effort | |
| 2 | EE | Excellent Effort | |

| | | | |
|---|----|-----------------------|-----------------------------|
| 3 | CA | Critical Applications | |
| 4 | VI | Video | < 100 ms latency and jitter |
| 5 | VO | Voice | < 10 ms latency and jitter |
| 6 | IC | Internet Control | |
| 7 | NC | Network Control | Highest |

XDSL

The **xDSL** view allows you to configure line settings and profiles.

The xDSL settings are divided into several tabs.

Modulation

The **modulation** tab lets you turn various line modulations on or off.

VSDL Profile

The **VSDL Profile** tab lets you turn various VDSL2 profiles on or off.

Capabilities

The **capabilities** tab lets you turn various xDSL capabilities on or off.

Modulation

The **modulation** tab lets you turn various line modulations on or off.

| Profile | Description | Down Mbit/s | Up Mbit/s |
|---------|--------------------|-------------|-----------|
| G.Dmt | G.Dmt modulation. | 12 | 1.3 |
| G.lite | G.lite modulation. | 1.5 | 0.5 |
| T.1413 | T.1413 modulation. | 8.1 | 1.5 |
| ADSL2 | ADSL2 modulation. | 12 | 1.0 |
| AnnexL | AnnexL modulation. | 5 | 0.8 |
| ADSL2+ | ADSL2+ modulation. | 24 | 1.0 |
| AnnexM | AnnexM modulation. | 24 | 3.5 |
| VDSL2 | VDSL2 modulation. | 100 | 100 |

VSDL Profile

The **VSDL Profile** tab lets you turn various VDSL2 profiles on or off.

| Profile | Bandwidth (MHz) | Downstream carriers | Carrier bandwidth (kHz) | Maximum downstream transmit power (dBm) | Max. downstream throughput (Mbit/s) |
|---------|-----------------|---------------------|-------------------------|---|-------------------------------------|
| 8a | 8.832 | 2048 | 4.3125 | +17.5 | 50 |
| 8b | 8.832 | 2048 | 4.3125 | +20.5 | 50 |
| 8c | 8.5 | 1972 | 4.3125 | +11.5 | 50 |
| 8d | 8.832 | 2048 | 4.3125 | +14.5 | 50 |
| 12a | 12 | 2783 | 4.3125 | +14.5 | 68 |
| 12b | 12 | 2783 | 4.3125 | +14.5 | 68 |
| 17a | 17.664 | 4096 | 4.3125 | +14.5 | 100 |

Capabilities

The **capabilities** tab lets you turn various xDSL capabilities on or off.

| Profile | Description | Comment |
|---------|------------------|----------------|
| US0 | Upstream 0 Band. | 20 to 138 kHz |
| Bitswap | . | Used for DMT . |
| SRA | . | |

Connections

The **Connections** view allows you configure various connection interfaces to use in your device.

This page allows to configure IP addresses used in your home network. In case DHCP is used, your router automatically assigns an IP address to devices connected to the network.

The page contains a list of interfaces, with one widget for each interface.

Connect

To connect a connection:

- Find the interface widget for the interface you are interested in
- Click **Connect** button

Disconnect

To disconnect a connection:

- Find the interface widget for the interface you are interested in
- Click **Edit** button

Create Interface

The **Create New Network Interface** dialog allows you to create a new according to your needs.

Configure Interface

You can configure the settings for interfaces from the page.

Create Interface

The **Create New Network Interface** dialog allows you to create a new according to your needs.

The dialog is a wizard where you add information in several steps.

The number of steps and their contents varies depending on the type of interface you create.

Note: As a last step you finalize the setup, but you can further from the page.

Connection Types

In the first step, you can choose the type of interface: Uplink, Downlink, or Unmanaged.

Depending on your choice in the first step, different options become available.

Uplink

An uplink interface type is an interface to services.

Downlink

A Downlink interface is an interface to subscribers/clients.

Unmanaged

The interface protocol type Unmanaged means that the connection has no defined protocol.

Uplink

An uplink interface type is an interface to services.

Interfaces

DHCP v4

An DHCP v4 connection uses an IPv4 address provided by a DHCP server.

DHCP v6 (Uplink)

An DHCP v6 connection uses an IPv6 address provided by a DHCP server.

Point-to-Point Protocol

A Point-to-Point Protocol connection uses PPP to establish the network.

Point-to-Point Protocol over Ethernet

A Point-to-Point Protocol over Ethernet connection uses PPPoE to establish the network.

Point-to-Point Protocol over ATM

A Point-to-Point Protocol over ATM connection uses PPPoA to establish the network.

3G

A 3G connection uses over *///*.

Point-to-point Tunnel

A Point-to-Point Tunnel connection uses across a tunnel to establish the network.

IPv6 Tunnel in IPv4

A IPv6 Tunnel in IPv4 connection uses IPv4 to transmit IPv6 traffic.

IPv6 Tunnel to IPv4

A IPv6 Tunnel to IPv4 connection uses IPv4 to transmit IPv6 traffic.

IPv6 rapid deployment

A IPv6 rapid deployment interface for IPv4 infrastructures.

WWAN (LTE/HSPA+)

The WWAN connection uses / .

WWAN

A Wireless Wide Area Network (WWAN), is a wireless network that extends over a large geographical distance.

LTE

Long-Term Evolution (LTE) is a standard for high-speed wireless communication for mobile phones and data terminals, based on and .

HSPA / HSPA+

High Speed Packet Access (HSPA) is an extension of 3G mobile networks utilizing .

Evolved High Speed Packet Access (HSPA+) is a further improvement on HSPA allowing for higher speeds.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

DHCP v6 (Uplink)

An DHCP v6 connection uses an IPv6 address provided by a DHCP server.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol, adapter and firewall settings for the interface.

| Item | Description |
|--------------------------------|--------------------------|
| Protocol | Select . |
| Interface Type | Select . |
| Ethernet Adapter | to create interface for. |
| Add network to a firewall zone | Connects interface to . |

DHCP v4

An DHCP v4 connection uses an IPv4 address provided by a DHCP server.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol, adapter and firewall settings for the interface.

| Item | Description |
|------|-------------|
|------|-------------|

| | |
|--------------------------------|--------------------------|
| Protocol | Select . |
| Interface Type | Select . |
| Ethernet Adapter | to create interface for. |
| Add network to a firewall zone | Connects interface to . |

Point-to-Point Protocol

A Point-to-Point Protocol connection uses PPP to establish the network.

PPP

Point-to-Point Protocol (PPP) is a protocol for providing a direct data link connection with authentication, encryption and compression.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

Point-to-Point Protocol over Ethernet

A Point-to-Point Protocol over Ethernet connection uses PPPoE to establish the network.

PPPoE

PPP over Ethernet (PPPoE) is a protocol using to provide an Internet connection over , by putting PPP frames inside Ethernet .

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|--------------------------|
| Protocol | Select . |
| Ethernet Adapter | to create interface for. |
| Add network to a firewall zone | Connects interface to . |

Point-to-Point Protocol over ATM

A Point-to-Point Protocol over ATM connection uses PPPoA to establish the network.

PPPoA

PPP over ATM (PPPoA) is a protocol using to provide an Internet connection over .

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|--------------------------|
| Protocol | Select . |
| Ethernet Adapter | to create interface for. |
| Add network to a firewall zone | Connects interface to . |

3G

A 3G connection uses over ///.

3G

Third-generation wireless telephone technology (3G), is a cellular network for digital mobile data communication for broadband traffic.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

Point-to-point Tunnel

A Point-to-Point Tunnel connection uses across a tunnel to establish the network.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PTPT) is a technology for through and a with packets.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|------|-------------|
|------|-------------|

| | |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

IPv6 Tunnel in IPv4

A IPv6 Tunnel in IPv4 connection uses IPv4 to transmit IPv6 traffic.

6in4

6in4 is a method to transmit traffic over explicit connections.

The traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

IPv6 Tunnel to IPv4

A IPv6 Tunnel to IPv4 connection uses IPv4 to transmit IPv6 traffic.

6to4

6to4 is a method to transmit traffic over networks without having to configure explicit tunnels.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

IPv6 rapid deployment

A IPv6 rapid deployment interface for IPv4 infrastructures.

6rd

6rd is a method for rapid deployment on Internet Service Provider infrastructures, operating within the ISP's network.

Wizard

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|----------------|-------------------------|
| Interface Name | Name for the interface. |
| Interface Type | Select . |

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description |
|--------------------------------|-------------------------|
| Protocol | Select . |
| Add network to a firewall zone | Connects interface to . |

Downlink

A Downlink interface is an interface to subscribers/clients.

Finalize

In the final step you select protocol and firewall settings for the interface.

| Item | Description | Applies to |
|--------------------------------|--|-------------------|
| Interface Type | Select (Standalone / Anywan / Bridge). | |
| Physical Device | Device(s) to use for the connection. | |
| Add network to a firewall zone | Connects interface to . | |

Physical Device

For Standalone, you need to select the to use for the connection.

For Anywan and Bridge, you need to add a physical device to use for the connection.

| Item | Description | Applies to |
|------------------|--|-------------------|
| Ethernet Adapter | Selector for to use for the connection. | Standalone |
| Add Device | Dialog to select network device to use for the connection. | Anywan / Bridge |

Ethernet Adapter

- Select a base device from the dropdown menu.

Add Device

- Click **Add**

The **Select Network Device** dialog is shown.

- Select a network device from the dropdown menu

Unmanaged

The interface protocol type Unmanaged means that the connection has no defined protocol.

Step 1

In the first step you select basic settings for the interface.

| Item | Description |
|--------------------|-------------|
| Interface Type | Select . |
| Add/Remove Devices | Select . |

- Select Interface Type
- Add as many devices as needed

Add Device

- Click **Add**

The Add Device dialog is shown.

- Select a network device from the dropdown menu
- Click **OK**

Finalize

- Click **OK** again
- Click **Apply**

Configure Interface

You can configure the settings for interfaces from the page.

Edit Connections

To edit a connection:

- Click **Edit** button

The **Connection Section** is displayed at the bottom of the page.

The connection section consists of a number of tabs, showing details the connection.

Depending on connection type the tabs will be different, but the standard tabs are **General**, **Physical Settings**, and **Advanced**.

Additional tabs become visible as they are needed.

Default Connections

LAN

The default LAN connection is a DHCP v4 connection using a static IPv4 address.

WAN

The default WAN connection uses an IPv4 address provided by a DHCP server.

WAN6

The default WAN6 connection is a IPv6 address provided by a DHCP server.

Connection Types

Unmanaged

An unmanaged connection has no predefined protocol for the connection.

Static Address

A static address uses a fixed IP address for the connection.

DHCP v4

An DHCP v4 connection uses an IPv4 address provided by a DHCP server.

DHCP v6

An DHCP v6 connection uses an IPv6 address provided by a DHCP server.

Point-to-Point Protocol

A Point-to-Point Protocol connection uses PPP to establish the network.

Point-to-Point Protocol over Ethernet

A Point-to-Point Protocol over Ethernet connection uses PPPoE to establish the network.

Point-to-Point Protocol over ATM

A Point-to-Point Protocol over ATM connection uses PPPoA to establish the network.

3G

A 3G connection uses over *///*.

4G

A 4G connection uses interface over */* .

Point-to-point Tunnel

A Point-to-Point Tunnel connection uses across a tunnel to establish the network.

IPv6 Tunnel in IPv4

A IPv6 Tunnel in IPv4 connection uses IPv4 to transmit IPv6 traffic.

IPv6 Tunnel to IPv4

A IPv6 Tunnel to IPv4 connection uses IPv4 to transmit IPv6 traffic.

IPv6 rapid deployment

A IPv6 rapid deployment interface for IPv4 infrastructures.

Edit (ade:network:connections:6rd:start)

Dual-Stack Lite

A Dual-Stack Lite connection uses through an to establish the network.

Point-to-Point Protocol over L2TP

A Point-to-Point Protocol over L2TP connection uses PPP and L2TP server to establish the network.

LAN

The default LAN connection is a DHCP v4 connection using a static IPv4 address.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

DHCP

The DHCP tab allows you to enable and use a specific DHCP server for the connection.

WAN

The default WAN connection uses an IPv4 address provided by a DHCP server.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

WAN6

The default WAN6 connection is a IPv6 address provided by a DHCP server.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Unmanaged

An unmanaged connection has no predefined protocol for the connection.

Unmanaged

The interface protocol type Unmanaged means that the connection has no defined protocol.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Static Address

A static address uses a fixed IP address for the connection.

Static address

A static IP address is an address that doesn't change, unless manually changed by the administrator.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

DHCP

The DHCP tab allows you to enable and use a specific DHCP server for the connection.

DHCP v4

An DHCP v4 connection uses an IPv4 address provided by a DHCP server.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

DHCP v6

An DHCP v6 connection uses an IPv6 address provided by a DHCP server.

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Point-to-Point Protocol

A Point-to-Point Protocol connection uses PPP to establish the network.

PPP

Point-to-Point Protocol (PPP) is a protocol for providing a direct data link connection with authentication, encryption and compression.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Point-to-Point Protocol over Ethernet

A Point-to-Point Protocol over Ethernet connection uses PPPoE to establish the network.

PPPoE

PPP over Ethernet (PPPoE) is a protocol using to provide an Internet connection over , by putting PPP frames inside Ethernet .

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Point-to-Point Protocol over ATM

A Point-to-Point Protocol over ATM connection uses PPPoA to establish the network.

PPPoA

PPP over ATM (PPPoA) is a protocol using to provide an Internet connection over .

General

The general tab contains status information and settings relating to the protocol.

Physical Settings

The physical settings tab contains settings for hardware management and devices for the connection.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

3G

A 3G connection uses over *///*.

3G

Third-generation wireless telephone technology (3G), is a cellular network for digital mobile data communication for broadband traffic.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

WWAN (LTE/HSPA+)

The WWAN connection uses / .

WWAN

A Wireless Wide Area Network (WWAN), is a wireless network that extends over a large geographical distance.

LTE

Long-Term Evolution (LTE) is a standard for high-speed wireless communication for mobile phones and data terminals, based on and .

HSPA / HSPA+

High Speed Packet Access (HSPA) is an extension of 3G mobile networks utilizing .

Evolved High Speed Packet Access (HSPA+) is a further improvement on HSPA allowing for higher speeds.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

4G

A 4G connection uses interface over / .

4G

Fourth-generation wireless telephone technology (4G), is a cellular network for digital mobile data communication for high-speed broadband.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Point-to-point Tunnel

A Point-to-Point Tunnel connection uses across a tunnel to establish the network.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PTPT) is a technology for through and a with packets.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

IPv6 Tunnel in IPv4

A IPv6 Tunnel in IPv4 connection uses IPv4 to transmit IPv6 traffic.

6in4

6in4 is a method to transmit traffic over explicit connections.

The traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

IPv6 Tunnel to IPv4

A IPv6 Tunnel to IPv4 connection uses IPv4 to transmit IPv6 traffic.

6to4

6to4 is a method to transmit traffic over networks without having to configure explicit tunnels.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

IPv6 rapid deployment

A IPv6 rapid deployment interface for IPv4 infrastructures.

Edit (ade:network:connections:6rd:start)

6rd

6rd is a method for rapid deployment on Internet Service Provider infrastructures, operating within the ISP's network.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Dual-Stack Lite

A Dual-Stack Lite connection uses through an to establish the network.

DS-Lite

Dual-Stack Lite (DS-Lite) is a method for sharing of addresses by combining and .

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Point-to-Point Protocol over L2TP

A Point-to-Point Protocol over L2TP connection uses PPP and L2TP server to establish the network.

PPP

Point-to-Point Protocol (PPP) is a protocol for providing a direct data link connection with authentication, encryption and compression.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a protocol used to support , where security is provided in the transmitted packages rather than in the tunneling.

General

The general tab contains status information and settings relating to the protocol.

Advanced

The advanced tab contains settings for management of advanced features for the connection.

Routes

Static routes are useful if you have several networks accessible from your router and you want to correctly route packets between them.

IPv4 Routes

The IPv4 section lets you add for .

IPv6 Routes

The IPv4 section lets you add for .

Add Static Route

To add a static route:

- Click the **add** button
- Enter information for the route fields.
- Click **Apply**

IPv4 Routes

The IPv4 section lets you add for .

| Item | Description | |
|-----------|------------------------------|--|
| Interface | Affected for the route. | |
| Target | Destination . | |
| Netmask | Applicable . | |
| Gateway | IP address to the internet . | |
| Metric | Route . | |
| MTU | size to use. | |
| Delete | Remove route. | |

IPv6 Routes

The IPv4 section lets you add for .

| Item | Description | |
|-----------|------------------------------|--|
| Interface | Affected for the route. | |
| Target | Destination . | |
| Gateway | IP address to the internet . | |
| Metric | Route . | |
| MTU | size to use. | |
| Delete | Remove route. | |

Firewall

The firewall lets you filter traffic, set up port forwarding or expose particular services to the outside world.

General Settings

The **general settings** view allows you to turn the firewall on or off.

Zones

The **Zones** view lets you can configure to group your firewall rules.

Rules

Firewall rules are more fine grained filtering rules for filtering your traffic.

Forwarding

allows remote computers to connect to a specific device within your private network.

DMZ / Exposed Host

A local network device can be made an *Exposed Host*. It is placed in the outside of the firewall, which provides unrestricted Internet access to the network device.

General Settings

The **general settings** view allows you to turn the firewall on or off.

Firewall Settings

To enable the firewall:

- Click **Enable Firewall**

Zones

The **Zones** view lets you can configure to group your firewall rules.

At the top of the page is a list of selectable zones.

By default this list contains the LAN and WAN zones, which contain default settings for local and Internet traffic.

When a particular interface is selected, details about it is shown in the configuration section.

Zone configuration

| Item | Description |
|------------------------------------|---------------------------------------|
| Name | Identifier for the zone. |
| Default policy | Default behavior for various traffic. |
| Masquerading | Enable firewall . |
| MSS Clamping | limit. |
| Allow forward to destination zones | Check zones to permit forwarding. |
| Allow forward from source zones | Check zones to permit forwarding. |

| | |
|--------------|---------------------------------------|
| Zone members | Interfaces that are part of the zone. |
|--------------|---------------------------------------|

Default Policy

The default policy setting defines firewall rules that apply unless specific rules override them.

| Item | Description |
|---------|----------------------------|
| Input | Incoming traffic from WAN. |
| Output | Outgoing traffic to WAN. |
| Forward | Traffic from LAN to WAN. |

The different default policy values determine the firewall behavior, through the firewall actions:

Firewall Action

The firewall action defines how traffic is handled by the firewall.

| Item | Description |
|---------|-------------------------|
| ACCEPT | Allow the traffic. |
| REJECT | Refuse the traffic. |
| DROP | Ignore the traffic. |
| FORWARD | Pass the traffic along. |

Add Firewall Zone

To add a firewall zone:

- Click the **Add** button
- Enter information in the fields
- Click **Apply**

Once the zone has been created, you can use it with your .

Add Zone Members

If you have networks/devices set up, you can add them to the zone.

To add a device as a zone member:

- Click the **Add** button

The **Select network device** dialog opens.

- Open the **select network** menu

- Select the device
- Click **OK**
- Click **Apply**

Rules

Firewall rules are more fine grained filtering rules for filtering your traffic.

At the top of the page is a list of selectable interfaces.

When a particular interface is selected, details about it is shown in the configuration section.

Where applicable, the configuration is divided into separate sections for **source** and **destination** zones.

| Item | Description |
|-----------------|--|
| Name | Identifier for the rule. |
| Zone | Device / Any / LAN / WAN |
| IP | / address. |
| MAC | address. |
| Port | affected. |
| IP version | Any / / |
| Protocol | Protocol affected: (/ / / TCP + UDP /) |
| Firewall action | to perform. |

Add Firewall Rule

If you have networks/devices set up, you can add them to the zone.

To add a device as a zone member:

- Click the **Add** button



The **Select network device** dialog opens.

- Open the **Select network** menu
- Select the device
- Click **OK**
- Click **Apply**

Reorder Firewall Rules

The firewall rules are applied in order from top to bottom in the list.

You can rearrange the rules by using the buttons:

| | |
|---|-----------|
|  | Move up |
|  | Move down |

Forwarding

allows remote computers to connect to a specific device within your private network.

The forwarding list shows information about any configured port forwarding rules.

| Item | Comment |
|-----------------|-----------------------------|
| Name | Identifier for the mapping. |
| Direction | involved |
| Dst. IP Address | Client address. |
| Protocol | Mapping (// TCP + UDP). |
| Public port(s) | Public (external) . |
| Private port(s) | Private (client) . |

Port Mapping Settings

To map incoming connections:

- Click the  **add** button to open the settings

The port mapping dialog lets you add configuration settings for the mapping.

Ports can be added one by one (80) or as ranges (21 : 22).

- Add information:
 - Add a name as identification
 - Add ports:
 - Add public/incoming port(s)
 - Add private/client port(s)
 - Select protocol
- Click **Save**
- Click **Close**

Your information is saved and is visible in the mapping list.

Add or Edit Port Mapping

The **Add or Edit Port Mapping** view allows you to add or change mapping settings.

| Item | Comment |
|-------------------|---------------------------|
| Rule Name | Rule name. |
| Source Zone | Incoming . |
| Destination Zone | Destination . |
| Source IP Address | Source (for filtering). |
| Dst. Device | Client . |
| Dst. IP Address | Client address. |
| Protocol | Mapping (// TCP + UDP). |
| Public port(s) | Public (external) . |
| Private port(s) | Private (client) . |
| NAT Loopback | Enable |

Protocol

The protocol setting filters traffic by protocol for the port forward.

| Protocol | Description |
|-----------|-------------|
| TCP + UDP | Both and . |
| TCP | only. |
| UDP | only. |

Add or Edit Port Mapping

The **Add or Edit Port Mapping** view allows you to add or change mapping settings.

| Item | Comment |
|-------------------|---------------------------|
| Rule Name | Rule name. |
| Source Zone | Incoming . |
| Destination Zone | Destination . |
| Source IP Address | Source (for filtering). |
| Dst. Device | Client . |
| Dst. IP Address | Client address. |
| Protocol | Mapping (// TCP + UDP). |
| Public port(s) | Public (external) . |
| Private port(s) | Private (client) . |
| NAT Loopback | Enable |

Protocol

The protocol setting filters traffic by protocol for the port forward.

| Protocol | Description |
|-----------|-------------|
| TCP + UDP | Both and . |
| TCP | only. |
| UDP | only. |

DMZ / Exposed Host

A local network device can be made an *Exposed Host*. It is placed in the outside of the firewall, which provides unrestricted Internet access to the network device.

| | |
|----------------------|---------------------------------------|
| WAN IP Address | Public and address for the DMZ. |
| Host IPv4 Address | IPv4 of device to place in DMZ. |
| Host IPv6 Address | IPv6 of device to place in DMZ. |
| Select Existing Host | Dropmenu to select connected devices. |

Add Exposed Host

To allow DMZ/exposed host:

- Click **Enable** to enable an exposed host
- Enter the local IP address to expose
- Alternatively, click **select existing host**

Note: You should also configure the DMZ IP address as static DHCP address for your device.

Parental Control

Parental control is used to restrict access to the network for particular devices.

Internet Access Scheduling

Parental control is handled by setting schedules where access is restricted to explicitly named addresses.

| Item | Description |
|------------|----------------------------------|
| Weekdays | List of days the filter applies. |
| Start Time | Time of day to start filtering. |
| Stop Time | Time of day to stop filtering. |

| | |
|---------------|---------------------------|
| MAC Addresses | List of device addresses. |
|---------------|---------------------------|

Start and Stop Times

The start time for a rule has to be lower than the end time.

If you want to have a rule that goes over midnight, you need to add two rules, one up until midnight, and one from midnight to when you want the rule to end.

For example:

Rule one: **From** 21:00 **To** 23:59 Rule two: **From** 00:00 **To** 06:00

A single rule of **From** 21:00 **To** 06:00 will **not** be saved.

Quality Of Service

The **Quality Of Service** view allows you to configure parameters for through applying of to interfaces.

Interface views

Interface

The **interface** tab lets you select interfaces and configure profiles for them.

Class

The **class** tab lets you manage QoS [classes](#).

Classification Group

The **Classification Group** tab lets you manage groupings of .

This is useful when you have multiple and want to manage classes differently for them.

Classify

The **classify** tab lets you configure filtering parameters in order to define types of traffic to include in which .

Workflow

Workflow

In order to use on the traffic for your device, you need to perform a number of configurations.

1: Class

The define how network traffic is to be prioritized and allocated.

There are a number of predefined classes, but you can add your own.

2: Classify

In order to direct traffic to the correct classes, you need to define classification rules in the **Classify** tab.

3: Group

With the classes defined, you can add and order them in a class group in the **Group** tab.

If you have multiple interfaces, and want different QoS settings for them, you can create multiple class groups.

4: Enable

As a final step, you enable QoS for the desired interface in the **Interface** tab.

Interface

The **interface** tab lets you select interfaces and configure profiles for them.

Overview

At the top of the page is a list of selectable interfaces.

When a particular interface is selected, details about it is shown in the configuration section.

| Item | Description | | |
|----------------------|---|--|--|
| Enable QoS | Turn the on for the interface. | | |
| Classification Group | to use for the interface. | | Note: You need to for it to be available in the list. |
| Calculate Overhead | Include in the packet calculations for and . | | |
| Limit Download Speed | Restrict the network speed <i>to</i> clients. | | |
| Limit Upload Speed | Restrict the network speed <i>from</i> clients. | | |

Add Interface

To add an interface:

- Click the **Add** button

The interface dialog opens.

- Select an **Interface** from the list
- Click **OK**
- Enable other settings as needed:
 - Turn QoS on with the **Enable QoS** slider
 - Select an available **Classification Group**
 - Turn QoS on with the **Limit Download Speed** slider
 - Enter a speed value (kbps)
 - Turn QoS on with the **Limit Upload Speed** slider
 - Enter a speed value (kbps)
- Click **Apply**

Class

The **class** tab lets you manage QoS [classes](#).

Overview

At the top of the page is a list of selectable classes.

When a particular class is selected, details about it is shown in the configuration section.

| Item | Description | Comment |
|--------------|---------------------------------|-----------|
| Priority | Bandwidth allocation limit (%). | |
| Average Rate | Average target rate (%). | |
| Limit Rate | Maximum allowed (%). | |
| Packet Size | Size of (bytes). | See note. |
| Packet Delay | Target for packets (ms). | See note. |
| Max Size | Maximum size of (bytes). | |

Note: Packet Size and Packet Delay rely on the Average Rate setting. The average rate is impacted by the maximum packet delay and the transfer time for the packet size. Generally the delay is lower for smaller packet sizes.

Add Class

You can add as many classes as you like.

To add a class:

- Click the **Add** button
- Enter a **Name** for the class
- Enter QoS values as needed.

- Click **Apply**

Classification Group

The **Classification Group** tab lets you manage groupings of .

This is useful when you have multiple and want to manage classes differently for them.

Overview

At the top of the page is a list of selectable classification groups.

When a particular group is selected, details about it is shown in the configuration section.

| Item | Description | Comment |
|---------------|--|--|
| Default Class | Class to use as fallback if packets don't match any other class. | |
| Classes | Classes to include in the group. | Note: You need to for it to be available in the list. |

The **Default** Classgroup contains these [standard classes](#): - **Priority** - **Express** - **Normal** - **Bulk**

Add Classification Group

To add a class group:

- Click the **Add** button
- Enter a **Name** for the group
- Select **Default group**
- Add classes as needed:
 - Click **Add a new class**
 - Select the desired class from the list
- Click **Apply**

Classify

The **classify** tab lets you configure filtering parameters in order to define types of traffic to include in which .

Overview

At the top of the page is a list of selectable classification groups.

When a particular group is selected, details about it is shown in the configuration section.

Adding a parameter will filter out traffic according to the parameters and assign it to the

group.

| Item | Description |
|-------------------|--|
| Target | to assign. |
| Protocol | Protocol affected (All / / /). |
| Source Host | (All / Specific host). |
| Destination Host | (All / Specific host). |
| Ports | Included anywhere . |
| Source Ports | Included in source. |
| Destination Ports | Included in destination. |
| Port Range | Range of anywhere. |
| Precedence | . |
| Packet Size | Size of to match. |
| Direction | (Both / In / Out) |
| Mark | Hexadecimal to att to the packets. (0x000000-0xFFFFFFFF) |
| Connbytes | for when to start filtering. |
| TCP flags | to match. |

Add Filter



To add a filter:

- Click the **Add** button
- Select **Classification group**
- Enter QoS values as needed.
- Click **Apply**

Reorder

The filters are prioritized in order from top to bottom in the list.

You can rearrange the classes by using the buttons:

| | |
|---|-----------|
|  | Move up |
|  | Move down |

Workflow

In order to use on the traffic for your device, you need to perform a number of configurations.

Process

Configuration steps

The order of operations involved in configuring QoS is different from the order in which the interface displays the setting tabs. Not all settings are needed in all cases.

1: Class

The define how network traffic is to be prioritized and allocated.

There are a number of predefined classes, but you can add your own.

2: Classify

In order to direct traffic to the correct classes, you need to define classification rules in the **Classify** tab.

3: Group

With the classes defined, you can add and order them in a class group in the **Group** tab.

If you have multiple interfaces, and want different QoS settings for them, you can create multiple class groups.

4: Enable

As a final step, you enable QoS for the desired interface in the **Interface** tab.

MultiWAN

The **MultiWAN** view allows you to create and configure WAN traffic divisions for and and apply traffic rules.

The MultiWAN settings are divided into tabs.

MultiWAN Settings

The **MultiWAN Settings** tab allows you to turn MultiWAN feature on or off, and configure Mutiple WAN connections.

Traffic Rules

The **Traffic Rules** tab allows you to filter LAN traffic and assign it to the appropriate WAN.

MultiWAN Options

Some aspects of MultiWan configuration require a bit of thinking and decisions.

MultiWAN Settings

The **MultiWAN Settings** tab allows you to turn MultiWAN feature on or off, and configure Multiple WAN connections.

Below the general settings is a list of selectable WANs.

When a particular WAN is selected, details about it is shown in the configuration section.

| Item | Description |
|------------------------------|---|
| Load Balancer Distribution | Disable / 1-10 (only used in balancer mode. |
| Health Monitor Method | Ping / Statistics. |
| Health Monitor Interval | Time between health checks. |
| Health Monitor ICMP Host(s) | host. |
| Health Monitor ICMP Timeout | timeout. |
| Attempts Before WAN Failover | Number of connection attempts before switching to failover WAN. |
| Attempts Before WAN Recovery | Number of connection attempts before attempting to recover WAN. |
| Failover Traffic Destination | Destination for traffic in case of failover. (Fast/ Load). |
| DNS Server(s) | Specified DNS / Automatic Selection / Customized DNS |

Add WAN

You can add as many WANS as you have WAN connections.

To add a WAN:

- Click the **Add** button
- Select an available WAN

A new WAN is added to the list.

- Edit the parameters as needed.
- Click **Apply**

Add Custom DNS Servers

To add a custom DNS server:

- Open the **DNS Server(s)** dropdown menu
- Select **Custom**

Click the  **add** button

- Add the IP numbers to the DNS server
- Click **Save**

Traffic Rules

The **Traffic Rules** tab allows you to filter LAN traffic and assign it to the appropriate WAN.

At the top of the page is a list of rules.

When a particular rule is selected, details about it is shown in the configuration section.

| Item | Description |
|---------------------|---------------------------------|
| Source Address | Originating device. |
| Destination Address | External target address. |
| Protocol | Protocol affected: (/ / |
| Ports | |
| WAN Uplink | Target WAN or balancing option. |

Add Rule

You can add as many rules as you like.

To add a rule:

- Click the **Add** button

A new rule is added to the list.

- Edit the parameters as needed.
- Click **Apply**

MultiWAN Options

Some aspects of MultiWan configuration require a bit of thinking and decisions.

Sample Configurations

Example configurations for failover and balancer are available from the [OpenWRT site](#)

Load Balancer Weights

You can add any number of servers to a server load balancing action. You can also add a weight to each server to make sure that your most powerful servers are given the heaviest load.

The weight refers to the proportion of load that the XTM device sends to a server. By default, each server has a weight of 1.

If you assign a weight of 2 to a server, you double the number of sessions that the XTM device sends to that server, compared to a server with a weight of 1.

Load Balancing Interfaces

If an interface is not specified for some particular traffic - and metric and weight are the same - the default behavior is to use both interfaces, which is the Linux default load sharing mechanism.

Interface Selection

When selecting which interface weights you need to take into account how the operator handles traffic. For example, usually a fiber or DSL WAN connection should have higher weight than a mobile connection.

Health Monitor Ping / Statistics

-Health Monitor Method Ping / Statistics. Ping I understand. What kind of statistics are used? Where can one configure statistics limits? E.g if you monitor like wan stats when does the box determine that interface has failed ? No stats at all at some interval? Some stats in some interval but it doesn't trigger wan failover because.....?

Ping and Statistics are health monitor methods.

Statistics checks the rx bytes value with the Health Monitor Interval, and if the value has not changed it marks the link as unhealthy.

Failover Traffic Destination

Failover is used when the original link is not available. It is needed both when using a specified interface or when using a balancing mechanism.

When selecting the Failover Traffic Destination, you can choose between Load Balancer, Fast Balancer or using a specific interface. Fast balancer uses netfilter and

load balancer uses .

Services

The **Services** view allows you to configure the services connected device.

Printer Server

The **Printer Server Settings** view allows you to change different features about your printer server for connected printers.

MiniDLNA

The **MiniDLNA** view lets you configure the server.

UPnP

The **UPNP** view allows you to configure services.

DDNS

The **DDNS** view allows you configure services for your device.

IPTV

The **IPTV** view lets you configure the server.

DHCP

The **DHCP** view lets you configure the server settings.

SNMP

The **SNMP Configuration** view lets you configure the service.

Samba

In the **Samba** view you can change settings for the server.

Printer Server

The **Printer Server Settings** view allows you to change different features about your printer server for connected printers.

| Item | Comment |
|--------------------|---|
| Enable | Turn printer server on or off. |
| Interface | Interface to listen on |
| Port | to listen on. |
| Bidirectional mode | Allow printer to communicate with client. |

MiniDLNA

The **MiniDLNA** view lets you configure the server.

Status

At the top of the page is a status window that can be expanded to display the current MiniDLNA status.

General

In the **General** settings tab you can change different general features about your MiniDLNA server.

Advanced

In the **Advanced** tab you can change different advanced features about your media server.

UPnP

The **UPNP** view allows you to configure services.

At the top of the page is a list of currently open UPnP ports, if any.

The UPnP settings are divided into tabs.

General

The **General** tab allows you to enable and configure the service parameters.

Advanced

The **Advanced** tab lets you configure advanced settings.

ACL

The **ACL** tab lets you configure the for access.

DDNS

The **DDNS** view allows you configure services for your device.

At the top of the page is a list of selectable services.

When a particular service is selected, details about it is shown in the connection section.

| Item | Description |
|--------------------------------------|--|
| Enabled | Turn service on or off. |
| Label | Identifier in the service list. |
| IP Retrieval Method | Interface / Network / Script / Web. |
| Select Interface | For Interface : Interface. |
| Select Connection | For Network : Connection. |
| Script Path | For Script : Local path to IP detection script. |
| Enter website to poll for ip address | For Web : Address to IP detection service. |
| Provider | Service provider list. |
| Enter DDNS Provider | Manually add service provider. |
| Domain name | Full hostname to use for the device. |
| Username | Service account username. |
| Password | Service account password. |
| Use HTTPS | Use secure communication with service. |

DDNS Services

You can add as many DDNS Services as you like.

To add a DDNS Service:

- Click the **add** button

A new service is added to the list.

- Edit the parameters as needed.
- Click **Apply**

IPTV

The **IPTV** view lets you configure the server.

| Item | Description |
|------------------------------------|---|
| Differentiated Services Code Point | to use for tagging outgoing packets. |
| Proxy interface | Interface to use as proxy. |
| Default version | version. |
| Query interval | Time between query messages. |
| Query response interval | Time to wait for response to query before timeout. |
| Last member query interval | Time between queries to determine the loss of the last member in a group. |
| Robustness value | Tolerance for lost packets. |
| LAN to LAN multicast | Allow multicast between LANs. |
| Max groups | Maximum allowed groups. |
| Max sources | Maximum allowed sources. |
| Max members | Maximum allowed members in a multicast group. |
| Fast leave | Leave multicast groups immediately after the last host. |
| Join immediate | Join group directly. |
| Enable IGMP proxy | Turn on handling. |
| Ignore SSM Range | Ignore and deliver regular . |
| IGMP snooping mode | mode: Disabled / Standard / Blocking. |
| IGMP snooping interfaces | Interfaces to use for . |

DHCP

The **DHCP** view lets you configure the server settings.

The DHCP settings are divided into tabs.

General

The **General** tab allows you to configure the basic settings.

Advanced

The **Advanced** tab allows you to configure advanced settings for the server.

Hostnames

The **Hostname** tab allows you to configure for IPv4 or IPv6 addresses in the LAN.

SNMP

The **SNMP Configuration** view lets you configure the service.

The SNMP settings are divided into tabs.

System

The **System** tab lets you configure general information about the SNMP service.

Agent

The **Agent** tab allows you to manage .

Com2Sec

The **Com2Sec** tab lets you configure access profiles for the SNMP service.

Group

The **Group** tab allows you to configure access groups for the SNMP service.

View

The **View** tab lets you configure views for the SNMP service.

Access

The **Access** tab allows you to configure access directives for the SNMP service.

Pass

The **Pass** tab lets you configure passthrough for the SNMP service.

Samba

In the **Samba** view you can change settings for the server.

The Samba settings are divided into sections.

General

The **General section of the** view allows you to change the general Samba settings, such as name, workgroup and interface.

Samba Users

The **Samba Users** section of the view allows you to change the user settings.

Samba Shares

The **Samba Shares** section lets you configure Samba shares and user access.

WiFi

The **WiFi view** shows you information about your wireless network.

General

In the **General WiFi** view you can view and edit the .

Band Steering

The **Band Steering** view allows you to enable and configure for the device.

WPS Settings

The **WPS Settings** view lets you change the default wireless security settings () to make your network more secure.

MAC Filter

In the **MAC Filter** view you can make your wireless network more secure. Just specify which devices are allowed to connect, or explicitly lock out devices.

General

In the **General WiFi** view you can view and edit the .

Radios

The **Wireless Radios** view allows you to configure wireless radios installed on your system.

Wireless

In the **Wireless** view you can view and edit the .

Radios

The **Wireless Radios** view allows you to configure wireless radios installed on your system.

| Item | Comment |
|----------------------------------|---|
| Wireless Radio List | List of selectable radios. |
| Radio On/off | Turn radio on or off. |
| WiFi Mode (SSID) | Choose . |
| Channel | Choose . |
| Bandwidth | Choose . |
| Beamforming | Turn on or off. |
| DFS Channels | Turn channels on or off. |
| RX Chain PowerSave Quiet Time | Turn on or off. |
| RX Chain PowerSave PPS | Turn on or off one of the receive chains to save power. |
| Max. Assoc Clients | Maximum number of clients allowed. |
| Scan Timer | Determine the for channel hopping. |
| Enable WMM Multimedia Extensions | Turn multimedia extensions on or off. |
| Disable WMM Ack | Turn on or off. |
| Enable WMM UAPSD Power Saving | Turn WMM power saving on or off. |

Wireless

In the **Wireless** view you can view and edit the .

| Item | Comment |
|-------------------|---|
| Enabled | Turn on or off. |
| WiFi Network Name | Edit name of network |
| Broadcast SSID | Toggle to make network visible or invisible |
| Encryption | Change to a different encryption method |

| | |
|---------------------|--------------------------------|
| Cipher | Choose form of |
| WiFi Key (Password) | Reset to default password |
| Show Key Text | Change format of wifi key text |

Add Wireless Interface

- Click **Add**

A dialog is shown

- Click **Select Wireless Radio**
- Choose wireless radio
- Add new
- Click **OK**

Band Steering

The **Band Steering** view allows you to enable and configure for the device.

| Item | Comment |
|-----------------|------------------------------------|
| Enable | Turn on or off. |
| Steering Policy | or . |
| Threshold | Bandwidth or RSSI threshold value. |

Enable Band Steering

To enable band steering:

- Click **Enable** toggle
- Choose steering policy
- Set threshold value to use for the selected policy.

WPS Settings

The **WPS Settings** view lets you change the default wireless security settings () to make your network more secure.

General WPS Settings

The **WPS Settings** section allows you to choose and configure different connection methods on an encrypted channel.

WPS-PBC: Push Button on Device

The WPS-PBC: Push Button on Device section lets you your devices.

WPS/REG: Device provides PIN

The section WPS-REG: Device provides PIN lets you generate a personal identification number through .

WPS-PIN: Another Device provides PIN

The section WPS-PIN: Another Device provides PIN allows you to enter a PIN provided by another device.

WPS-PIN: Another Device provides PIN

The section WPS-PIN: Another Device provides PIN allows you to enter a PIN provided by another device.

| Item | Comment |
|-------------------------|------------------|
| Enter your device PIN | Enter device PIN |
| Pair (within 2 minutes) | Pair button. |

WPS/REG: Device provides PIN

The section WPS-REG: Device provides PIN lets you generate a personal identification number through .

| Item | Comment |
|-------------------------|---------------------|
| WPS Using Generated PIN | Turn on or off. |
| Generated PIN | Generated PIN shown |
| Generate PIN | Generate button. |

Generating a PIN

To generate a PIN through WPS:

- Click the **Generate** button

General WPS Settings

The **WPS Settings** section allows you to choose and configure different connection methods on an encrypted channel.

| Item | Comment |
|------------------------|-------------------------------|
| WPS Function | Turn on or off for device. |
| Enable WPS on (5GHz) | Turn WPS on or off for radio. |
| Enable WPS on (2.4GHz) | Turn WPS on or off for radio. |

WPS-PBC: Push Button on Device

The WPS-PBC: Push Button on Device section lets you your devices.

| Item | Comment |
|--|-----------------|
| Enable WPS button on device | Turn on or off. |
| Pressing WiFi on/off button on your device for long time activates pairing | Turn on or off. |
| Pair (within 2 minutes) | Pair button. |

Pairing Your Device

To a device via WPS:

- Click the **Pair** button
- Press the corresponding button on the device you wish to connect

Your device will be open for pairing for two minutes.

MAC Filter

In the **MAC Filter** view you can make your wireless network more secure. Just specify which devices are allowed to connect, or explicitly lock out devices.

Filters can be applied separately for each .

The devices are identified by their address. You can manage up to 32 devices.

| Section | Description |
|---|---|
| MAC Filtering | Turn filtering on or off. |
| Access for listed devices | Access setting for clients in the list. |
| Currently added devices | List of filtered devices. |
| Add currently connected hosts of the list | Collect all currently active devices to the list. |

Enable MAC Filter

To enable MAC Filtering:

- Click the **MAC Filtering** toggle button
- Choose type of **Access for listed devices**
 - Allow - Access
 - Deny - No access
- Click the **add** button next to **Currently added devices**
- Enter the MAC address for the device
- Click **Save**
- Click **Apply**

System

The **System** view provides access to device information, management, provisioning and settings.

General Settings

The **General Settings** view contains basic device settings.

| Item | Description |
|------------|----------------------------|
| Local Time | Local time for the device. |
| Timezone | Device timezone setting. |
| Hostname | Device . |

Menu Access

The **Menu Access** view allows you to switch access to menus and menu items in the web interface on or off.

Passwords

The **Passwords** view lets you change passwords for device users.

Firmware Upgrade

The **Firmware Upgrade** view lets you upgrade the device firmware by using image files.

Backup/Restore

The **Backup/Restore** view allows you to manage backups and resets of the device.

IUP

The **IUP** view allows you to set up parameters for provisioning services and configurations with .

TR69

The **TR69 Settings** view allows you to configure support for device management and provisioning from the WAN.

Management

The **Management** view lets you configure WAN to connections and access to services.

Hardware

Power Management

The **Power Management** view allows you to manage CPU efficiency and Ethernet hardware ports.

Services

The **Services** view lets you manage system services on the device.

Restart

The **Restart** page allows to restart your Internet connection and reboot your device.

General Settings

The **General Settings** view contains basic device settings.

| Item | Description |
|------------|----------------------------|
| Local Time | Local time for the device. |
| Timezone | Device timezone setting. |
| Hostname | Device . |

Time Servers

The Time Servers section shows time servers in use.

| Item | Description |
|--------------------|-------------------------|
| Time Servers (NTP) | List of servers to use. |
| Server Mode | Turn on or off. |

Add Server

To add a time server:

- Click the  **add** button
- Enter the server address in **URL** box
- Click **Apply**

Log Settings

The **Log Settings** view contains settings for the system logs.

Current Firmware

| Item | Description |
|------------------|--|
| System Log Level | System |
| Cron Log Level | Cron |
| Kernel Log Level | Kernel |
| Log File | Location to save the log file. |
| Log IP | IP address of remote log server. |
| Log Port | Port for the remote log server. |
| Log Prefix | Prefix to use in log. |
| Log Protocol | Protocol for transfer of log information (/). |
| Log Remote | Turn remote logging on or off. |
| Log Size | Max size of log in Kb. |
| Trailing null | Use trailing null insted of newline when using TCP |
| Log Type | Type of logging to use (circular = limited /file = unlimited number of files). |

Connectivity Test

The **Connectivity Test** view allows for automatic verification of the Internet connection by accessing a predefined URL.

Current Firmware

| Item | Description |
|----------|---------------------------------------|
| Internet | URL for checking Internet connection. |

Menu Access

The **Menu Access** view allows you to switch access to menus and menu items in the web interface on or off.

Note: The admin account cannot have restrictions on menu access.

At the top of the page is a list of user roles.

When a particular role is selected for editing, all menu and menu items are shown in the list.

You can change the access status of any item by moving the associated slider.

Passwords

The **Passwords** view lets you change passwords for device users.

Change Password Dialog

| Item | Description |
|-------------------|---|
| Current Password | The existing password. |
| New Password | Password to change to. |
| Reenter Password | Verification of new password. |
| Password Strength | Indicates the security level of the new password. |

Note: For security reasons, the current password is never displayed.

Change password

To change password for a user:

- Open the **Change password for user**
- Select a user role
- Click **Change Password**

The change password dialog opens.

- Enter the current password
- Enter the new password
- Enter the new password again
- Click **Change Password**

Firmware Upgrade

The **Firmware Upgrade** view lets you upgrade the device firmware by using image files.

Current Firmware

The **Current Firmware Version** shows currently installed firmware on the device.

USB Firmware Upgrade

In the **USB Firmware Upgrade** section you can perform an automatic search for upgrade image file on USB devices, and perform the upgrade.

The **check for upgrade** starts a search for image files on any connected USB devices.

Note: The type of image file to use for upgrades is defined in .

Manual Firmware Upgrade

In the **manual firmware upgrade** section you can select an image file on your computer, upload it to the device, and perform the upgrade.

| Item | Description |
|--------------------------------|---------------------------------------|
| Select firmware file to upload | Upgrade image file on local computer. |
| Start upgrade | Button to start upgrade. |

Upgrade Options

The **Upgrade Options** view lets you configure parameters for firmware upgrades.

Firmware image extensions

The firmware image extension setting defines which type of image file to use for upgrades.

| Item | Description |
|----------|---------------------|
| .y | UBIFS Image |
| .w | JFFS Image with CFE |
| .y | UBIFS Image |
| .y2 | new UBIFS Image |
| fs_image | JFFS Image |

Online Upgrade

The online upgrade settings define where the online upgrade images are located.

| Item | Description |
|---|--|
| URL for file with latest image filename | URL to a text file containing the latest image filename on the server. |
| Upgrade URL base path | URL to directory containing upgrade image files. |

Backup/Restore

The **Backup/Restore** view allows you to manage backups and resets of the device.

Backup Settings

In the **Backup Settings** section you can save a copy of your device configuration or load a saved configuration into the device.

Save Backup

- Click **Save**

The **Save Configuration** dialog opens.

- If you want to encrypt the backup file:
 - Enter a **Backup file password**
 - Retype the password
- Click **Continue**

The file is saved as a compressed file archive to your local computer.

Load Backup

To load a saved configuration the factory reset:

- Click **Load**
- Click **Continue**

The **Load New Configuration** dialog opens.

- Click **Choose File**
- If the backup file is encrypted:
 - Enter a **Backup file password**

Factory Settings

In the **Factory Settings** you can

Note: Reset restores your device to the factory defaults and remove any configurations you have made.

To perform the factory reset:

- Click **Reset**

Backup Settings

The **Backup Settings** view lets you select which services and settings to include in backups.

The list contains a selection of services and settings that can be included when performing backups.

You can change the status of any item by moving the associated slider.

IUP

The **IUP** view allows you to set up parameters for provisioning services and configurations with .

The IUP view is divided into several sections.

General

In the **General** section you can manage general provisioning settings.

| Item | Description |
|----------------------------|------------------------------|
| Enabled | Turn provisioning on or off. |
| Update interval start time | Time of day to start update. |

| | |
|-----------------|-----------------------------|
| Update interval | Hourly / Daily / Weekly. |
| Export file | Download provisioning file. |

Main Provisioning Server

In the **Main Provisioning Server** section you can add a manual provisioning server address.

Note: This will override DHCP Discover Provisioning, even if it is enabled.

| Item | Description |
|----------------|--|
| Enabled | Turn main provisioning server on or off. |
| Reboot | Reboot after configuration has been applied. |
| URL | Address to the provisioning server. |
| Decryption Key | Key for encrypted provisioning archive. |

DHCP Discover Provisioning Server

In the **DHCP Discover Provisioning Server** section you can enable automatic discovery of provisioning server.

| Item | Description |
|---------|---------------------------------|
| Enabled | Turn software update on or off. |

Software Update Config

In the **Software Update Config** section you can configure online update of software.

| Item | Description |
|---------|---------------------------------|
| Enabled | Turn software update on or off. |

| Item | Description |
|---------------|--|
| Enabled | Turn software update on or off. |
| Default reset | Remove device configurations and set to default. |
| Software URL | Location of software configuration. |

Sub Configs

In the **sub configs** section you can add sub configurations of specific parts.

| Item | Description |
|-----------------|------------------------------------|
| URL | Location of configuration file. |
| Package Control | |
| Enabled | Turn sub configurations on or off. |

Add Sub Config

To add a sub configuration:

- Click **Add sub config**
- Enter the **URL** for the configuration file
- Enter the relevant **Package Control**
- Select if the su config should be **Enabled**

TR69

The **TR69 Settings** view allows you to configure support for device management and provisioning from the WAN.

The TR69 view is divided into sections.

Configure ACS Specific Settings

In the **ACS** section, you can configure settings.

| Item | Description |
|------------------------|---|
| ACS User Name | USer name for the connection. |
| ACS Password | Password for the connection. |
| URL | Location of the ACS server. |
| Periodic Inform Enable | Turn on or off. |
| Periodic Inform Time | Absolute UTC time when will send calls. |
| DHCP Discovery | Turn automatic discovery of server on or off. |

Configure CPE Specific Settings

In the **CPE** section, you can configure connection settings.

| Item | Description |
|------------------------------|--|
| WAN Interface | Interface for the connection. |
| Connection Request User Name | User name for the connection |
| Connection Request Password | Password for the connection. |
| Port | Specific connection . |
| Log Severity Level | . |
| Log to console | Display logging messages in the console. |
| Log to file | Turn logging to file on or off. |

| | |
|-------------------|------------------------------|
| Log file max size | Size of log file. |
| Provisioning Code | Identifier for provisioning. |

Management

The **Management** view lets you configure WAN to connections and access to services.

SSH

The **SSH** view allows you to configure access, server instances, and keys.

Services

The **Services** view lets you configure WAN access to device services.

OWSD

The **OWSD** view lets you configure settings for the .

The server listens on a number of interfaces, and allows for separate configuration of access for each of them.

At the top of the page is a list of interfaces the server listens on.

When a particular interface is selected, details about it is shown in the configuration section.

Configuration

The **Configure firewall rule** section allows you to enable and configure a firewall rule for the selected service.

| Item | Description |
|-------------------------|---------------------------------------|
| Interface | Listening . |
| Port | to listen on. |
| IPv6 | / address. |
| IPv6 only | Limit to |
| List of allowed origins | Filter for origin (* for allow all). |

Add Listen Interface

- Click **Add**

- Enter a **Name**

The firewall settings are displayed.

- Add interface settings as needed.
- Click **Apply**

Add Origin

Select an interface in the list.

- Click **Add**
- Enter the **Origin**
- Click **Add**
- Click **Apply**

SSH

The **SSH** view allows you to configure access, server instances, and keys.

General Settings

The **General Settings** section contains management options for the SSH service.

| Item | Description |
|-----------------|---------------------------------|
| Enabled | Turn SSH on or off. |
| Verbose Logging | Turn verbose logging on or off. |

Dropbear Instances

The **Dropbear Instances** section lets you create SSH server instances with different parameters.

| Item | Description |
|---------------------------|--|
| Password Autentication | Turn access with password authentication on or off. |
| Port | Connection . |
| Enable Root Password Auth | Turn root access with password authentication on or off. |
| Enable Root Login | Turn root account access on or off. |
| Enable Forwarded Ports | Turn forwarded on or off. |
| Interface | Restrict SSH server to particular interface. |

Add SSH Server instance:

To add a SSH Server instance:

- Click **Add**
- Enter parameters for the instance
- Click **Apply**

Accepted SSH Keys

The **SSH** view allows you to configure access, server instances, and keys.

To add a SSH key:

- Click **Add**
- Copy the public SSH key
- Paste the public SSH key into the window
- Click **OK**
- Click **Apply**

Services

The **Services** view lets you configure WAN access to device services.

Allow WAN Access To Running Services

At the top of the page is a list of services.

When a particular service is selected, details about it is shown in the configuration section.

Configure firewall rule for this service

The **Configure firewall rule** section allows you to enable and configure a firewall rule for the selected service.

Where applicable, the configuration is divided into separate sections for **source** and **destination** zones.

| Item | Description |
|--|--|
| Enable WAN forwarding for this service | Turn WAN access on or off. |
| Name | Identifier for the rule. |
| Zone | Device / Any / LAN / WAN |
| IP | / address. |
| MAC | address. |
| Port | affected. |
| IP version | Any / / |
| Protocol | Protocol affected: (/ / / TCP + UDP /) |
| Firewall action | to perform. |

Add Firewall Rule

Select a service in the list.

- Click the **Enable WAN forwarding for this service** button

The firewall settings are displayed.

- Add rule settings as needed.
- Click **Apply**

Hardware

Configure Buttons

The **Configure Buttons** view allows you to enable or disable the buttons on your device.

The exact buttons available vary with device type.

LEDs

The **LED view** allows you to enable or disable the status LEDs on your device.

Configure Buttons

The **Configure Buttons** view allows you to enable or disable the buttons on your device.

The exact buttons available vary with device type.

Examples

Reset

Status

Wireless

WPS

DECT

EXT

Toggle Button

To switch a button on or off:

- Find the desired button in the list
- Click the slider button in the interface
- Click **Apply**

LEDs

The **LED view** allows you to enable or disable the status LEDs on your device.

Displayed Leds

The exact LEDs available vary with device type. The status of each LED is shown on the left of the name.

Examples

BROADBAND

DECT

DSL

EXT

INTERNET

LOGO

STATUS

VOICE1

WAN

WIFI

WPS

Toggle LED

To switch a LED on or off:

- Find the desired LED in the list
- Click the slider button in the interface
- Click **Apply**

Power Management

The **Power Management** view allows you to manage CPU efficiency and Ethernet hardware ports.

| Item | Description |
|---------------------------|---------------------------|
| CPU Speed | CPU Sync. |
| CPU r4k Wait | Sleep mode configuration. |
| Ethernet Auto Power Down | Turn on or off. |
| Energy Efficient Ethernet | Turn on or off. |

Services

The **Services** view lets you manage system services on the device.

The list contains system running and available services.

| Item | Description |
|----------|---|
| Priority | System priority. |
| Service | Service identifier. |
| Enable | Enable or disable service. |
| Action | Buttons to start, stop and restart the service. |

Restart

The **Restart** page allows to restart your Internet connection and reboot your device.

Restart device

Note: Restarting the device will disconnect all phone, Internet and TV services while the device is restarting.

To restart your device:

- Click **Restart**

A confirmation dialog is shown

- Click **Yes**

A restart dialog is shown.

When the device has restarted, the browser reconnects and the [login](#) dialog is shown.

Status

The Status area provides an overview of the current situation for your device, network and services, and also contains diagnostic tools.

System

The **System Status** view displays information about a number of parameters regarding your gateway and its operation.

IGPM TV Status

The **IGPM TV Status** views shows information about your IPTV services and their connection status.

WiFi Status

The **WiFi Status** view shows information about the wireless network, and allows you to scan the local area for other wireless access points.

DSL Status

The **DSL status** view shows information about any connections to the device.

USB Status

The **USB devices** views displays information about any devices connected to the gateway device.

Network Status

The **Network Status** view shows information about various aspects of your network.

Diagnostics

The **Diagnostic Utility** allows you to perform diagnostic tests from the web interface.

Voice Status

The **Voice Status** view shows information about SIP accounts, phone numbers and voice lines connected to the device.

System

The **System Status** view displays information about a number of parameters regarding your gateway and its operation.

System Status

The **System Status** overview shows basic data about the device.

Processes

The **Processes** view shows information about system processes and CPU usage.

System Status

The **System Status** overview shows basic data about the device.

Configuration

| Option | Description | Sample value | |
|--------------------|---|--|--|
| Hostname | The for the gateway. | Inteno | |
| Model | Gateway model. | DG400A | |
| Firmware Version | Version of installed firmware. | DG400-WU7U/NT3.5.5-1605131617 | |
| Kernel Version | The gateway operating system kernel version. | 3.4.11-rt19 | |
| Filesystem | Filesystem used in gateway storage. | | |
| BRCM Version | Version number for the Broadcom driver. | 4.16L.04 | |
| Local Time | Time according to the gateway internal clock. | Mon May 23 2016 17:21:12 GMT+0200 (CEST) | |
| Uptime | Time the gateway has been running since last startup. | 5d 2h 53m 14s | |
| CPU | Percentage of CPU processing in use. | 0% | |
| Active Connections | Number and percentage of connections to the gateway. | 259 / 7660 (3%) | |

Processes

The **Processes** view shows information about system processes and CPU usage.

Overview

The overview shows a summary of the processes:

| Item | Description | Comment |
|---------------------------|-------------|---------|
| Total number of processes | | 96 |
| Total CPU usage | | 9% |

Process Detail Toggle

You can access detailed realtime information about running processes, by clicking the information toggle.

To open the **Details** view:

- Click [Click here to view details](#)

Network Status

The **Network Status** view shows information about various aspects of your network.

Status

The **Network Status** view provides an overview of network elements for your device.

Clients

The **Connected Clients** view shows a list of clients connected to the network.

Routing

The **Routing Status** view shows the static routes configuration for the various network types.

UPnP

The **UPnP Open Ports** view shows the status of any ports currently in use.

DHCP

The **Active DHCP Leases** view shows the status of any currently in use.

NAT

The **NAT** view shows a list of active mappings in the device network.

Status

The **Network Status** view provides an overview of network elements for your device.

WAN6

The **WAN6** view shows information about any connected network.

LAN

The **LAN** view shows information about the local network connected network.

| Option | Description | Comment |
|------------|-------------------------------------|------------------------------|
| IP Address | of the device on the local network. | Typically 192 . 168 . 1 . 1. |

WAN

The **WAN** view shows information about any connected network.

| Option | Description | |
|---------------|---------------------------------|--|
| IP Address | for the device on the Internet. | |
| Gateway | IP address to the internet . | |
| Primary DNS | First priority . | |
| Secondary DNS | Second priority . | |

Clients

The **Connected Clients** view shows a list of clients connected to the network.

Table

| Column | Description | Comment |
|--------------------|-------------------------------|---------|
| Hostname | Client . | |
| MAC Address | Client . | |
| IPv4 Address | Client . | |
| IPv6 Address | Client . | |
| Active Connections | Number of active connections. | |

Routing

The **Routing Status** view shows the static routes configuration for the various network types.

ARP

The **ARP status** view shows information about routes.

IPv4

The **IPv4 status** view shows information about routes.

IPv6

The **IPv6 status** view shows information about routes.

IPv6 Neighbors

The **IPv6 Neighbors** view shows information about devices in the network neighborhood.

UPnP

The **UPnP Open Ports** view shows the status of any ports currently in use.

DHCP

The **Active DHCP Leases** view shows the status of any currently in use.

DHCPv4 Leases

| Column | Description |
|---------------------|-------------------------------|
| Hostname | Client . |
| IPv4 Address | Client . |
| MAC Address | Client . |
| Leasetime remaining | Time until the lease expires. |

DHCPv6 Leases

| Column | Description |
|--------------|-------------|
| Hostname | Client . |
| IPv6 Address | Client . |
| DUID | Client . |

| | |
|---------------------|-------------------------------|
| Leasetime remaining | Time until the lease expires. |
|---------------------|-------------------------------|

NAT

The **NAT** view shows a list of active mappings in the device network.

Connections

The **Active Connections** gauge shows how many NAT mappings are in use out of the allowed total, as a percentage and as a count.

NAT Connection Table

Connections to and from the local network to the external network are added to the table, allowing the device to handle traffic routing decisions.

The table displays information about active NAT connections.

| Column | Description | Comment |
|------------------|------------------------------|---------|
| Protocol | Communication protocol used. | |
| Source | Internal . | |
| Destination. | External . | |
| Source Port | Internal . | |
| Destination Port | External . | |

WiFi Status

The **WiFi Status** view shows information about the wireless network, and allows you to scan the local area for other wireless access points.

WiFi Status

The **general WiFi Status** view displays information about your wireless channels and network interfaces.

WiFi Scan

The **WiFi scan** view allows you to scan the area around the device to find out what other access points are visible.

WiFi Status

The **general WiFi Status** view displays information about your wireless channels and

network interfaces.

Configuration

For each information is displayed about:

- in use.
- in dB for the channel.
- name.
- used by the interface.

Client

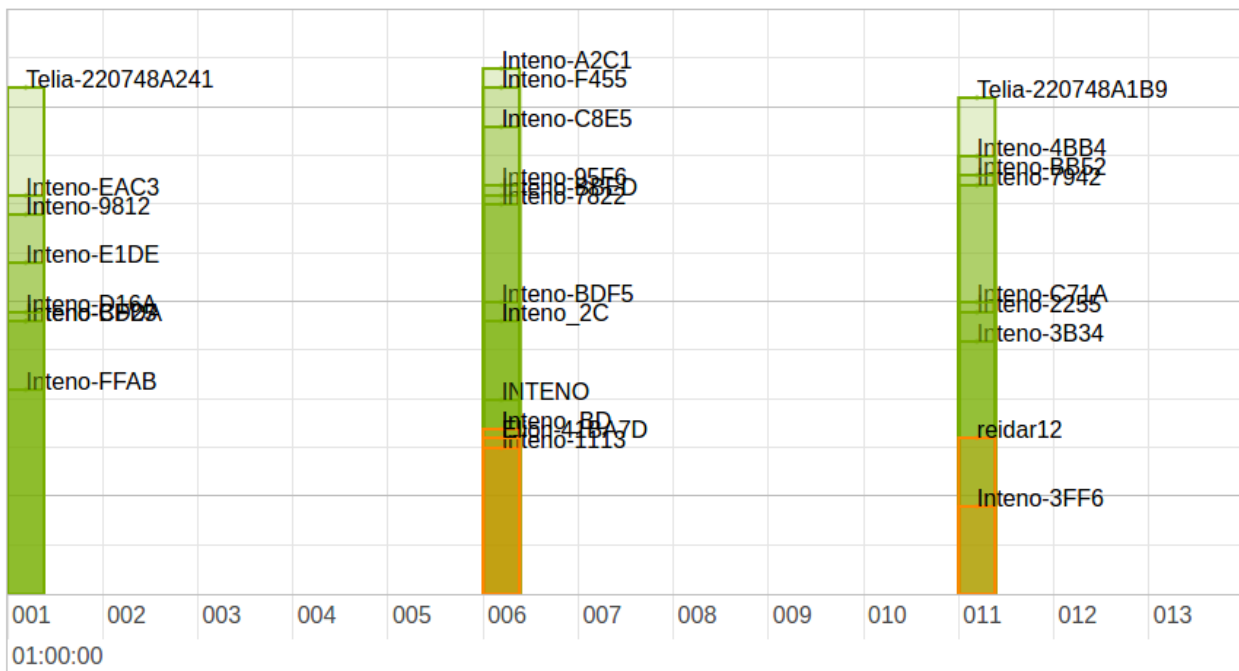
For each connected client, more information about the connected client is available.

WiFi Scan

The **WiFi scan** view allows you to scan the area around the device to find out what other access points are visible.

Chart

The scan results table displays all detected access points and information about each in a graphical manner.



raph

Axes

The horizontal axis shows the discovered .

The vertical axis shows the signal strength, according to .

| Color | Description | Comment |
|--------|-------------|---------|
| Red | Poor. | |
| Yellow | Acceptable. | |
| Green | Good. | |

Table

The scan results table displays all detected access points and information about each:

| Column | Description | Comment |
|-----------|--|---------|
| SSID | identifying the . | |
| Frequency | for the access point. | |
| Channel | used by the access point. | |
| RSSI | strength for the signal. | |
| Noise | for the connection to the access point. | |
| Cipher | used for encryption in the access point. | |
| WPS | version used by the access point. | |

Scan WiFi

To scan a frequency band:

- Select **Frequency to Scan**
- Click **Scan**

The results for the selected band are displayed in the graph and table.

Band Steering

The **Band Steering** view shows information about .

Status

The **status** section shows the current band steering status.

The information is displayed in the STA info summary table.

| Column | Description |
|--|--------------------|
| STAMAC <i>Station (client) address.</i> <i>Interface</i> | Transmission rate. |

| | |
|--|--|
| <i>Client name. TimeStamp Timestamp for the steering event. Txrate</i> | |
| RSSI | . |
| Bounce | Does the client bounce back to a particular band after steering? (yes/no). |
| Picky | Does the client prefer a particular band? (yes/no). |
| PSTA | Is the client a station? (yes/no). |
| DUALBAND | Is the client dual-band capable? (yes/no). |

Log

The **log** section contains the log file, which shows the band steering events.

The information is displayed in the Band Steering Record table.

| Column | Description |
|--|-----------------------------------|
| Seq | |
| TimeStamp | Timestamp for the steering event. |
| <i>STAMAC Station (client) address. Fmch</i> | From channel (hex code). |
| To_ch | To channel (hex code). |
| Reason | Event (hex code). |
| Description | Description of event. |

DSL Status

The **DSL status** view shows information about any connections to the device.

DSL Status Information

The DSL Status Information section shows the status for the DSL line.

Line Status

| Status | Description |
|-----------------|---|
| Idle | No connection. |
| Handshake | Searching for connection, negotiating transfer. |
| Training | Connection found, testing cable. |
| Showtime/Active | Connection established. |

DSL Mode

The DSL Mode section shows the .

Bit Rate

The Bit Rate section shows transmission rates for streams in bits per second (bps).

Actual Data Rate

| Column | Description |
|------------|------------------------|
| Downstream | Rate to the device. |
| Upstream | Reate from the device. |

Operating Data

The Operating Data section shows signal strength for the DSL line.

SNR margin

The SNR Margin section displays the for the streams.

| Column | Description |
|------------|------------------|
| Downstream | To the device. |
| Upstream | From the device. |

Loop Attenuation

The Loop Attenuation section shows for the streams.

| Column | Description |
|------------|------------------|
| Downstream | To the device. |
| Upstream | From the device. |

Error Counter

The Error Counter section lists the number of (discovered) errors for the connection.

FEC Corrections

The FEC Corrections table shows for the streams.

| Column | Description |
|------------|------------------|
| Downstream | To the device. |
| Upstream | From the device. |

CRC Corrections

The CRC Corrections table shows for the streams.

| Column | Description |
|------------|------------------|
| Downstream | To the device. |
| Upstream | From the device. |

Cell Statistics

The Cell Statistics section shows the number of transmitted for the streams.

| Column | Description |
|-------------|------------------|
| Received | To the device. |
| Transmitted | From the device. |

IGMP TV Status

The **IGMP TV Status** view shows information about your IPTV services and their connection status.

Configuration

The table shows any connected IGMP TV channels and information about each:

| Column | Description |
|-----------|--|
| Group IP | IP address of the group. |
| Client IP | IP address of the client. |
| LAN Port | used for the group. |
| WAN Port | used for the group. |
| Timeout | Time until the gateway triggers IGMP query reelection. |

USB Status

The **USB devices** view displays information about any devices connected to the gateway device.

Table

The **USB device information** table shows information about the USB devices.

| Column | Description | Comment |
|-------------|--------------------------------------|---------|
| Device ID | Identification for the USB device. | |
| Vendor ID | Identification for the manufacturer. | |
| Vendor Name | Name of the manufacturer. | |
| Device Name | Name reported by the USB device. | |

CATV

The **CATV Status** view shows information about services connected to the device.

Note: Available on EG300 & EG400 only.

| Option | Description | Example |
|--------------|-------------|----------|
| Inteno model | Model. | CATV-302 |

| | | |
|-----------|---------------------------------------|-----------|
| VPD | Reverse voltage on Protection Device. | -inf dBm |
| RF | Range. | 75.7 dBμV |
| RF enable | Enable RF. | OFF |

SFP

The **SFP Status** view shows information about connectors enabled in the device.

Configuration

Information is shown in two tables; information and information.

Note: Available on EG300 & EG400 only.

DDM

The DDM table shows information about the retrieved from the SFP.

| Option | Description | Example |
|-------------|------------------------|---------------|
| voltage | Port voltage. | 3.1872 (V) |
| current | Port current. | 26.448 (mA) |
| tx-pwr | Broadcasting power. | 0.3530 (mW) |
| tx-pwr-dBm | Broadcasting power. | -4.5223 (dBm) |
| rx-pwr | Received signal power. | 0.3026 (mW) |
| rx-pwr-dBm | Received signal power. | -5.1913 (dBm) |
| rx-pwr-type | Recieved power type. | average |

ROM

The ROM table shows information about the .

| Option | Description | Example |
|-------------|------------------------------|-----------------|
| connector | Connector type. | SC |
| ethernet | Ethernet type. | LX |
| encoding | Encoding type. | 8B10B |
| rate | Line rate. | 1300 |
| single-mode | Single mode distance. | 20000 |
| vendor | Port manufacturer or vendor. | Skylane Optics |
| oui | . | 00:25:cd |
| pn | Product name. | SBU35020DR3D000 |
| rev | ROM Revision. | A |
| sn | Serial Number | b19bmj rx1857 |
| date | ROM date. | 2016-04-21 |
| ddm | version | 9.3 |

Diagnostics

The **Diagnostic Utility** allows you to perform diagnostic tests from the web interface.

Ping

The **Ping Test** view allows you to perform a for a selected host.

Trace

The **Tracing tool** view allows you to perform a for a selected host.

Speed Test

The **Speed Test** view allows you to perform a for your network, using your device as the endpoint.

Ping

The **Ping Test** view allows you to perform a for a selected host.

Ping Test

To perform a ping test against an endpoint:

- Enter a valid or in the **Host to ping** box
- Click **Ping**

The result of the ping is shown below the utility.

Example:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=64 time=0.208 ms
64 bytes from 127.0.0.1: seq=1 ttl=64 time=0.130 ms
64 bytes from 127.0.0.1: seq=2 ttl=64 time=0.129 ms
64 bytes from 127.0.0.1: seq=3 ttl=64 time=0.146 ms
64 bytes from 127.0.0.1: seq=4 ttl=64 time=0.130 ms

--- 127.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.129/0.148/0.208 ms
```

Trace

The **Tracing tool** view allows you to perform a for a selected host.

Traceroute Test

To perform a ping test against an endpoint:

- Enter a valid or in the **Host to trace** box
- Click **Trace**

The result of the trace is shown below the utility.

Example:

Trace results:

```
traceroute to 127.0.0.1 (127.0.0.1), 30 hops max, 38 byte packets
 1  127.0.0.1  0.033 ms
```

Speed Test

The **Speed Test** view allows you to perform a for your network, using your device as the endpoint.

Configuration

| Option | Description | Comment |
|------------------|-----------------------------|--|
| Direction | Traffic direction to test. | Up and Down, Up, Down. |
| Package Size | Size of test to send. | Size of test packages to send. |
| Speedtest Server | Server to use for the test. | A number of default servers are provided, but you can edit the list. |

Perform Speed Test

Example

Test results:

```
Downstream: 103.45 Mbit/s
Upstream: 44.10 Mbit/s
```

Add test server

If you have additional test servers you want to use, you can add them to the dropdown list.

To add a test server:

- Click the + plus sign

A dialog is shown allowing you to enter parameters:

| Option | Description | Comment |
|----------|-------------|---------|
| Hostname | Test Server | |
| Port | Test server | |

- Add a valid Server **Hostname**
- Add a valid server **Port**
- Click **OK**

Remove test server

Servers in the test server list can be removed.

To remove a test server:

- Select the server in the **Speedtest Server** list
- Click the - minus sign

The server is removed from the list immediately.

Voice Status

The **Voice Status** view shows information about SIP accounts, phone numbers and voice lines connected to the device.

Configuration

Information is shown in two tables.

Your phone numbers

| Option | Description | Comment |
|-----------------------|-----------------------------|--|
| Name | name. | Uses type and number unless otherwise set. |
| User | . | |
| Domain | . | |
| Registration interval | domain. | |
| Last registration | Last registration time. | |
| Status | Current status of the line. | |

Voice lines

The Voice lines shows a list of connected voice lines.

| Option | Description | |
|--------|----------------------------|--|
| Name | Voice line name. | Uses type and number unless otherwise set. |
| State | Current state of the line. | |

Event Log

The **Event Log** view lets you view and manage the event log for the device.

Log

The **Log** section contains log settings and lets you download the logs.

| Item | Description |
|-------------------------------|--|
| Download All Logs | Save the logs to the local computer. |
| Limit Log List | Limit the number of events. |
| Filter Log Messages By Source | Filter out events by freetext search in source. |
| Filter By Type | Filter out event types by . |
| Filter By | Filter out events in the log (firewall / network / system / iptv). |

ACS

An Auto Configuration Servers (ACS) is a server used for automatic device and user provisioning and configuration through .

ARP

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

ATM - Asynchronous Data Transfer Mode

ATM - Asynchronous Data Transfer Mode is a protocol for high-throughput data traffic and streaming.

Assured Forwarding

Assured Forwarding (AF) is a mechanism for assurance of delivery, given a defined rate.

The four AF classes have the same priority. For each class, packets are given a drop *precedence*.

In case of congestion, traffic that exceeds the rate have a higher probability of being dropped.

Packets with a lower drop precedence are dropped before packets with a higher drop precedence.

| Drop Precedence | Class 1 | Class 2 | Class 3 | Class 4 |
|-----------------|---------|---------|---------|---------|
| Low | AF11 | AF21 | AF31 | AF41 |
| Medium | AF12 | AF22 | AF32 | AF42 |
| High | AF13 | AF23 | AF33 | AF43 |

Auto-Negotiation

Auto-negotiation is a method in Ethernet where two devices agree on the best performance transmission mode they both support.

Access Control List

An Access Control List (ACL) is an table containing permissions for a particular service or device, defining access to objects and allowed operations.

APN

An Access Point Name (APN) is the name of a gateway between a mobile network providing access to Internet.

Ad SPECification

An ADvertisement SPECification (ADSPEC) is a part of an PATH message which contains information from network devices between a sender and receiver.

Typically the message allows *advertise* supported services, availability and transmission information.

AMPDU

An Aggregated MAC Protocol Data Unit - AMPDU - is an of .

Asterisk

Asterisk is a software that handles calls betwen telephones and connections to and services.

AMSDU

An Aggregated MAC Service Data Unit is an of .

ADPCM

Adaptive Differential Pulse-Code Modulation (ADPCM) is a variant where the size of ranges is modified with a scaling factor before encoding. This means that the bandwidth requirements are reduced.

ADSL

Asymmetric digital subscriber line (ADSL) is a technology providing network traffic over copper wires.

ADSL is slower than , with up to 24 Mbit/s downstream and 3.3 Mbit/s upstream speeds.

Access point

An access point is a device or interface that connects users to other users within the network. It can also serve as the point of interconnection between the and a fixed wire network.

The number of required access points depends on the number of network users and the area the network covers.

ABR

The Available Bit Rate (ABR) is used primarily for traffic that is not time sensitive and don't need service level guarantees.

AFTR

An Address Family Transition Router (AFTR) is a server implementing the to provide IPv4 to IPv4 communication over IPv6.

Band Steering

Band steering allows the device to determine if a connected client is dual-band capable. If so, the client can be forced to use the less congested 5GHz network.

This is done by blocking the client from connecting to the 2.4GHz network.

Bit Error Rate

The Bit Error Rate (BER) is the percentage of transmitted bits which contain errors.

Bitswap

Bitswap is a method for adjusting the number of bits allocated to channels. Congested

channels are assigned fewer bits, and available channels are allocated more bits.

Beamforming

Beamforming is technique used for radio signals to improve quality and performance. It is done by creating multiple signals and finding the best paths, thereby “shaping” the antenna output to provide minimum interference.

Back-Off

Back-Off is a method for decreasing the frequency of retransmissions of request in order to avoid congestion and collision.

Bandwidth

The bandwidth is is a measure of network capacity. It indicates the capacity.

Bit Rate

The bit rate is a measure of traffic speed in a network. It indicates the number of bits per second transmitted.

BSS

The basic service set (BSS) is the basic building block in a wireless LAN. It is a set of all stations that can communicate with each other. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

Comanding

A compressing-expanding (comanding) is a method for managing dynamic range in channels with limited dynamic range. It compresses the dynamic range of a signal transmission and expands it at the receiving end, according to the defined.

CRC

Cyclic Redundancy Check (CRC) is a method for discovering errors in data transmission by verifying the received data against an attached check value.

CA

A Certificate Authority (CA) is an entity that issues *digital certificates* which guarantee that a public key is owned by the certificate subject, verifying their identity.

Certificates typically include the owner's public key, the expiration date of the certificate,

the owner's name and other information about the public key owner.

CPE

The term Customer-Premises Equipment (CPE) is used in and refers to devices in a network that is located in the premises of a subscriber.

Cell (DSL)

DSL cells are data encoded into small, fixed-sized packets (frames).

Congestion

Network congestion is when the traffic volume in the network becomes so large it affects the transmission and delivery of data, thereby causing a reduced quality of service.

CLR

Cell Loss Ratio (CLR) is the percentage of network that do not arrive at their destination.

Connection Bytes

Connection Bytes is a filtering property that delays matching until after the specified number of bytes has been transferred through the connection.

The Connection Bytes is configured with a **From** value and an (optional) **To** value. Packets sent while the connection has transmitted more than from and less than To will be matched.

Classful QDisc / Packet Scheduler

A Classful QDisc is a function containing . The classes may contain other QDiscs, which in turn can be classful or classless.

Class Selector

The Class Selector (CS) is used by maps to indicate .

It is backwards compatible with values (CS0 = IP precedence 0, CS1 = IP precedence 1, and so on) .

| DSCP | Binary | Typical Application | Examples | |
|---------------|---------|---------------------|-----------|--|
| CS0 (Default) | 000 000 | 0x00 | | |
| CS1 | 001 000 | 8 | Scavenger | |
| CS2 | 010 000 | 16 | OAM | |

| | | | | |
|-----|---------|----|-----------------|--|
| CS3 | 011 000 | 24 | Signaling | |
| CS4 | 100 000 | 32 | Realtime | |
| CS5 | 101 000 | 40 | Broadcast video | |
| CS6 | 110 000 | 48 | Network control | |
| CS7 | 111 000 | 56 | | |

%CPU

The CPU percentage for a process indicates how much of CPU processing power is being used.

Checksum

A checksum is a value used as an error control mechanism. It works by calculating a sum for the data using a predefined algorithm, and then comparing the result to some expected value, or the checksum itself. If the result is not as expected, this indicates that something has gone wrong in transmission.

CCMP

CCMP – CTR mode with CBC-MAC Protocol is based on the Advanced Encryption Standard (AES) cipher along with strong message authenticity and integrity checking.

CDMA

Code division multiple access (CDMA) is a radio communication standard, where several transmitters can send information simultaneously over a single channel.

CATV

Community Antenna TeleVision (CATV), or “cable TV”, is a system of delivering television programming radio frequency (RF) signals transmitted through coaxial cables or fiber-optic cables.

CBR

The Constant Bit Rate (CBR) is used for applications that transport traffic at a constant bit rate, where time synchronisation between source and destination is important, providing predictable response times and a static amount of bandwidth.

Cipher

A WiFi security cipher is the method through which a connection is secured against intrusion.

For information about cipher strings, see <https://www.openssl.org/docs/manmaster/apps/ciphers.html>.

Codec

A coder-decoder (codec) is a method for encoding or decoding digital data streams or signals. It uses various algorithms to encode data for transmission or storage, or decodes encoded data for use.

CPU

The CPU value indicates how much of CPU processing power is being used.

Com2Sec

Com2Sec is a security protocol and access method for management.

Cron Log Level

The Cron Log level determines how much information to display or write to file when creating system logs.

| Level |
|-----------------------|
| Everything |
| High Verbosity |
| Low Verbosity |
| Executions and Errors |
| Only Errors |

CHAP

Challenge Handshake Authentication Protocol (CHAP) is a method used to authenticate sessions.

CHAP uses a randomly generated string as a unique challenge phrase for each authentication. This is combined with device host names and hash functions so that no static secret information is sent.

DS-Lite

Dual-Stack Lite (DS-Lite) is a method for sharing of addresses by combining and .

Dial Plan

A dial plan defines what sequence of digits need to be dialled in the to get access to specific calling networks or enable other features.

Device Flags

The Device Flags field shows information about the physical device.

Domain Name

A domain name is typically a name that identifies a resource on the internet with an , according to the .

Delay

Network delay is a network characteristic indicating how long it takes for a piece of data to travel across the network.

Dwell Time

The dwell time is the amount of time spent on each channel in the hopping sequence when hopping from channel to channel.

DLNA

Digital Living Network Alliance (DLNA) is designed to act as a bridge between media and device. It needs either a wired or a wireless network.

DNS

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.

DHCP

DHCP – Dynamic Host Configuration Protocol

A device can be used as a DHCP server to automatically assign an IP address to each computer or device on a network.

DHCP lease

A DHCP Lease is a reservation of a particular provided to a client by a . It is called lease because it expires after a certain amount of time (usually 24 hours). Before the lease expires, the DHCP server should renew the lease or provide a new lease.

DHCP Pool

A DHCP pool is a collection of available for allocation.

The **Pool Start** number is the first available number in the pool.

The **Pool Size** is the count of available numbers, counting from the pool start.

Example: with Pool Start of 50 and a Pool Size of 100, the available pool addresses are 50 to 150.

DHCP Options

When sending DHCP requests, additional options can be requested by providing a space separated list of codes.

| Code | Description |
|------|--|
| 0 | Pad. |
| 1 | Subnet Mask. |
| 2 | Time Offset(deprecated). |
| 3 | Router. |
| 4 | Time Server. |
| 5 | Name Server. |
| 6 | Domain Name Server. |
| 7 | Log Server. |
| 8 | Quote Server. |
| 9 | LPR Server. |
| 10 | Impress Server. |
| 11 | Resource Location Server. |
| 12 | Host Name. |
| 13 | Boot File Size. |
| 14 | Merit Dump File. |
| 15 | Domain Name. |
| 16 | Swap Server. |
| 17 | Root Path. |
| 18 | Extensions Path. |
| 19 | IP Forwarding enable/disable. |
| 20 | Non-local Source Routing enable/disable. |
| 21 | Policy Filter. |
| 22 | Maximum Datagram Reassembly Size. |
| 23 | Default IP Time-to-live. |
| 24 | Path MTU Aging Timeout. |
| 25 | Path MTU Plateau Table. |
| 26 | Interface MTU. |
| 27 | All Subnets are Local. |
| 28 | Broadcast Address. |
| 29 | Perform Mask Discovery. |
| 30 | Mask supplier. |
| 31 | Perform router discovery. |
| 32 | Router solicitation address. |

| | |
|----|---|
| 33 | Static routing table. |
| 34 | Trailer encapsulation. |
| 35 | ARP cache timeout. |
| 36 | Ethernet encapsulation. |
| 37 | Default TCP TTL. |
| 38 | TCP keepalive interval. |
| 39 | TCP keepalive garbage. |
| 40 | Network Information Service Domain. |
| 41 | Network Information Servers. |
| 42 | NTP servers. |
| 43 | Vendor specific information. |
| 44 | NetBIOS over TCP/IP name server. |
| 45 | NetBIOS over TCP/IP Datagram Distribution Server. |
| 46 | NetBIOS over TCP/IP Node Type. |
| 47 | NetBIOS over TCP/IP Scope. |
| 48 | X Window System Font Server. |
| 49 | X Window System Display Manager. |
| 50 | Requested IP Address. |
| 51 | IP address lease time. |
| 52 | Option overload. |
| 53 | DHCP message type. |
| 54 | Server identifier. |
| 55 | Parameter request list. |
| 56 | Message. |
| 57 | Maximum DHCP message size. |
| 58 | Renew time value. |
| 59 | Rebinding time value. |
| 60 | Class-identifier. |
| 61 | Client-identifier. |
| 62 | NetWare/IP Domain Name. |
| 63 | NetWare/IP information. |
| 64 | Network Information Service+ Domain. |
| 65 | Network Information Service+ Servers. |
| 66 | TFTP server name. |
| 67 | Bootfile name. |
| 68 | Mobile IP Home Agent. |
| 69 | Simple Mail Transport Protocol Server. |
| 70 | Post Office Protocol Server. |
| 71 | Network News Transport Protocol Server. |
| 72 | Default World Wide Web Server. |
| 73 | Default Finger Server. |
| 74 | Default Internet Relay Chat Server. |
| 75 | StreetTalk Server. |
| 76 | StreetTalk Directory Assistance Server. |
| 77 | User Class Information. |
| 78 | SLP Directory Agent. |
| 79 | SLP Service Scope. |
| 80 | Rapid Commit. |

| | |
|-----------|--|
| 81 | FQDN, Fully Qualified Domain Name. |
| 82 | Relay Agent Information. |
| 83 | Internet Storage Name Service. |
| 84 | N/A |
| 85 | NDS servers. |
| 86 | NDS tree name. |
| 87 | NDS context. |
| 88 | BCMCS Controller Domain Name list. |
| 89 | BCMCS Controller IPv4 address list. |
| 90 | Authentication. |
| 91 | Client-last-transaction-time. |
| 92 | Associated-ip. |
| 93 | Client System Architecture Type. |
| 94 | Client Network Interface Identifier. |
| 95 | LDAP, Lightweight Directory Access Protocol. |
| 96 | N/A |
| 97 | Client Machine Identifier. |
| 98 | Open Group's User Authentication. |
| 99 | GEOCONF_CIVIC. |
| 100 | IEEE 1003.1 TZ String. |
| 101 | Reference to the TZ Database. |
| 102-111 | N/A |
| 112 | NetInfo Parent Server Address. |
| 113 | NetInfo Parent Server Tag. |
| 114 | URL. |
| 115 | N/A |
| 116 | Auto-Configure |
| 117 | Name Service Search. |
| 118 | Subnet Selection. |
| 119 | DNS domain search list. |
| 120 | SIP Servers DHCP Option. |
| 121 | Classless Static Route Option. |
| 122 | CCC, CableLabs Client Configuration. |
| 123 | GeoConf. |
| 124 | Vendor-Identifying Vendor Class. |
| 125 | Vendor-Identifying Vendor-Specific. |
| 126 - 127 | N/A |
| 128 | TFPT Server IP address. |
| 129 | Call Server IP address. |
| 130 | Discrimination string. |
| 131 | Remote statistics server IP address. |
| 132 | 802.1P VLAN ID. |
| 133 | 802.1Q L2 Priority. |
| 134 | Diffserv Code Point. |
| 135 | HTTP Proxy for phone-specific applications. |
| 136 | PANAAuthentication Agent. |
| 137 | LoSTServer. |
| 138 | CAPWAP Access Controller addresses. |

| | |
|-----------|--|
| 139 | OPTION-IPv4_Address-MoS. |
| 140 | OPTION-IPv4_FQDN-MoS. |
| 141 | SIP UA Configuration Service Domains. |
| 142 | OPTION-IPv4_Address-ANDSF. |
| 143 | OPTION-IPv6_Address-ANDSF. |
| 144 - 149 | N/A |
| 150 | TFTP server address. |
| 150 | Ether boot. GRUB configuration path name. |
| 151-174 | N/A |
| 175 | Ether boot. |
| 176 | IP Telephone. |
| 177 | Ether boot. Packet Cable and Cable Home. |
| 178- 207 | N/A |
| 208 | pxelinux.magic (string) = F1:00:74:7E (241.0.116.126). |
| 209 | pxelinux.configfile (text). |
| 210 | pxelinux.pathprefix (text). |
| 211 | pxelinux.reboottime (unsigned integer 32 bits). |
| 212 | OPTION_6RD. |
| 213 | OPTION_V4_ACCESS_DOMAIN. |
| 214-219 | N/A |
| 220 | Subnet Allocation. |
| 221 | Virtual Subnet Selection. |
| 222-223 | N/A |
| 224-254 | Private use. |
| 255 | End. |

Downlink

A Downlink interface is an interface to subscribers/clients.

DMZ

DMZ (demilitarized zone) is used to provide an extra layer of security. It's a network added between a protected network and an external network.

DSL

DSL – Digital Subscriber Line is a way of providing high bandwidth data communication through regular copper telephone lines.

Discrete MultiTone Modulation

Discrete MultiTone Modulation is a modulation method where the available bandwidth is divided into a large number of channels. Data is allocated to maximize the throughput of every channel. Channels that can't carry data are not used, and the bandwidth reallocated.

DMT is the technology which divides the whole bandwidth on the telephone line into lots of sub-channels and then controlling these 'virtual modems' as one together in order to get higher speeds.

DNS Server

A DHCP server is a server that provides to clients on the a network.

See also: .

Dynamic DNS (DDNS or DynDNS)

Dynamic DNS (DDNS) is a method for automatically providing DNS servers with up to date information about configured hostnames and addresses.

DTMF

Dual Tone - Multi Frequency (DTMF) is a signalling method for telephone systems, which uses a set of eight audio frequencies transmitted in pairs to represent 16 signals, represented by the ten digits, the letters A to D, and the symbols # and *.

DSL Mode

The DSL mode indicates the operation of a line.

DNS Server

A Domain Name System Server runs networking software containing a database of network names and addresses to resources on the internet.

DSCP

A Differentiated Services Code Point (DSCP) is a 6-bit code point in the differentiated services field (DS field) inside the packet IP header.

It is used by for classification purposes to provide functionality.

The bit code corresponds to // values:

| DSCP Name | Binary | Decimal | IP Precedence |
|-----------|---------|---------|---------------|
| CS0 | 000 000 | 0 | 0 |
| CS1 | 001 000 | 8 | 1 |
| AF11 | 001 010 | 10 | 1 |
| AF12 | 001 100 | 12 | 1 |
| AF13 | 001 110 | 14 | 1 |
| CS2 | 010 000 | 16 | 2 |
| AF21 | 010 010 | 18 | 2 |

| | | | |
|------|---------|----|---|
| AF22 | 010 100 | 20 | 2 |
| AF23 | 010 110 | 22 | 2 |
| CS3 | 011 000 | 24 | 3 |
| AF31 | 011 010 | 26 | 3 |
| AF32 | 011 100 | 28 | 3 |
| AF33 | 011 110 | 30 | 3 |
| CS4 | 100 000 | 32 | 4 |
| AF41 | 100 010 | 34 | 4 |
| AF42 | 100 100 | 36 | 4 |
| AF43 | 100 110 | 38 | 4 |
| CS5 | 101 000 | 40 | 5 |
| EF | 101 110 | 46 | 5 |
| CS6 | 110 000 | 48 | 6 |
| CS7 | 111 000 | 56 | 7 |

Differentiated Services

Differentiated Services (DiffServ) is a method for classifying traffic and providing for networks.

DiffServ uses a in the IP header for packet classification purposes.

Packets entering the local network are classified into a *flow* defined by:

- Source
- Destination
- Source
- Destination

Classified flows can be object of multiple QoS mechanisms.

Classification Process

The classification works as follows:

1. Packets are first classified by their .
2. Packets are separated into queues for routing or examination
3. Examined packets are sent for marking or to / mechanisms.
4. Packets leave the interface.

Duplex

The term duplex indicates how traffic is performed. It can be either:

- Half - only one side can communicate at a time.
- Full - both sides can communicate with each other simultaneously.

DFS

Dynamic Frequency Selection (DFS) means that the automatically selects the least congested to use.

DUID

The DHCP Unique Identifier – DUID – is a unique identifier associated with each client and server in a environment. The DUID should be permanently stored and not changed.

Data Package

A data package is a portion of data that transmitted between a source and destination in a network, normally of larger size.

DECT

DECT - Digital Enhanced Cordless Telecommunications is a European standard for cordless telephone systems over radio.

In the United States a slightly different radio frequency range is used, and it is called DECT 6.0.

DCPM

Differential Pulse-Code Modulation (DPCM) is a signal encoding method that uses as a baseline and then compares nearby values to encode a difference instead of a fixed value.

Dropping

Dropping is when a is deliberately dropped due to congestion or other reasons, such as rules.

DDM

Digital diagnostics monitoring (DDM) is a feature for parameter monitoring in a device.

DTMF Mode

The DTMF mode is a setting that governs how signalling is to be performed.

| Mode | Description |
|---------------|---|
| Compatibility | Use RFC2833 by default but switch to inband when reciever does not support RFC2833. |
| RFC2833 | Send DTMF information as messages. |
| SIP INFO | Send DTMF information as messages. |

Ethernet Auto Power Down

Ethernet Auto Power Down allows the hardware ports to be turned off automatically when not in use.

EEE

Energy-Efficient Ethernet (EEE) is a technology for allowing for less power consumption during periods of low data activity.

EoA

Ethernet over ATM (EoA) is a protocol using to provide an Internet connection over .

ESP

Encapsulating Security Payload (ESP) is a security protocol for network data in IPv4 and IPv6 networks.

Ethernet

Ethernet a family of computer networking technologies commonly used in .

Communication over ethernet consists of data frames. Each frame contains source and destination addresses, and error-checking data.

EVDO

Evolution-Data Optimized (EVDO) is a standard for broadband Internet through wireless data transmission.

Firewall Zone

A firewall zone is a grouping of or interfaces, with a common set of firewall rules.

Failover

Failover means switching over to a different network when the selected network cannot be accessed.

Firewall group

A firewall group is a collection of IP addresses that have the same firewall rules.

Firewall Action

The firewall action defines how traffic is handled by the firewall.

| Item | Description |
|---------|-------------------------|
| ACCEPT | Allow the traffic. |
| REJECT | Refuse the traffic. |
| DROP | Ignore the traffic. |
| FORWARD | Pass the traffic along. |

Flow Specification

A flow specification defines data traffic contents and requirements, and is used by devices to decide how to handle packets on the network. It consists of two parts - a , which describe traffic parameters and a that defines requirements for the flow.

Frame

In networking, a frame is a unit of data, consisting of addressing and synchronization information around a payload with data to be transmitted.

Frames of smaller size are often encapsulated in larger frames.

FEC - Forward error correction

Forward error correction entails encoding the signal with redundant information that can be matched to discover errors in the transmission.

GSM

Global System for Mobile Communications (GSM) is a standard for protocols for digital cellular networks used by mobile phones.

GRE

Generic Routing Encapsulation (GRE) is a multipurpose tunneling protocol using networks to encapsulate a number of different network layer protocols.

Genmask

A genmask is the for the destination net. For example 255 . 255 . 255 . 255 for a host destination and 0 . 0 . 0 . 0 for the default route.

Gateway

A gateway is a node in a network that provides interconnectivity between networks of

different types.

For a basic Internet connection, the gateway provides Internet access to the local network.

GPRS

General Packet Radio Service (GPRS) is a mobile data service for mobile communication over and .

Gateway metric

The gateway metric is used for routing decisions, and is added to to enable routing decisions.

Host ID

A host ID is a (label assigned to a network device used to identify the device in the network for addressing purposes.

Hostname

A hostname is a (label assigned to a network device used to identify the device in the network for addressing purposes.

HT Capabilities

HT Capabilities are information about which data rates are supported by a device or network.

HSPA / HSPA+

High Speed Packet Access (HSPA) is an extension of 3G mobile networks utilizing .

Evolved High Speed Packet Access (HSPA+) is a further improvement on HSPA allowing for higher speeds.

IUP

Inteno Universal Provisioning (IUP) is a technology for automatic delivery of service configuration and device settings.

ICMP

The Internet Control Message Protocol (ICMP) is used to send error messages about services or device status.

IP Datagram

A IP datagram is a unit of data transmitted using the protocol, following a specific format which describes various aspects of the datagram, its source and its destination.

The IPv4 datagram consists of the following headers and fields:

| Bits | Name | Description |
|------|-----------------|--|
| 4 | VERS | IP version number 0100 (4) or 0110 (6). |
| 4 | HLEN | Header length in 32-bit words, so if the number is 6, then 6 x 32 bit words are in the header i.e. 24 bytes. The maximum size is 15 x 32-bit words which is 60 bytes. The minimum size is 20 bytes or 5 x 32-bit words. |
| 8 | Type of Service | The field. |
| 16 | Total Length | is the number of octets that the IP datagram takes up including the header. The maximum size that an IP datagram can be is 65,535 octets. |
| 16 | Identification | The Identification is a unique number assigned to a datagram fragment to help in the reassembly of fragmented datagrams. |
| 3 | Flags | Bit 0 is always 0 and is reserved. Bit 1 indicates whether a datagram can be fragmented (0) or not (1). Bit 2 indicates to the receiving unit whether the fragment is the last one in the datagram (1) or if there are still more fragments to come (0). |
| 13 | Frag Offset | in units of 8 octets (64 bits) this specifies a value for each data fragment in the reassembly process. Different sized Maximum Transmission Units (MTUs) can be used throughout the Internet. |
| 8 | TTL | the time that the datagram is allowed to exist on the network. A router that processes the packet decrements this by one. Once the value reaches 0, the packet is discarded. |
| 8 | Protocol | Layer 4 protocol sending the datagram, UDP uses the number 17, TCP uses 6, ICMP uses 1, IGRP uses 88 and OSPF uses 89. |
| 16 | Header Checksum | Header error control. |
| ?? | IP Options | Optional field for testing, debugging and security. |
| ?? | Data | Packet contents, actual data. |

| | | |
|----|---------|--|
| ?? | Padding | Optionally, padding is added to make the datagram into multiples of 32 bits. |
|----|---------|--|

IGMP Snooping

IGMP snooping is the process of listening to network traffic to determine which paths are associated with which IP multicast streams, and allow management of the multicast traffic.

IP Route

Iproute2 is a collection of Linux utilities for handling routing, network interfaces, tunnels, traffic control, network-related device drivers, and other aspects.

IP in IP

IP in IP is an method to provide data tunneling by encapsulating one IP packet in another IP packet, using header information.

IPUI

International Portable User Identity (IPUI), is a unique identifier for each DECT Handset, allowing it to be assigned a identity. The identifier is a 10-digit (40-bit) hexadecimal code

IP ECN

The IP Explicit Congestion Notification (ECN) field is part of the IP header field.

It is used to signal that the network is, or is about to, experience .

A device can use the ECN field to mark a instead of dropping it. The receiver of the packet repeats the ECN back to the sender, which can reduce the transmission rate.

ECN uses the two last bits of the TOS field encode four different codepoints:

| Binary | Value | Description |
|--------|---------|----------------------------|
| 00 | Non-ECT | Non ECN-Capable Transport. |
| 10 | ECT(0) | ECN Capable Transport. |
| 01 | ECT(1) | ECN Capable Transport. |
| 11 | CE | Congestion Encountered. |

IP Address

An Internet Protocol address (IP address) is a numerical identifier for a device address.

IP Quality of Service Algorithm

The IP Quality of Service Algorithm determines which type of QoS to provide; or .

Strict Priority Precedence

Strict Priority Precedence means that where the the packets with the highest priority always are sent first.

Weighted Fair Queuing

Weighted Fair Queuing means that bandwidth is adjusted automatically according to traffic priority and weight value.

Interface Protocol Type

The Interface Protocol Type defines the interface basic type and direction.

Uplink

An uplink interface type is an interface to services.

Downlink

A Downlink interface is an interface to subscribers/clients.

Unmanaged

The interface protocol type Unmanaged means that the connection has no defined protocol.

IPoE

Internet Protocol over Ethernet (IPoE) is a protocol to provide an Internet connection over , by directly encapsulating the data in Ethernet .

IGMP

IGMP – Internet Group Management Protocol is a communications protocol used on IPv4 networks to establish group memberships.

IPv4 Broadcast Address

Broadcast addresses in IPv4 networks are special values in the host-identification part of

an IP address.

IPv4

An IPv4 address is an address represented as four groups separated by a period. Each group consists of decimal numbers between 0 and 255.

An example of an IPv4 address is 192 . 168 . 22 . 12.

Inotify

Inotify (inode notify) is a subsystem to detect changes to the filesystem, and report those changes to applications.

Interface Protocol

The Interface Protocol setting defines the protocol/behavior for an interface.

| Protocol | Description |
|-----------------------|--------------------------|
| Unmanaged | No defined protocol. |
| Static Address | Static IP address. |
| DHCP v4 | Retrieve address through |
| DHCP v6 | Retrieve address through |
| PPP | interface. |
| PPP over Ethernet | interface. |
| PPP over ATM | interface. |
| 3G | over /// |
| 4G | interface over / . |
| Point-to-Point Tunnel | interface. |
| IPv6 Tunnel in IPv4 | interface. |
| IPv6 Tunnel in IPv6 | interface. |
| IPv6 rapid deployment | interface. |
| Dual Stack Lite | interface. |
| PPP over L2TP | over . |

Interface Type

The Interface Type defines the base settings for the interface.

| Type | Description |
|------------|-------------------------|
| Standalone | Not requiring hardware. |
| Any WAN | Any interface. |
| Bridge | . |

lopsys

lopsys stands for Inteno Open Platform System. It combines the efficiency and power of the SOC (System on Chip) with the open source distribution. It further enables the operator to leverage on the modularity of OpenWrt to integrate new applications to the CPE.

IP Precedence

IP precedence is a method to assign priority to data packets by using part of the field in the IP datagram header.

With IP precedence, the first three bits of the TOS field is used to provide one of eight possible precedence values.

| Binary | Value | Priority |
|--------|-------|----------------------|
| 000 | (0) | Routine |
| 001 | (1) | Priority |
| 010 | (2) | Immediate |
| 011 | (3) | Flash |
| 100 | (4) | Flash Override |
| 101 | (5) | Critical |
| 110 | (6) | Internetwork Control |
| 111 | (7) | Network Control |

IP

The Internet Protocol (IP) is a for transmission of over computer networks. It is combined with the to provide Internet networking.

Addressing is done through the use of for and addressing systems.

IntServ

Differentiated Services (DiffServ) is a method for classifying traffic and providing for networks.

DiffServ uses to handle traffic flow management.

IPTV

Internet Protocol Television (IPTV) delivers television services over networks as a streaming service.

IPv6 Address

An IPv6 address is an address represented as eight groups separated by colons (:). Each

group contains four hexadecimal digits.

An example of an IPv6 address is 2011:09bd:583a:0000:8a2e:0000:0370:7334.

IAID

The Interface Association Identifier – IAID – that is a binding between the interface and one or several IPv6 addresses. It is used in servers together with with a to identify IP allocations.

IGMP Proxy

An Internet Group Management Protocol (IGMP) Proxy is a setting to enable the device to handle IGMP host tasks such as sending membership and leave group membership reports to groups.

IP TOS

The IP Type of Service (TOS) field (also known as DiffServ or DSCP field) is a part of an header, originally meant to describe the purpose of a datagram.

It is used by for the , and the optional .

IPtables

Iptables is a firewall application that uses configured tables to determine firewall rules and routes.

Jitter

Jitter is variations in packet arrival time, which may be caused by network congestion, timing delays, or changed routes.

Jitter Buffer

A jitter buffer is storage for voice packets so they can be sent out in evenly spaced intervals used to reduce , providing better transmission reliability.

There are two **jitter buffer implementation** types which are used by the SIP channel reciever.

| Implementation | Description |
|----------------|-----------------------------|
| Fixed | Use a fixed buffer size. |
| Adaptive | Use a variable buffer size. |

JUCI

JUCI (Java User Control Interface) provides a command line and graphical user interface for administration of devices.

LTE

Long-Term Evolution (LTE) is a standard for high-speed wireless communication for mobile phones and data terminals, based on and .

LCP

The Link Control Protocol (LCP) is part of the and is used to set up the PPP connection.

LLC

The logical link control (LLC) layer provides multiplexing to enable different network protocols to coexist and be transported over the same network medium.

Lease Time

Client lease time or lease time is the length of time a local device retains an IP address.

Logging Level

The Logging level determines how much information to display or write to file when creating system logs.

Error messages come with a identifying level tag which makes it possible to filter out messages according to severity.

| |
|--------------|
| Level |
| Emergency |
| Alert |
| Critical |
| Error |
| Warning |
| Notice |
| Info |
| Debug |

LSAP

Link Service Access Point (LSAP) fields are used to identify which protocol handler should process an incoming .

LSAP fields allow the receiving node to pass each received frame to an appropriate device driver which understands given protocol.

L2TP

Layer 2 Tunneling Protocol (L2TP) is a protocol used to support , where security is provided in the transmitted packages rather than in the tunneling.

Latency

Latency is the time it takes for a packet of data to get from source to destination, normally measured by performing a round-trip test: sending a packet that is returned to the sender.

LAN

LAN – Local Area Network is a number of connected units within a limited area, typically a building.

Loop Attenuation

Loop Attenuation is a measure of the quality of the line - how much the signal weakens over the loop.

Attenuation is measured in Decibel (dB). A value between 20dB-45dB can be considered normal.

Latency Path

The DSL Latency Path comes in three modes: *Path 1* (Fast), *Path 2* (Interleaved) and *Both 1 & 2*. Fast is used for applications sensitive to delay. Interleaved suits applications sensitive to errors.

Load Balancing

Load balancing distributes traffic over multiple networks to provide an even load on each WAN interface.

Link Speed

The link speed for a connection is the maximum transmission rate the device can provide. The actual speed may be lower.

MCR

The Minimum Cell Rate (MCR) defines the lowest rate at which cells can be transported in

an connection.

Multicast

Multicast is group communication where information is addressed to a group of destination computers simultaneously.

IP multicast is a method of sending Internet Protocol data messages to a group of interested receivers in a single transmission. It is often employed for streaming media applications on the Internet and private networks. The method is the IP-specific version of the general concept of multicast networking.

It uses specially reserved multicast address blocks in IPv4 and IPv6.

In IPv6, IP multicast addressing replaces broadcast addressing as implemented in IPv4.

MPDU

A MAC Protocol Data Unit - MPDU - is a message transmitted to and from devices.

MIB

A management information base (MIB) is used in to describe the management data structure, in the form of a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

Masquerading

Firewall masquerading entails modifying addressing to allow devices to communicate with the WAN without being visible externally. To the external network, all traffic will look as originating from the gateway.

MiniDLNA

MiniDLNA is media server for / clients.

MTU

Maximum Transmission Unit (MTU) is the largest physical packet size that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. MTU is measured in bytes.

MAC

A Media Access Control (MAC) address is a unique identifier for physical network interfaces.

MSS Clamping

Maximum Segment Size Clamping entails changing the of all connections with a lower than 1500.

MSDU

A MAC Service Data Unit - MSDU - is a unit of data transmitted to and from devices, containing the packet and additional link layer information.

MBS

Maximum Burst Size (MBS) is the maximum size of that can be transmitted in direct sequence on a particular connection.

MSS

Maximum Segment Size (MSS) is a parameter specifying the largest byte size a a single TCP segment can contain for a device.

NIC

A Network Interface Controller – NIC, is an hardware component that connects a device to a network.

Netmask

A netmask is a mask used to divide an IP address into subnets and specify the network's available hosts.

For example, in 255.255.225.0, “0” is the assigned network address. In 255.255.255.255, “255” is the assigned broadcast address. The 0 and 255 are always assigned.

NTP - Network Time Protocol

NTP is a networking protocol for clock synchronization between devices in networks.

Network interface

A network interface is the access point between a device and a computer network. A network interface can be either a physical connection or a software access address.

NAT Loopback

NAT loopback is a method using to provide access to services via the public IP address

from inside the local network.

Network Profile

A network profile is a global setting for your device that defines how it will work in the network.

For example, selecting a particular profile may configure your device as a wireless repeater or as a fully routed NAT gateway.

Depending on the selected profile, available features and settings will be different.

Some sample profiles:

| Profile | Description |
|---------------------|--------------------------------|
| Bridged IPTV | service in a network. |
| VoIP + Bridged IPTV | Both and service in a network. |
| Wireless Repeater | Wireless . |
| Fully Routed (NAT) | All features with capability. |

NAT

Network Address Translation (NAT) is a method to to device translate local network addresses into external addresses for the Internet.

Next Hop

Next hop refers to the next closest device a packet can go through, according to the routing table.

NTP Mode

The NTP Server mode allows the device to act as a local server even when losing connection to the providing NTP server.

NAT-PMP

The NAT Port Mapping Protocol (NAT-PMP) is a network protocol to automatically detect and determine the gateways to configure NAT settings and .

Noise level

The WiFi Noise level is the amount of interference in your wireless signal, such as crosstalk, radio frequency interference, distortion, and so on.

It is measured in decibels from zero to -120, where a lower value is better.

Typical environments range between -100db and -80db.

Network bridge

A network bridge combines two network segments into an aggregated network, making them behave as if they are one continuous segment.

OBSS Coexistence

Overlapping basic service sets (OBSS) is a setting that configures the to allow coexistence between 20 MHz and 40 MHz overlapping basic service sets (OBSS).

OpenWRT

OpenWrt is an open source distribution with an excellent overall user space environment, modular and flexible system design. It has a large and active development community.

More information:

More information and documentation is available at <http://wiki.openwrt.org/>.

OSWD

The Open Web-Server Daemon - OSWD - handles web requests to the configuration framework. It allows access to device configuration services through the configuration framework.

Overhead

Overhead is extra data or processing needed to manage delivery of a network data.

OUI

An Organizationally Unique Identifier - OUI - is a 24-bit number used to uniquely identify a vendor.

Usually makes up the first three octets of the address.

Port

A port is a communication endpoint, identified by a number, which combined with an IP address provides the necessary addressing for a service on the network.

Packet Scheduler / Queueing Discipline

A queueing discipline / packet scheduler is a network function that distributes available to different connections according to an algorithm.

The management is done by deciding how many each connection is handed, by handling the device traffic queue and making prioritizing incoming/ingress or outgoing/egress packets.

The scheduling can be done either by automatically, based on observed traffic, or following rules according to a protocol such as or .

Port Forwarding

Port forwarding is a feature that forwards inbound traffic from the internet on a specific port (or ports) to a specific device (or port) on your local network ().

PTM Priority

The PTM Priority defines how traffic packets should be handled.

| Priority | Description |
|-----------------|--|
| Normal Priority | Sen packets according to their priority. |
| High Priority | Use preemption; lower-priority packets are paused when higher-priority packets are sent. |

Packet Loss

When are transmitted in a network they may travel different routes from source to destination. This means there is no guarantee that packets will arrive in time or arrive at all. They may also be denied at the receiver due to a full buffer or other issues. A collective term this is packet loss.

Precedence

Precedence in uses a to assign priority to data packets.

The Precedence setting defines parameters, by indicating priority though the and using values.

| ID | Setting |
|-----|----------------------|
| All | Default |
| 0 | CS1, AF11, AF12 |
| 1 | CS2, AF21, AF22 |
| 2 | CS3, AF31, AF32 |
| 3 | CS4, AF41, AF42 |
| 4 | CS5, Voice-admit, EF |

| | |
|---|-----|
| 5 | CS5 |
| 6 | CS6 |
| 7 | CS7 |

Proxy

A proxy server works as an intermediary between the client and other servers, forwarding traffic to and from the servers and client. It adds functionality for improving aspects of the connection, such as security, reliability or simplicity.

Periodic Inform

The Periodic Inform setting determines whether must periodically send information to the .

PTM - Pulse-Time Modulation

Pulse-Time Modulation means encoding traffic into a pulsing signal for transfer.

Traffic Policing

Traffic Policing is a process where are handled according to user-defined criteria. Depending on the criteria, the packets may be marked, dropped or completely ignored.

The purpose of traffic policing is to make sure that bursts in traffic are handled and the designated traffic flows get appropriate bandwidth.

Packet Aggregation

Packet aggregation means combining into larger units, in order to reduce the overhead associated with each transmission.

Pairing

Pairing is the process of making two compatible wireless devices able to communicate with each other. This is normally done by making them visible to each other, and providing a PIN code for identification.

PLC

Packet loss concealment (PLC) is a technique to mask the effects of in communications.

PCR

Peak Cell Rate (PCR) defines the highest rate at which cells can be transported in an connection.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PTPT) is a technology for through and a with packets.

Port Speed

Port speed settings affect how a LAN or WAN port negotiates the speed setting.

Negotiation can be turned off (speed setting: **only**) or use (speed setting **max**) to determine actual speed.

Communication on a port can be either half or full .

A port that is set to **disabled** does not handle any traffic.

PoP

A Point of Presence (PoP) is an access point to the Internet.

Ping

Ping is a network tool which tests accessibility of hosts on an Internet Protocol network. It measures how long a it takes for a message to travel from the measuring host to the destination and back.

PPP

Point-to-Point Protocol (PPP) is a protocol for providing a direct data link connection with authentication, encryption and compression.

PSK

A Pre-Shared Key (PSK) is a shared secret which was previously shared between the two parties using some secure channel before it is used.

PPPoA

PPP over ATM (PPPoA) is a protocol using to provide an Internet connection over .

Protocol

A protocol is a set of rules for how to handle data, specifically for transmission and management. The sender and reciever noth use the same protocol to structure, send and receive it, ensuring that the data remains intact, readable and usable.

PAP

Password Authentication Protocol (CHAP) is a method used to authenticate sessions.

PAP works like a standard login procedure; using a static user name and password combination.

PPID

The PPID – Parent Process ID – is the of the process that started a particular process.

Prefix delegation

Prefix delegation is used in DHCPv6 to assign a network address prefix and automate configuration and provisioning of the public addresses for the network.

PSDN

A packet-switched data network - PSDN - is a network where communication is done by transmitting and receiving data . Devices are not connected directly, but packets from different sources going to different destinations share transmission channels.

PPPoE

PPP over Ethernet (PPPoE) is a protocol used to provide an Internet connection over , by putting PPP frames inside Ethernet .

PSTN

The Public Switched Telephone Network (PSTN) is the publicly available network of telecommunication systems and services provided by telephone operators.

Packetization

Packetization is the process of dividing data into for transmission according to a defined .

PCM

Pulse-code modulation (PCM) is the standard method for digital audio. PCM entails converting analog signals to digital values by sampling the amplitude of the analog signal at set time intervals. Each sample is to the nearest value within a range of digital steps. With PCM, the ranges vary with the source amplitude, so that the steps are larger at higher amplitudes.

PCM is defined by *sampling rate* (number of times per second that samples are taken) and

bit depth (number of different digital values).

PBX

A Private Branch Exchange (PBX) is a switch used for connecting telephone devices or virtual applications in an organization. It manages internal communication in the network and provides access to the external public switched telephone network, and allows for sharing of lines and direct communication between internal devices.

PID

The PID – Process ID – is a unique identifier for a process, assigned to it when it is loaded into memory.

Packet

A packet is a portion of data that is transmitted between a source and destination in a network. It is normally a smaller part of some larger unit of data, which is tagged with an identification number and an address. When all packets for a specific data unit arrive at their destination, they are reassembled to form the original data.

Division into packets, transmission and reassembly is governed by a transmission .

Quantization

Quantization of signals is a method where a signal is sampled at specified time intervals and the input values are approximated to provide a smaller set of values compared to the actual signal.

QoS Mark

The Mark is used when classifying traffic. Packets matching the filter will be marked with the provided hexadecimal code 0x000000-0xFFFFFFFF.

This mark can then be used for identification and filtering purposes, for example by [iptables](#) .

QoS

Quality of Service (QoS) involves setting for data traffic that affects performance, allowing resources to be allocated depending on the needs of various types of traffic.

QoS Filter

A Filter is used by [classful QDiscs](#) and should belong to.

The filter contains a number of parameters/conditions that the packet needs to match in order to be enqueued in the appropriate class.

Scheduling

Scheduling is a process when a decides to make a leave earlier than other packets.

QoS Class

A Class is a set of rules for various traffic settings that can be applied to data traffic to ensure particular needs for .

It is used by to determine which a should belong to.

QoS Classification Group

A QoS Class group is a collection of which can be added to an interface to provide a combination of settings.

Queueing Discipline / Packet Scheduler

A queueing discipline / packet scheduler is a network function that distributes available to different connections according to an algorithm.

The management is done by deciding how many each connection is handed, by handling the device traffic queue and making prioritizing incoming/ingress or outgoing/egress packets.

The scheduling can be done either by automatically, based on observed traffic, or following rules according to a protocol such as or .

Routing

Routing is the process of selecting paths in a network along which to send network traffic, making routing decisions to ensure that traffic moves from the source to the destination.

Dynamic routing is the most common method, where routing protocols are used to manage routing automatically.

Static routing means that routes are set up permanently using a .

Policy based routing entails selecting routes based on the type of traffic being transmitted, tryingt to use more efficient routes for priority traffic.

RTSP

The Real Time Streaming Protocol (RTSP) is a for control over transmission of real-time

data with the .

Route

The IP Route is the path a data message takes through an Internet Protocol network.

RX Chain Power Save Quiet Time

The number of seconds the packets per second must be below the value before the feature activates itself.

Root QDisc

A Root Queueing Discipline is a collection point for multiple QDiscs/ containing and used for QoS.

Routing Table

A routing table is a table stored in a device used for keeping track of routes to network destinations and metrics belonging to those routes. The information in the routing table is used by devices to make routing decisions for traffic in the network.

Types of routes

| Route | Description | Comment |
|---------|---|--|
| Network | Path to a specific network address. | |
| Host | Route to a specific network address by network and host ID. | Used to optimize specific types of traffic. |
| Default | Route stored in the routing table. | Used when no other routes for the destination are found. |

Route metric

The route metric is used for routing decisions, and is added to to enable routing decisions.

RX Chain Power Save

The RX Chain Power Save feature turns one of the off to save power.

Request SPECification

A Request SPECification (RSPEC) is part of a , and defines the requirements for a flow.

Different possible service types:

| Type | Description | Examples |
|-------------|--------------------|-----------------|
|-------------|--------------------|-----------------|

| | | |
|-----------------|---|---------------------------------------|
| Best Effort | No guaranteed level of service. | WWW, FTP |
| Controlled Load | Behaves as Best Effort for an network without load. | |
| Guaranteed | Guarantees a minimum level of service, but no benefit would be provided by higher levels. | Real-time control, latency and delay. |
| Qualitative | Not immediately quantifiable, but better than Best Effort. | |

RFC2275

RFC 2275 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)- defines an access method for resources based on view access. It limits the access of multiple users having various security levels different views of the object tree.

ROM

A Read Only Memory - ROM - is a read-only memory containing firmware for the device.

Typically, the term ROM actually refers to media that can be erased and re-programmed (is an Erasable Programmable ROM - EPROM, and Electrically Erasable Programmable ROM - EEPROM.)

RFC1918

RFC 1918 - Address Allocation for Private Internets - defines standards for IP addresses in a private local network.

Addresses with in these ranges cannot be routed on the Internet:

10.0.0.0 - 10.255.255.255 (10/8 prefix) 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

RXC

A RX chain is the transmit/receive signal processing hardware, such as a radio transceiver with its own antenna.

RSSI

Received signal strength indicator (RSSI) is a measurement of the power of a received radio signal.

RSVP

The Resource ReSerVation Protocol - RSVP - is a signalling mechanism used for network

management of .

It uses a method where resources available to handle traffic is broadcasted throughout the network.

Listening devices reply with a RESV (Reserve) message containing a for the traffic.

Devices on the route between sender and listener either accept the reservation and handle the flow, or send a reject message.

Reservations can end normally or time out as needed.

RSS (Memory)

RSS – Resident Set Size indicates how much memory is allocated to a process and is in RAM.

It includes all stack and heap memory, and shared libraries also in memory, but not memory that is swapped out.

RX Chain Power Save PPS

The maximum number of packets per second that the WLAN interface should process for during before the feature activates itself.

RTP

The Real-time Transport Protocol (RTP) is a for handling transmission of real-time data, typically audio or video over networks services. Control and monitoring features are provided through the .

Shaping

Traffic Shaping is a process where are delayed, in order to keep exiting traffic under a maximum rate, or make bursts smoother.

Static Route

A static route is a manually entered route to a network destination, which is used instead of any routes discovered automatically.

Static address

A static IP address is an address that doesn't change, unless manually changed by the administrator.

SNR - Signal to Noise Ratio

Signal-to-noise ratio (SNR) is defined as the power ratio between a signal and background noise.

It is normally measured in decibels (dB).

| dB value | Description |
|------------|---|
| < 6dB | Poor. No sync, or intermittent sync problems. |
| 7dB - 10dB | Fair. Vulnerable to conditions. |
| 11dB-20dB | Good. |
| 20dB-28dB | Very good. |
| 29dB < | Excellent. |

Seamless Rate Adaptation

Seamless Rate Adaptation (SRA) allows devices to change data transfer rates on the fly to avoid losing a connection due to interference.

SRV

A Service Record (SRV record) is a specification of data in the containing information about and for a specific service.

It is used by domain servers to keep track of their own changes without having to contact a central DNS server.

An SRV record has the form:

`_Service._Proto.Name TTL Class SRV Priority Weight Port Target`

| Item | Description |
|----------|---|
| Service | Identifier for the service. |
| Proto | The service protocol. |
| Name | Domain name where the record is valid. |
| TTL | DNS . |
| Class | DNS class (IN for Internet). |
| Priority | Target host priority, lower value means more preferred. |
| Weight | A relative weight for records with the same priority. |
| Port | Port for the service. |
| Target | for the service provider. |

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a protocol for managing and devices on an IP network.

SNAP

The Subnetwork Access Protocol (SNAP) is an extension used to distinguish additional higher layer protocols compared to .

SNAP fields allow the receiving node to pass each received frame to an appropriate device driver which understands given protocol.

SSID

SSID – Service Set IDentifier, also known as network name, identifies a wireless network .

SIP Realm

A SIP realm is a authentication/authorization component, defining the set of usernames and passwords for a particular protection domain. The SIP realm does not have to be the same as a the .

The SIP Realm is used together with an to provide access to SIP services.

SNR Margin

The SNR margin is the difference between the current and minimal SNR required to sync at a specific transfer speed.

Higher SNR margin means a better signal, with less background noise, which in turn means a more stable the connection.

STUN

Session Traversal Utilities for NAT (STUN) consists of methods and a protocol to allow a server to discover its public IP address from behind a . It is used for real-time voice, video, messaging, and other interactive IP services.

The protocol requires a STUN server located on the public side of the NAT.

SIP Reg Interval

The SIP Reg Interval is how often connections to a provider is updated. This is normally done by updating the registration with the server.

Samba

Samba is an open source software that provides file and print services between Linux/Unix servers and Windows-based clients.

SSDP

Simple Service Discovery Protocol (SSDP) is a network protocol capable of discovering universal plug and play devices on a home network.

SIP

The Session Initiation Protocol (SIP) is a protocol for handling communication sessions, most commonly for Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol networks.

State Code

The process state code indicates the state for a process.

| Short Code | Meaning | Description |
|------------|---|---|
| D | Uninterruptible sleep | Usually refers to IO processes. |
| I | Is multi-threaded (using CLONE_THREAD, like NPTL pthreads do) | |
| L | Has pages locked into memory (for real-time and custom IO) | |
| N | Low-priority (nice to other users) | |
| R | Running runnable (on run queue) | |
| s | Is a session leader | |
| S | Interruptible sleep | Waiting for an event to complete. |
| T | Stopped | May have been stopped by control signal or trace. |
| W | Paging | Storing or retrieving data. |
| Z | Defunct ("zombie") process | Terminated but not collected by its parent process. |
| < | High-priority | |
| + | Belongs to foreground process group. | |

Source-Specific Multicast

Source-specific multicast (SSM) is a method of limiting delivery of packets only from a requested source address.

SIP Server/Registrar

A SIP server (also called SIP Registrar or SIP Proxy) handles management for a -based .

It handles setup and connections for SIP calls in a network, but does not handle actual transmission of real-time data.

Service Type

Service types define the guaranteed level of service in a network. This involves such things as the timing between the source and destination, the guaranteed bandwidth and how many cells get lost in transmission.

| Setting | Description |
|------------------|---------------------|
| UBR without PCR | Use without . |
| UBR with PCR | Use with . |
| CBR | Use . |
| Non-Realtime VBR | Use Non-Real-Time . |
| Realtime VBR | Use Real-Time . |

SRTP

The Secure Real-time Transport Protocol (SRTP) is used for providing authentication, encryption, and other security features with the .

SIP Account

A SIP Account contains the identifying information and configuration for communication.

SSH

Secure Shell (SSH) is a protocol for secure communication on networks. Most commonly it is used for remote login to devices, typically to unix shell accounts.

Subnet Mask

A subnet mask is used to divide the IP address into network and host addresses.

SIP Domain

A SIP domain is a DNS hostname for traffic routing.

SIP User

A SIP User is the identifier for a . This may be a phone number.

SIP Address

A SIP Address is similar to a phone number for voice calls to other .

SIP Codec

SIP codecs are designed for use with traffic.

G.711ALaw

G.711ALaw is a standard using non-linear encoding and decoding to provide pulse code modulation mainly of voice frequencies with the A-law variant algorithm.

G.711MuLaw

G.711MuLaw is a standard using non-linear encoding and decoding to provide pulse code modulation mainly of voice frequencies with the μ -law variant algorithm. It provides higher compression than A-Law, with higher distortion for smaller packets.

G.729a

G.729 is a compression standard with linear compression for voice with low bandwidth requirements, suitable for applications where bandwidth conservation is an issue. It divides 10ms packets for a 8kbit/s transmission rate.

G.726

G.726 is a compression standard used to transmit voice at transmission rates of 16, 24, 32, and 40 kbit/s. The 32 kbit/s mode is the standard codec for wireless phone systems.

SFP

The Small Form-factor Pluggable (SFP) connector is a hot-pluggable transceiver used for telecommunication and data.

More information:

For more information see [the wikipedia article](#).

SCR

Sustained Cell Rate (SCR) is the maximum average rate at which can be sent over the connection. SCR can never be greater than .

Strict Priority Precedence

Strict Priority Precedence means that where the the packets with the highest priority always are sent first.

SSL

Secure Sockets Layer (SSL) is a for providing security features such as authentication, privacy and data integrity in a network.

SIP Authentication Name

A SIP Authentication Name is used together with an to provide access to SIP services. The authentication username doesn't have to be the same as the name.

SNMP Agents

An SNMP agent provides access to management data as variables that can be modified to perform management tasks remotely. The variables accessible via SNMP are organized in hierarchies and stored together with metadata in .

TR069

TR-069 CPE WAN Management Protocol (CWMP) was created by the DSL Forum to standardize the Wide Area Network (WAN) management of CWMP. The TR-069 protocol specifically defines a common method for CPE devices to communicate with an Auto Configuration Server (ACS).

Traceroute

Traceroute is a network diagnostic tool to discover the and data delivery time over an Internet Protocol network.

See also .

TPtest

TPTEST allows you to measure the speed of your Internet connection, by sending a number to and from a defined reference test server.

More information:

A list of TP test servers is available at <http://tptest.sourceforge.net/servers.php>.

TLS

Transport Layer Security (TLS) is a for providing security features such as authentication, privacy and data integrity in a network.

TD-SCDMA

Time Division Synchronous Code Division Multiple Access (TD-SCDMA) is an 3G mobile networks in China.

TCP

The Transmission Control Protocol (TCP) is a protocol to provide reliable data streams over an network.

TTL

Time to live (TTL) is a mechanism to determine when data in a network should be discarded, for example for cache expiry, or to prevent data from being transmitted forever.

Token Bucket

A token bucket algorithm is a method of handling packet traffic, by using an analogy of a *bucket* containing a number of *tokens* that arrive at a particular rate. Tokens are used to limit when data packets are transmitted.

The *depth* of the bucket limits the number of tokens, and the rate of arriving tokens limits how quickly packets can be sent.

The concept is as follows:

- Tokens are added to the bucket at a fixed rate.
- If the bucket becomes full, arriving tokens are thrown away.
- Arriving data packets use up tokens from the bucket and are transmitted on the network.

This means that the bucket needs to be deep enough to handle bursts of traffic, and the token rate limits the transmission rate.

TCP Flags

Transmission Control Protocol (TCP) Flags are control bits for messages which indicate how packets should be handled or indicate connection states.

| Flag | Description |
|------|--------------------------------------|
| SYN | Synchronize sequence numbers. |
| ACK | Acknowledgment field is significant. |
| FIN | No more data from sender. |
| RST | Reset the connection. |
| URG | Urgent pointer field is significant. |
| PSH | Push function. |
| CWR | Congestion Window Reduced. |
| ECE | TCP peer is ECN capable. |

TPC

Transmission Power Control (TPC) is used to automatically adjust the transmission power

level on to avoid interference.

TKIP

TKIP (Temporal Key Integrity Protocol) is a RC4 stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.

Traffic SPECification

A Traffic SPECification (TSPEC) is part of a , and describes traffic flow properties, typically involving algorithm parameters.

UDP

User Datagram Protocol (UDP) is a protocol to provide relatively unreliable data streams over an network. It provides no guarantees for delivery and no protection from duplication.

The simplicity of UDP reduces the overhead from using the protocol and the services may be adequate in many cases.

Unicast

Unicast is communication where information is addressed to a single destination.

UBIFS

UBIFS file-system stands for “Unsorted Block Images File System”.

It is a flash file system, designed to work with flash devices, using Memory Technology Device (MTD) device files.

UAPSD

Unscheduled Automatic Power Save Delivery (UAPSD) is a wifi device feature which allows them to save power by dozing between transmissions.

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols used for automatic discovery and communication on a network. It makes it possible for various devices to connect and share services.

UPnP involves automatic port forwarding set up without user interaction. This may constitute a security risk.

USB

USB – Universal Serial Bus is a standard for connection, communication, and power supply between computers and electronic devices.

UBR

Unspecified Bit Rate (UBR) is used for non-real-time applications that do not require any maximum bound on the transfer or .

UMTS

Universal Mobile Telecommunications System (UMTS) is a third generation mobile cellular system for networks based on the GSM standard.

Uplink

An uplink interface type is an interface to services.

UUID

A Universally Unique Identifier (UUID) is an 128-bit identifier used to uniquely identify objects.

Example: 65613210-44d4-11e6-beb8-9e71128cae77

Unmanaged

The interface protocol type Unmanaged means that the connection has no defined protocol.

VOIP

VoIP - Voice Over IP is a group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol networks.

VC-MUX

Virtual Circuit Multiplexing (VC-MUX) is a method for identifying the protocol carried in used in .

Using virtual circuit multiplexing, hosts agree on the high-level protocol for a given circuit. Each high-level protocol requires a separate virtual circuit.

VCI

Virtual Channel Identifier - VCI, is used together with to enable networks.

In an ATM network, each circuit is given a virtual channel identifier, and and each path is given a virtual path identifier.

The VCI identifies circuit/channel in use, and VPI matches the appropriate path to the desired destination host.

%VSZ

VSZ is the Virtual Memory Size. It includes all memory that the process can access, including memory that is swapped out and memory that is from shared libraries.

VPI

A Virtual Path Identifier - VPI, is used together with to enable networks.

In an ATM network, each circuit is given a virtual channel identifier, and and each path is given a virtual path identifier.

The VCI identifies circuit/channel in use, and VPI matches the appropriate path to the desired destination host.

VLAN

A virtual LAN (VLAN) is, as the name implies, a virtualized . Most commonly a VLAN is a subdivision of a network.

VLANs also allow grouping of hosts together even if the hosts are not connected to the same network device, and managing them through software.

VDSL

Very-high-bit-rate digital subscriber line (VDSL) is a technology providing network traffic over copper wires.

VDSL is faster than , with up to 52 Mbit/s downstream and 16 Mbit/s upstream speeds.

VPN

A virtual private network (VPN) is a secured, private network connected through a public network.

VBR

The Variable Bit Rate come in two variants: Non-Realtime VBR and Realtime VBR.

Non-Realtime VBR

Non-Real-Time Variable Bit Rate (nrt-VBR) is used for connections that need guaranteed or , but do not rely on accurate timing between source and destination.

Realtime VBR

Real-Time Variable Bit Rate (rt-VBR) is used for connections that need accurate timing between source and destination.

VSZ

VSZ is the Virtual Memory Size. It includes all memory that the process can access, including memory that is swapped out and memory that is from shared libraries.

Virtual Network Interface

Virtual network interfaces are linked to a hardware device, but are not hardware devices.

A virtual network interface is generally associated with a physical network, another virtual interface, a loopback interface or other standalone interfaces.

Types of Virtual Network Interfaces

| Type | Example | Description |
|-------------------|-----------------------|--|
| Aliases | eth4:5, eth4:6 | Used to handle multiple IP-addresses per interface. Supported for backwards compatibility. |
| Bridges | br0, br-lan | Used to make multiple network interfaces behave as one network interface. |
| Stacked VLANs | 10, 20 | IEEE 802.1ad type network, using two or more tags in each packet. |
| Special purpose | imq0, teql3 | Used to change the order of outgoing or incoming network packets. |
| Tunnel interfaces | pppoe-dsl, tun0, vpn1 | Used to send packets over a tunneling protocol. |
| VLANs | eth4.0, vlan0 | Used to separate a network into |

| | | |
|--|-------------|---|
| | | multiple virtual networks. |
| Wireless operating mode virtual interfaces | wlan0, ath3 | A wireless subsystem created automatically for a wireless master interface. |

Weighted Fair Queuing

Weighted Fair Queuing means that bandwidth is adjusted automatically according to traffic priority and weight value.

WEP

Wired Equivalent Privacy (WEP) is a security algorithm intended to provide security comparable a wired network.

WEP uses a key of 10 or 26 hexadecimal digits.

WiFi Mode

The WiFi Mode defines which to use for wireless communication in the network.

Auto

The Auto Mode allows the device to automatically select a suitable profile among the available options.

802.11a

802.11a is a specification for the 5 GHz band with a maximum data rate of 54 Mbit/s.

802.11ac

802.11ac is a specification for both the 2.4 GHz and the 5 GHz bands with support for multiple-input multiple-output antennas, providing a maximum data rate from 433 Mbit/s to 1300 Mbit/s.

802.11b

802.11b is a specification for the 2.4GHz band with a maximum data rate of 11 Mbit/s .

802.11b/g

802.11b/g is a specification combining and standards in dual band mode.

802.11g

802.11g is a specification for the 2.4 GHz band with a maximum data rate of 54 Mbit/s.

802.11n

802.11n is a specification for both the 2.4 GHz and the 5 GHz bands with support for multiple-input multiple-output antennas, providing a maximum data rate from 54 Mbit/s to 600 Mbit/s.

WPA2 PSK

Short for Wi-Fi Protected Access 2 – Pre-Shared Key, and also called WPA2 Personal, it is a method of securing your network using Pre-Shared Key (PSK) authentication,

Wi-Fi Protected Access 2 Personal uses pre-shared passphrases between 8 and 63 characters long.

The wireless device converts the pre-shared key to a hash and uses that for communication authentication.

WiFi Key

The WiFi Key or passphrase is a shared secret between client and server used for encryption and decryption in wireless networks.

Wireless radio

A wireless radio is the device sending out a wireless signal. Each radio can have several associated with it.

WMM

WMM (Multimedia) improves quality of service on a network by prioritizing data by four configurable categories:

Voice: Voice packets for Voice over IP (VoIP) calls.

Video: Video packets for support of TV streams.

Best effort: Support for legacy devices or devices lacking QoS standards.

Background: File downloads, print jobs and other traffic that does not suffer from increased latency.

WPA personal

Wi-Fi Protected Access (WPA), also referred to as WPA-PSK (pre-shared key) does not require an authentication server.

It uses , with a key either as a string of 64 hexadecimal digits, or as a passphrase of 8 to

63 characters.

WPA also includes a message integrity check, which is designed to prevent an attacker from altering and resending data packets.

WPA-Personal mode is available with both WPA and WPA2.

WCDMA

Wideband Code Division Multiple Access (W-CDMA) is a mobile communications technology using for broadband.

WiFi encryption

WiFi encryption means to encrypt the messages that are sent between nodes on a wireless network.

A can use one of several encryption options:

| | |
|------------------------------------|----------------|
| None | No encryption. |
| WEP | |
| WPA2 Personal (PSK) | |
| WPA/WPA2 Personal (PSK) Mixed Mode | |
| WPA2 Enterprise | |
| WPA/WPA2 Enterprise Mixed Mode | / |

WPA2 Enterprise

Wi-Fi Protected Access 2 Enterprise is designed for enterprise networks and requires an authentication server.

It provides additional security (e.g. protection against dictionary attacks on short passwords).

Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication.

WiFi channel

A wifi channel is a frequency range in a specific used for wifi communication.

WPA Enterprise

Also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK), is designed for enterprise networks and requires an authentication server.

It provides additional security (e.g. protection against dictionary attacks on short passwords).

Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication.

WMM Power Save

WMM Power Save allows small devices, such as phones and PDAs, to transmit data while in a low-power status.

WiFi band

A wifi band is a collection of provided by a particular .

Bands are identified by their frequency as measured in Gigahertz (GHz).

Standard bands are 2.4GHz and 5Ghz.

WiFi

WiFi or Wi-Fi is a technology allowing devices to connect to a wireless LAN () network. The term “Wi-Fi” is a play on words relating to hi-fi (high fidelity) from the music industry. Communication is commonly done over 2.4 gigahertz and 5 gigahertz radio bands.

WMM Acknowledgement

WMM (Multimedia) Acknowledgement is a verification signal sent from the client to the device to indicate that no error has been detected for the data .

WAN

A Wide Area Network (WAN) is network that extends over a large geographical distance.

WPS

Wi-Fi Protected Setup (WPS) is an authentication key distribution method. It can be performed in one of several ways.

PIN code: A PIN is entered on the client.

Push button: An actual or virtual button is pressed on the device and the client within a short amount of time.

Near field: The client is brought physically close to the device.

USB: An USB device is used to transfer data between the new client and the device.
(Deprecated)

LAN

A Wireless Local Area Network is connected through one or several .

WiFi interface

A wireless interface is the access point to a . Interfaces are identified by their .

Each radio can have several SSIDs and each SSID interface can be configured as part of a or .

WWAN

A Wireless Wide Area Network (WWAN), is a wireless network that extends over a large geographical distance.

6to4

6to4 is a method to transmit traffic over networks without having to configure explicit tunnels.

6rd

6rd is a method for rapid deployment on Internet Service Provider infrastructures, operating within the ISP's network.

802.11g

802.11g is a specification for the 2.4 GHz band with a maximum data rate of 54 Mbit/s.

802.11n

802.11n is a specification for both the 2.4 GHz and the 5 GHz bands with support for multiple-input multiple-output antennas, providing a maximum data rate from 54 Mbit/s to 600 Mbit/s.

3G

Third-generation wireless telephone technology (3G), is a cellular network for digital mobile data communication for broadband traffic.

802.11ac

802.11ac is a specification for both the 2.4 GHz and the 5 GHz bands with support for multiple-input multiple-output antennas, providing a maximum data rate from 433 Mbit/s to

1300 Mbit/s.

6in4

6in4 is a method to transmit traffic over explicit connections.

The traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41.

802.11a

802.11a is a specification for the 5 GHz band with a maximum data rate of 54 Mbit/s.

802.11b/g

802.11b/g is a specification combining and standards in dual band mode.

802.1q

IEEE 802.1Q is a standard for Ethernet where VLANs are given a numeric tag. The tag is used to identify traffic in networks, and decide how to handle it.

This allows multiple bridged networks to share the same physical link without leaking information to each other networks.

802.1p

802.1p is a standard for priority levels, identifying the class of service a is to be used for. There are 8 different levels, numbered from 0 to 7.

| Priority | Acronym | Traffic types | Comment |
|----------|---------|-----------------------|-----------------------------|
| 0 | BK | Background | Lowest |
| 1 | BE | Best Effort | |
| 2 | EE | Excellent Effort | |
| 3 | CA | Critical Applications | |
| 4 | VI | Video | < 100 ms latency and jitter |
| 5 | VO | Voice | < 10 ms latency and jitter |
| 6 | IC | Internetwork Control | |
| 7 | NC | Network Control | Highest |

802.11b

802.11b is a specification for the 2.4GHz band with a maximum data rate of 11 Mbit/s .

2G

Second-generation wireless telephone technology (2G), is a cellular network for digital mobile data communication.

4G

Fourth-generation wireless telephone technology (4G), is a cellular network for digital mobile data communication for high-speed broadband.