TORNADO M100 CELLNODE

USER MANUAL

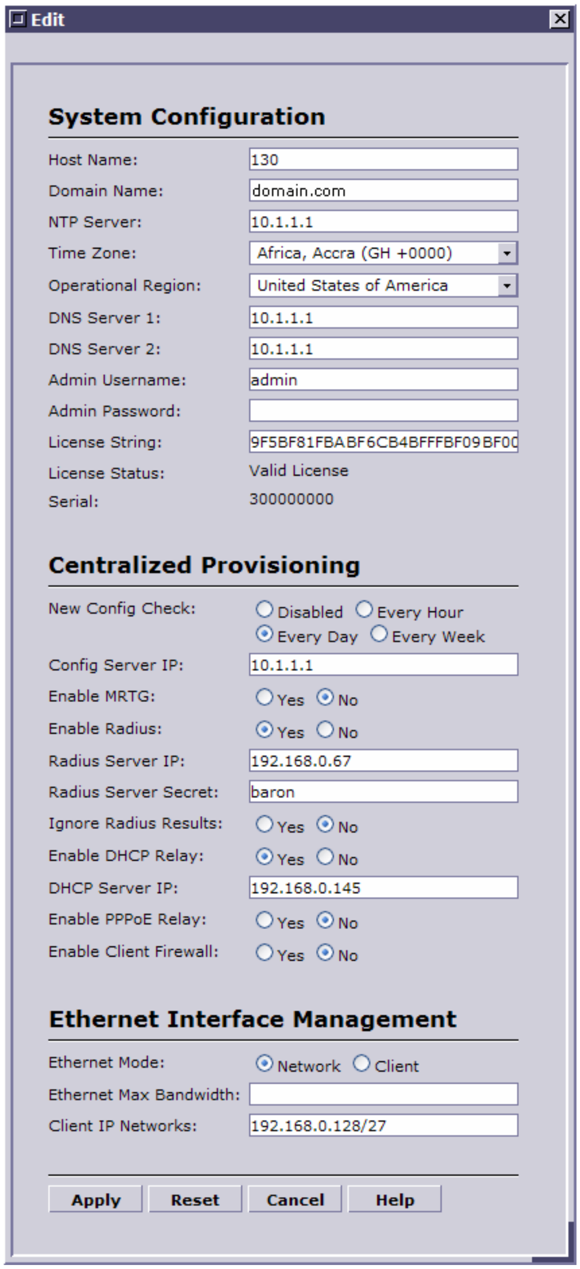
Contents

START Menu

Navigator	Initiate the main menu management function
Help	Initiates the Help file
Log Off	Logs of the currently logged web user
Get Remote Configuration	Gets the remote device configuration form a central provisioning server
Upgrade Firmware	Upgrade the device firmware
Restart All Services	Restarts all services
Reboot Cellnode	Reboots the OS of the CellNode M100
Reset Configuration	Resets the configuration to default values
Close Console	Closes the Web Console

System Configuration

System Configuration allows easy setup of the network parameter of the CellNode M100 device. All parameters in this dialog can be over-written at any time once the device is centrally provisioned.



System Configuration

Host Name: 130

Domain Name: domain.com

NTP Server: 10.1.1.1

Time Zone: Africa, Accra (GH +0000)

Operational Region: United States of America

DNS Server 1: 10.1.1.1

DNS Server 2: 10.1.1.1

Admin Username: admin

Admin Password:

License String: 9F5BF81FBABF6CB4BFFFBF09BF00

License Status: Valid License

Serial: 300000000

Centralized Provisioning

New Config Check: ○ Disabled ○ Every Hour ● Every Day ○ Every Week

Config Server IP: 10.1.1.1

Enable MRTG: ○ Yes ● No

Enable Radius: ● Yes ○ No

Radius Server IP: 192.168.0.67

Radius Server Secret: baron

Ignore Radius Results: ○ Yes ● No

Enable DHCP Relay: ● Yes ○ No

DHCP Server IP: 192.168.0.145

Enable PPPoE Relay: ○ Yes ● No

Enable Client Firewall: ○ Yes ● No

Ethernet Interface Management

Ethernet Mode: ● Network ○ Client

Ethernet Max Bandwidth:

Client IP Networks: 192.168.0.128/27

System Configuration	This section allows setup of the basic network parameters of the CellNode M100 device.
Host Name	This is the Name of the CellNode
Domain Name	This is the Domain name of the CellNode
NTP Server	This is the Network Time Server of the CellNode. This server is used to set the clock of the CellNode.
Time Zone	This is the time zone of the CellNode
Operational Region	This is the geographical region of the CellNode. The region is used to setup the radio properties of the device to allow lawful radio transmissions. If the Region is not defined properly the device may start to operate on unlicensed and/or unlawful frequencies. The manufacturer is not responsible for wrong configuration of this property.

DNS Server 1	This is the primary DNS server IP address
DNS Server 2	This is the secondary DNS server IP address.
Admin Username	This is the user name of the administrator used to log into the web interface of the device.
Admin Password	This is the password of the administrator used to log into the web interface of the device.
License String	This is the device license string. The license string is specific for each device and should not be copied to other devices or distributed to unlicensed equipment. Any such distribution is against the policy of the manufacturer and will be legally pursued.
License Status	This is the status of the license.
Serial	This is the serial number of the device
Enable MRTG	This option allows MRTG data to be reported to the central server for data, traffic, network, CPU and other statistical information.
Enable Client Firewall	This option will put a firewall for all clients on the network, to prevent them from accessing the CellNode directly. This make the CellNode transparent on the network and guarantees the device network security.
Radius Services	**Radius services allow Radius authentication of clients.**
Enable Radius	This enables Radius server communication. If enabled the CellNode M100 will send Radius request for every Wireless of LAN client request.
Radius Server IP	This is the IP address of the central Radius server.
Radius Server Secret	This is the shared secret password for the Radius server.
Ignore Radius Results	This option allows the CellNode to send radius requests but ignore the Radius results. This will allow collection of data but not enforcing radius authentication of clients.
DHCP/PPPoE Services	**DHCP services allow DHCP and PPPoE authentication and registration of clients.**
Enable DHCP Relay	This option will allow DHCP requests to pass-thru the CellNode. This is required to allow clients to get IP addresses before they are able to authenticate on the network.
DHCP Server IP	This is the IP address of the DHCP server. This option is required to allow DHCP request to securely pass-thru the device.
Enable PPoE Relay	This option allows PPPoE requests to pass-thru the device. This will allow clients to establish PPoE connection before they are authenticated on the network.
Streaming Services	Streaming services allow streamer and broadcast support on the network.
Enable Streamers	This option will allow the CellNode to support streaming services such as IPTV, VOD, AOD, etc.
Streamer IP List	This is the list of streamer IP addresses. The list is used to allow streaming services on the network. The IP addresses are comma delimited.
Muticast Source IP List	This is the list of Muticast IP addresses. The list is required to allow broadcasts from these IP addresses to pass-thru the CellNode M100 device. The IP addresses are comma delimited.
Centralized Provisioning	This section allows the device to function in a centrally provisioned network infrastructure.
New Config Check	This is the time period between checks for configuration changes. If new configuration is detected, the CellNode M100 will automatically download the encrypted configuration file and configure its parameters. Configuration changes can be submitted dynamically by the central provisioning server or can

	be downloaded manually using the button located in the START/Get Remote Configuration section.
Config Server IP	This is the IP of the central server that supports provisioning services.
Ethernet Interface Management	Ethernet Interface management allows network configuration of the Ethernet interface
Ethernet Mode	This is the operational mode of the Ethernet interface. If the 'Network' mode is selected the device will use this interface to bridge to other CellNode devices or servers on the network. Network mode does not allow high-level of security. In the 'Client' mode is selected the device will connect to clients and will allow clients to connect to it using the Ethernet interface. In this mode high-level of security is supported. Managers should never use bridge mode to interface clients to the network because this will violate the integrity of the whole network.
Ethernet Max Bandwidth	This is the maximum bandwidth that the device will allow to be processed via the Ethernet interface. This option is used to provide traffic shaping services thought the interface. If better traffic shaping/QoS services are required, the customer must purchase a specialized module from the manufacturer.
Client IP Network	This is the network of the clients that will connect to the device. The client network is required to be able to process the function required to authenticate and process clients in 'Client' mode. The network configuration uses the following format: ip_address/netmask (example: 192.168.0.0/24)
Enable Multicast Forwarding	This option allows the device to enable multicast forwarding of packets. This is required in environments that use broadcast based streaming.

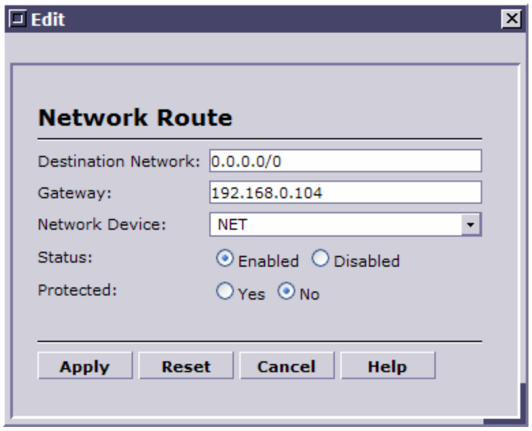
Firewall Filters

Firewall Filters allows advanced firewall configuration for the CellNode M100 device. The device provides firewall services for enhanced network security.

Source IP Network	This is the source network of the packets that need to be filtered. The network configuration uses the following format: ip_address/netmask (example: 192.168.0.0/24)
Source Port	This is the source port of the network packets.
Destination IP Network	This is the destination network of the packets that need to be filtered. The network configuration uses the following format: ip_address/netmask (example: 192.168.0.0/24)
Destination Port	This is the destination port of the network packets.
Action	This specifies the action that the firewall filter will perform on each captured packet.
Protocol	This is the list of packet protocols that will be used for filtering.
Direction	This is the network packet direction.
Protected	This option allows the firewall filter to become write-protected. This will guarantee that the filter will not be deleted or modified if the device is centrally provisioned or if the device retrieves a new configuration file. The protected mode makes the filter permanently present in the configuration.

Network Routes

Network Routes allows route management on the CellNode M100 device. The device supports unlimited number of routes.



Network Route

Destination Network: 0.0.0.0/0

Gateway: 192.168.0.104

Network Device: NET

Status: ● Enabled ○ Disabled

Protected: ○ Yes ● No

Destination Network	This is the destination network for the route. The network configuration uses the following format: ip_address/netmask (example: 192.168.0.0/24).
Gateway	This is the route gateway IP address.
Network Device	This is the route network interface.
Status	This is the route status
Protected	This option allows the route to become write-protected. This will guarantee that the route will not be deleted or modified if the device is centrally provisioned or if the device retrieves a new configuration file. The protected mode makes the route permanently present in the configuration.

Network Configuration

Network Configuration allows IP address management on the CellNode M100 device. The device supports unlimited number of IP addresses.

Local IP Address	This is the IP address that will be assigned to the device interface.
Network Device	This is the network interface that will have the IP address.
NAT	This is the network Address Translation flag. If the device needs to provide NAT services through the selected IP address, this option must be enabled.
VLAN ID	This is the VLAN ID tag for this interface.
Protected	This option allows the IP address to become write-protected. This will guarantee that the IP address will not be deleted or modified if the device is centrally provisioned or if the device retrieves a new configuration file. The protected mode makes the IP addresses permanently present in the configuration.

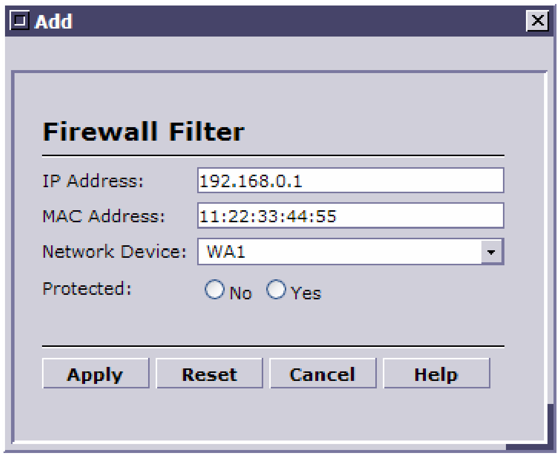
Tunnel Configuration

Tunnel Configuration allows packet tunneling support through WAN and Internet environments. This is very useful in situations where two LAN networks need to be connected via WAN so that this connection becomes transparent to the LAN clients.

Name	This is the name of the network tunnel.
Type	This is the role of the device. In 'Server' mode other clients will connect to this device, in 'Client' mode this device will connect to other tunnel servers. The base rule is that 'Server' mode is enabled on devices that have public IP address and 'Client' mode is enabled on devices that do not have such IP and need to connect to public servers.
Password	This is the Tunnel service password.
Server IP Address	This is the IP address of the Tunnel server that the device will connect to.
Server Port	This is the listening port of the Tunnel service.
Encryption	This option allows tunnel encryption. If the encryption option is enabled the device will have a lower throughput because of resource consumption due to the encryption process.
Inbound Bandwidth	This is the bandwidth limit that is placed on the Inbound tunnel traffic to provide QoS/Traffic Shaping services. The value is in kilo bits per second.
Outbound Bandwidth	This is the bandwidth limit that is placed on the Outbound tunnel traffic to provide QoS/Traffic Shaping services. The value is in kilo bits per second.
Status	This is the Tunnel service status
Protected	This option allows the tunnel service to become write-protected. This will guarantee that the tunnel service will not be deleted or modified if the device is centrally provisioned or if the device retrieves a new configuration file. The protected mode makes the tunnel services permanently present in the configuration.

Static Clients

Static Clients function allow the device to have a static client registrations to allow unauthorized services for selected clients. This function is used to allow static MAC-IP combinations to be assigned to the device to provide special client services. The function is also referred as Static ARP for clients.



Firewall Filter

IP Address: 192.168.0.1

MAC Address: 11:22:33:44:55

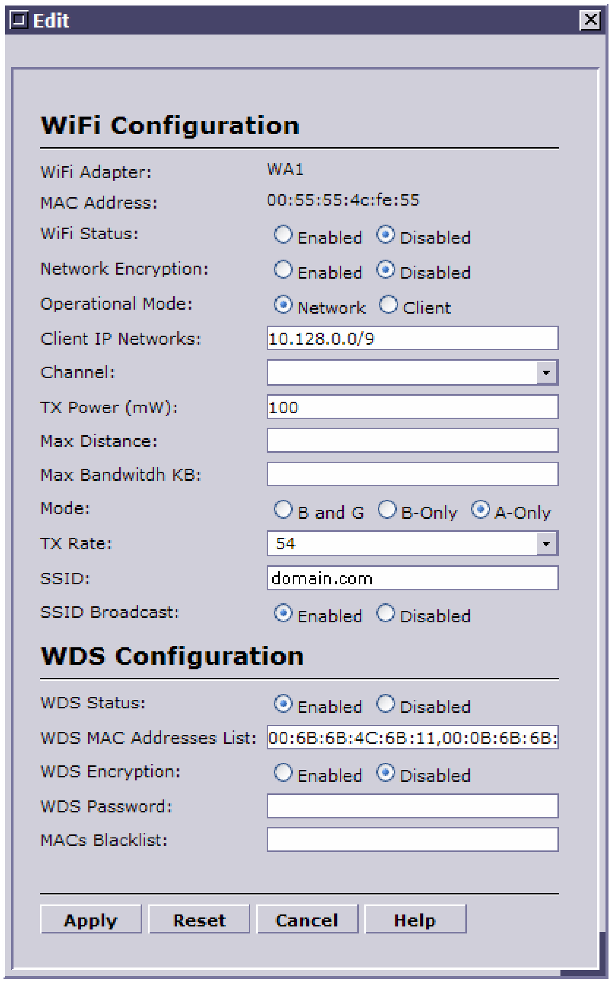
Network Device: WA1

Protected: ○ No ○ Yes

IP Address	This is the IP address of the client.
MAC Address	This is the MAC address of the client that needs to establish static ARP entry.
Network Device	This is the device that is used to store the IP-MAC combination
Protected	This option allows the static client service to become write-protected. This will guarantee that the static client service will not be deleted or modified if the device is centrally provisioned or if the device retrieves a new configuration file. The protected mode makes the static client services permanently present in the configuration.

WiFi Configuration

WiFi Configuration allows advanced setup for Wireless services on both Radio cards supported by the CellNode M100 device.



WiFi Configuration

WiFi Adapter: WA1
MAC Address: 00:55:55:4c:fe:55
WiFi Status: ○ Enabled ● Disabled
Network Encryption: ○ Enabled ● Disabled
Operational Mode: ● Network ○ Client
Client IP Networks: 10.128.0.0/9
Channel:
TX Power (mW): 100
Max Distance:
Max Bandwitdh KB:
Mode: ○ B and G ○ B-Only ● A-Only
TX Rate: 54
SSID: domain.com
SSID Broadcast: ● Enabled ○ Disabled

WDS Configuration

WDS Status: ● Enabled ○ Disabled
WDS MAC Addresses List: 00:6B:6B:4C:6B:11,00:0B:6B:6B:
WDS Encryption: ○ Enabled ● Disabled
WDS Password:
MACs Blacklist:

WiFi Configuration	This section provides basic configuration services for the Wireless interface.
WiFi Adapter	This is the ID of the Wireless Adapter. Available values are: WA1 and WA2
MAC Address	This is the MAC address of the adapter
WiFi Status	This is the status of the Wireless adapter.
Operational Mode	This is the operational mode of the Wireless interface. If the 'Network' mode is selected the device will use this interface to bridge to other CellNode devices or servers on the network. Network mode does not allow high-level of security. In the 'Client' mode is selected the device will connect to clients and will allow clients to connect to it using the Wireless interface. In this mode high-level of security is supported. Managers should never use bridge mode to interface clients to the network because this will violate the integrity of the whole network.
Client IP Networks	This is the network of the clients that will connect to the device. The client network is required to be able to process the function required to authenticate and process clients in 'Client' mode. The network configuration uses the following format: ip_address/netmask (example: 192.168.0.0/24)
Channel	These are the available Radio channels of the Wireless interface. The number of available channels is dependent on

	the Wireless Mode and on the Operational Region.
TX Power	This is the transmission power of the Wireless interface. The upper limit of the Wireless interface is defined by the use but can also be limited by the Operational Region and the Wireless Mode selections.
Max Distance	This is the statistical maximum distance in meters that the Wireless link should cover. The actual distance is limited by various factors such as weather, geographical area, operational region, radio channel, etc. The default value should be set to 5000 meters.
Max Bandwidth	This is the parameter that provides QoS/Traffic Shaping services. The limit is in Kilo Bytes. If more sophisticated QoS services are desire, the operator may purchase an additional QoS module from the manufacturer.
Mode	This is the radio mode of the interface. A - 802.11a 4.9GHZ-5.8GHZ including Super-A G – 802.11g 2.4GHZ including Turbo-G B – 802.11b 2.4GHZ
TX Rate	This is the transmission rate in kilo bits that the device supports. All parameters are theoretical and does not represent the actual data transfer speed because large traffic volumes are used for packet validation and system information. For 108MBps links, the operator must use ‘Auto’ or ‘54MBps’ setting. For B and G modes the operator must use the ‘Auto’ setting ot the TX rate.
SSID	This is the name of the Wireless ESSID/SSID network supported by the interface. Each Wireless interface may support its own SSID network.
SSID Broadcast	This parameter defines the SSID broadcast status. Usually, the SSID is used for interfaces that are operating in Client network mode.
Network Encryption	This parameter enables network encryption for the packets processed with the Wireless interface.
Password	This is the network encryption password. The password should be 13 characters or bytes.
Enable Multicast Forwarding	This option allows the device to enable multicast forwarding of packets. This is required in environments that use broadcast based streaming.
WDS Configuration	This section allows WDS mode configuration. The WDS mode supports the SPT (spanning tree) protocol to allow point-to-multi-point connections. WDS allows multiple CellNode M100 to create network infrastructure backbones.
WDS Status	This is the WDS mode status.
WDS MAC Addresses List	This is the list of MAC addresses of devices that the device must connect to. The MAC addresses are comma delimited. Usually the MAC address list is provided by the central server.
MACs Blacklist	This is the list of Blacklisted MAC addresses. The device will not allow connections from such devices. The MAC address list is comma delimited.

Links Management

Client Link Management – this is the list of the clients that have registered with the device. In order to register the clients must be within the Client IP Network specification of the CellNode interface that they use to connect.

Neighbor Link Management – this is the list of neighbors that are within the WDS link. The list displays the RSSI (signal strength) parameters of the link. Usually, RSSI of 25 or better are required to sustain a stable radio link.