User Manual

RM-20, RM-50, RM-100, RM-200, RM-500,
RM-1000
DT-5, DT-10, DT-20, DT-50

Firmware: 1.11

Introduction

The **SmartShare®** is an integrated **bandwidth manager** and **NAT router** with built-in **DHCP server** and optional **anti terror logger**. The SmartShare can supplement an existing Internet router or replace a traditional NAT router.

Key Features

Bandwidth Manager with User Load Balancing and Dynamic QOS. The patent pending SmartShare bandwidth management technology automatically monitors and manages the Internet connection, so every active user on the local network gets a fair amount of the shared Internet bandwidth, and ensures that the Internet connection always is available for all users on the local network. It also optimizes the use of bandwidth, so the Internet connection can be fully utilized, regardless of the number of active users – if only one user is active, that one user gets all the bandwidth. The Dynamic Quality of Service (Dynamic QOS) technology ensures that IP telephony and online gaming is not affected by other applications.

NAT Router with Individual IP Routing, SPI Firewall and Port Forwarding. The network address translation (NAT) technology makes it possible for multiple PCs to share a single Internet IP address, by translating the individual IP addresses of each PC on the local network to the shared IP address and keeping track of each translation, thereby maintaining the connection from each PC on the local network to the Internet. Combined with individual IP routing, dedicated PCs on the local network can use public IP addresses, thus bypassing the NAT. The stateful packet inspection (SPI) firewall ensures that no PC outside the local network can establish a connection to any PC on the local network, and thus protects the PCs on the local network from intruders coming from the Internet. With port forwarding, specific servers on the local network can be accessed from the Internet, so e.g. a public web server can be set up on the local network.

DHCP Server. The DHCP server technology automatically assigns the required network information to the PCs on the local network. This means that the users do not have to worry about configuring their PCs with the correct IP address, netmask, gateway and DNS servers.

Anti Terror Logger (firmware option). The anti terror logger (ATL) technology collects and records information about Internet traffic flows of individual users as required by EU and Danish legislation.

Developed in Denmark.
Made in Taiwan.

SmartShare Systems
Marielundvej 46 B
DK-2730 Herlev
Denmark
www.smartsharesystems.com

Table of Contents

Installation Guide

1. Connect to the local network equipment

Connect the LAN port on the SmartShare to any Ethernet port on the local network switch, using a straight Ethernet patch cable.

2. Start the setup menu

Use a web browser on a PC connected to the local network to start the setup menu in the SmartShare.
The setup menu address is: **`http://192.168.2.1/`**
The factory default administrator user name is: **`admin`** and password: **`admin`**

3. Configure the Internet connection

Go to the **WAN** page and configure the Internet connection and enter the download and upload speeds in Kbit/s.

The information that must be entered on the WAN page must be obtained from the Internet service provider (ISP). The ISP usually supplies this information in a letter accompanying the confirmation of the Internet subscription.

Please note that the connection speed advertised by most Internet service providers are the gross speeds, while the settings in the SmartShare must be entered as the net speeds, which means that the settings may need some adjustment to compensate for the difference.

Entering the speeds as 80% of the ISP's advertised speeds is a good rule of thumb.

Go to the **Save** page to save and activate the new settings.

4. Connect to the Internet equipment

Connect the WAN port on the SmartShare to the Ethernet LAN port on the Internet modem, using a straight Ethernet patch cable.

5. Test the configured Internet connection speed

Test that the download speed settings are correct by downloading from a very fast server on the Internet from two PCs simultaneously. Go to the **Status** page and check that the Download Limiter status changes from READY to ACTIVE while the download connection is saturated. If it does not change, try decreasing the download speed entered on the **WAN** page by 10-30%. Keep testing and decreasing the values until satisfied.

Test that the upload speed settings are correct by uploading to a very fast server on the Internet from two PCs simultaneously, while monitoring the Upload Limiter status.

The SmartShare Bandwidth Management System

This section describes the SmartShare bandwidth management system in details, and is written for network experts only.

User Load Balancing

Conventional routers simply forward all packets to/from users in the same order the packets arrive at the router, so the users with a lot of packets get a larger share of the available bandwidth than the users with fewer packets.

The SmartShare User Load Balancer intelligently forwards packets to/from individual users in turn, so every user gets a reasonable share of the available bandwidth.

User Identification

The SmartShare identifies individual users by their IP address presented to the LAN interface on the SmartShare. This also means that if a group of users in an apartment shares the apartment's network connection through another NAT router in the apartment, they will be treated as one single user, because that NAT router only presents one IP address to the SmartShare.

The IP address range controlled by the SmartShare is visible on the LAN configuration menu. Each IP address in this range is considered an individual user.

Advanced administrators can use the Bandwidth User Groups to specify which IP address ranges are controlled by the SmartShare. When specifying an address range, you have the option of choosing to identify all IP addresses from a /24 subnet as one user.

Overflow Users

All IP addresses outside the controlled address range are considered overflow users, and will be crammed together and treated as a single virtual user by the SmartShare. This means that the overflow users can access the Internet, but the entire group of overflow users will only get the bandwidth of one single user.

There is no bandwidth distribution within the group of overflow users. A single heavy user in the group of overflow users can consume all the bandwidth assigned to the group of overflow users, and thus block the connection for the other overflow users.

Download and Upload Limiters

The SmartShare monitors the download and upload bandwidth, and while there is bandwidth enough, all users can use all the bandwidth they like.
When the download bandwidth becomes overloaded, the SmartShare starts restricting the heavy users by activating the Download Limiter.
When the upload bandwidth becomes overloaded, the SmartShare starts restricting the heavy users by activating the Upload Limiter.
The SmartShare Download and Upload Limiters are designed to ensure that no single user is limited more than appropriate.

Advanced administrators can use the Bandwidth User Groups to specify maximum download and upload bandwidth per user in each group of users.

Dynamic Quality of Service

The SmartShare always prioritizes timing critical traffic flows, such as IP telephony and online gaming, over ordinary traffic flows.
The priority assignment is based on traffic pattern analysis of each flow. It is not based on the TCP/UDP port number, TOS precedence, DSCP or other fields set in the packet, because those properties can be controlled by peer-to-peer applications or malicious users.

Dynamic QOS is an integral part of the SmartShare bandwidth management system, so it does not require any configuration or allocation of bandwidth.

The SmartShare typically recognizes a timing critical flow and assigns it highest priority within one second.

Flow Management

All NAT routers contain a table, where each flow is registered while established. Each entry in the flow table contains the public IP addresses and TCP/UDP port numbers of the flow and the corresponding IP address and TCP/UDP port number of the computer on the LAN. The same principle applies to the NAT router in the SmartShare.

The SmartShare flow table is large enough to handle the many flows that can be expected when many users are active. In addition to having a very large flow table, the SmartShare Flow Manager is designed to handle excessive flows without crashing or freezing.

Just like the SmartShare Download and Upload Limiters prevent heavy users from eating up all the available Internet bandwidth at the expense of other users, the SmartShare Flow Manager prevents heavy users from eating up all the available flows in the flow table at the expense of other users.

LowLatency Network Overclocking®

As the name suggests, any Network Overclocking® may have unwanted side effects, and should be disabled if it causes problems.

When LowLatency is enabled, the TCP MTU is lowered significantly, and thus the packets become smaller. When the packets are smaller, the packet rate is increased, and thus the delay and jitter is decreased.
Obviously, using smaller packets means that more packets must be used to convey the same amount of data, so it does not increase the effective bandwidth.

Modifying the TCP MTU is known from PPPoE connections, where the MTU is lowered slightly to make room for the PPPoE header added to the packets.

Status menu

This page shows the current status of the Internet connection.

System

This shows system status, such as the name, location and contact information, current time (if an NTP server is available), the duration since the last time the SmartShare was powered on or rebooted, and the memory utilization.

WAN

This shows the status of logical connection to the ISP, regardless of the physical connection's link status.
If the WAN is configured to use a Static IP address, the status will always show the link as being up, because the SmartShare can not know if the ISP will respond to traffic or not.
When the WAN has received its configuration from the ISP, the status will show the link as being up and the assigned IP Address will be visible.
The permanent MAC address of the WAN is visible, because some ISP's ask for the MAC address when they set up their customer's access.

Bandwidth Usage

Download and Upload Rates

The download and upload rates show the current bandwidth utilization in Kbit/s.

Flow Rate

The flow rate shows the number of new flows established per second.

Bytes Downloaded and Uploaded

This shows the total number of bytes transferred in each direction.

Flows Processed

This shows the total number of flows processed, including currently established flows.

Bandwidth Manager

Concurrent Flows

When analyzing the utilization of the Internet connection, it is not only interesting to know the bandwidth utilization, but also how many concurrent flows are established, because each flow uses memory in the SmartShare. Flows are sometimes called sessions or connections. A high number of concurrent flows means that the computers on the local net are connected to many servers on the Internet, but it does not necessarily mean that packets are flowing and bandwidth is being used.

Download Limiter

The SmartShare monitors the download bandwidth, and while there is bandwidth enough, all users can use all the bandwidth they like. In this situation, the Download Limiter status is shown as READY.

When the download bandwidth becomes overloaded, the SmartShare starts restricting the heavy users by activating the Download Limiter. In this situation, the Download Limiter status is shown as ACTIVE.

Upload Limiter

The SmartShare monitors the upload bandwidth, and while there is bandwidth enough, all users can use all the bandwidth they like. In this situation, the Upload Limiter status is shown as READY.
When the upload bandwidth becomes overloaded, the SmartShare starts restricting the heavy users by activating the Upload Limiter. In this situation, the Upload Limiter status is shown as ACTIVE.

Anti Terror Logger

Log Servers

This shows the overall status of the FTP servers where the SmartShare stores the ATL log files. The status can be: Initializing, OK, Warning or Error.

SNMP Agents

This shows the overall status of the SNMP agents in the switches and routers on the local network. The status can be: Initializing, OK or Error.

Buffer Usage

The SmartShare temporarily stores the ATL log files in a buffer until they are transferred to the FTP server. Buffer Usage shows the utilization of this buffer.

Flows Logged

Shows how many flows have been logged by the SmartShare since the last time the SmartShare was powered on or rebooted.

Internet/WAN (Wide Area Network) configuration menu

The Internet service provider usually supplies all the information that is needed to set the WAN configuration in a letter accompanying the confirmation of the Internet subscription.

Internet Service Provider connection type

The WAN can be configured for 3 types of connection to the Internet service provider:

- Static IP
- DHCP
- PPPoE

WAN with Static IP

The following information is required:

- IP address
- Netmask
- Router (Default Gateway)
- Primary DNS Server

The following information is optional:

- Secondary DNS Server

WAN with DHCP

This type of connection is fully automatic. If the Internet service provider (ISP) requires a device name in the DHCP request, it can be configured here.

WAN with PPPoE

The following information is required:

- PPPoE username
- PPPoE password

Connection Speed

The Internet connection speed must be set correctly, or the bandwidth distribution will not function as intended.

The following information is required:

- Download speed in Kbit/s
- Upload speed in Kbit/s

If the connection speed advertised by the Internet service provider (ISP) contains two numbers, for example 1024/256; the download speed is normally the larger of the numbers and the upload speed is the lesser.
Please note that an advertised speed of 1M sometimes means 1024 and 2M sometimes means 2048, but 10M typically means 10000 and 100M always means 100000.

Many ISPs advertise the gross connection speed, which does not include overhead in the ISP's network (e.g. PPPoE encapsulation and ATM cell alignment). The speed settings in the SmartShare must be entered as net values. This means that they may need some adjustment to compensate for the overhead in ISP's network. Entering the speeds as 80% of the ISP's advertised speeds is a good rule of thumb.

External Servers (optional)

NTP Server

If the system time must be synchronized with an external NTP server, its host name or IP address can be set.

The default configuration is: (empty)

LAN (Local Area Network) configuration menu

Network Setup

The router name must be set. Optionally a domain name can be configured. This information is used by the built-in DHCP server (if enabled) to configure clients on the LAN using DHCP for automatic IP configuration.

The default router name is: router
The default domain name is: local

IP Address Range

The IP address range must be set. This information is used to distribute the bandwidth among the active users and by the built-in DHCP server (if enabled) to configure clients on the LAN using DHCP for automatic IP configuration.

The default IP address range is: 192.168.2.1-192.168.2.255

Local DNS Servers (optional)

If there are any DNS servers on the LAN, their IP addresses can be set. This information (in addition to the DNS server information from the WAN) is used by the built-in DHCP server (if enabled) to configure clients on the LAN using DHCP for automatic IP configuration.

The default configuration is: (empty)

Local NTP Server (optional)

If there is an NTP server on the LAN, its IP address can be set. This information is used by the built-in DHCP server (if enabled) to configure clients on the LAN using DHCP for automatic IP configuration.

The default configuration is: (empty)

Built-in DHCP Server

If enabled, the built-in DHCP server automatically configures clients on the LAN using DHCP for automatic IP configuration.

The default configuration is: Enabled

NAPT (Network Address and Port Translation) configuration menu

Port Forwarding to Local Servers

These fields can be configured to make servers on the local network available from the Internet.

If the port number of a local network device can not be configured on the device, e.g. port 80 on a web-managed switch, the port numbers can be remapped by NAPT.

The default configuration is: (empty)

All Ports Forwarding to Local Servers

These fields can be configured to make servers on the local network available from the Internet by mapping their LAN address to a public IP address on the Internet.

The default configuration is: (empty)

ATL (Anti Terror Logger) configuration menu

Log File Storage

The SmartShare stores the ATL log files on an external FTP server.

If ATL is enabled, it is possible to configure up to two FTP servers for storing the ATL log files. When the SmartShare is ready to store an ATL log file, it will use the primary FTP server. Every time the primary FTP server fails to receive an ATL log file, the SmartShare will store it on the secondary FTP server instead.

FTP Server, User Name and Password are required fields, Directory Path is optional. The Status field shows the result of the last FTP transfer.

Local Network SNMP Agents

The SmartShare uses the SNMP agents in the switches and routers on the local network to locate where each MAC address and IP address is connected, and thus identifies the users.

If ATL is enabled, it is possible to configure which SNMP agents are present on the local network. Information about each switch and router on the LAN should be set, so the SmartShare is able to poll them for the required information to identify the users.

IP Address and Community are required fields. The Status field shows the result of the last SNMP poll of the device.

Advanced configuration menu

Remote Management

The built-in web based setup menu can be changed to a different port.
The built-in SNMP agent can be changed to a different port.

The default web management port is: 80
The default SNMP agent port is: 161

Router Mode

If you want to use the SmartShare as a traditional IP router without the NAT, select IP Routing.

The default router mode is: NAT Routing

Network Features

VoIP Extra Priority

Enabling VoIP Extra Priority has the following effects:

- VoIP will always have highest priority, even if it takes excessive bandwidth from the other users.

The default setting for VoIP Extra Priority is: Disabled

LowLatency Network Overclocking

Enabling LowLatency Network Overclocking has the following effects:

- The “ping time” in online games is lowered.
- The delay and jitter for IP telephony is minimized.

LowLatency Network Overclocking works by reducing the TCP MTU significantly, and may not be compatible with all web sites and Internet services. If it causes problems, it can be disabled again.

The default setting for LowLatency Network Overclocking is: Disabled

DHCP Proxy

If a DHCP server is not connected to the layer 2 LAN, and the built-in DHCP server is disabled, the DHCP proxy can be used to relay DHCP requests from DHCP clients on the LAN to remote DHCP servers via layer 3.

The default configuration is: Disabled

Built-in DHCP Server Options

If the built-in DHCP server is used its default and maximum DHCP lease time can be changed from their default values.

The default configuration is: 720 minutes and 1440 minutes.

Outgoing SMTP Connections

The SmartShare has 4 different modes for handling outgoing SMTP (TCP port 25) connections from the local network to the WAN:

- Allow All.
- Allow to External Server only.
- Redirect all to External Server.
- Allow from Local Mail Servers only.

The default configuration is: Allow All

Allow All

Allow all local users to connect to any SMTP server on the WAN.

Allow to External Server only

Allow all local users to connect to the specified SMTP server on the WAN only. Attempts to connect to other SMTP servers on the WAN will be rejected by the SmartShare.

Redirect all to External Server

Redirect all outgoing SMTP connections to the specified SMTP server on the WAN. In this mode, the packet headers of all outgoing SMTP connections are modified, so the connection is established to the specified SMTP server instead.

This mode is useful if the local users are only allowed to use a specific SMTP server, but are unable or unwilling to configure their email applications.

Allow from Local Mail Servers only

Allow the specified local mail servers to connect to any SMTP server on the WAN, and reject attempts from all other local users to connect to SMTP servers on the WAN.

System Information

System contact and location can be configured. This is not used by the system itself. It is shown on the status web page and available via SNMP.

Bandwidth User Groups

Bandwidth User Groups can be used to configure which IP address ranges the bandwidth manager controls, and optionally set per-user bandwidth limits within each user group.

The following can be configured for each user group:

- First and last IP address.
- User type. Choose "IP Address" for normal user identification, where each IP address identifies one user. Choose "/24 Subnet" if you want all IP addresses within a /24 subnet to be identified as one single user. This can be used in routed networks, where each apartment (or office) is assigned a /24 subnet.
- Download and Upload bandwidth per user (optional). This can be used to set the per-user maximum bandwidth allowed for users in the user group. If left blank, there will be no specific bandwidth limits; the users will participate normally in the smart management of all the available bandwidth.
- Description. This can be used to store an informative description of the user group.

The default configuration is: Disabled

Additional LAN Subnets

Routes in addition to the LAN subnet can be added here. Each route added can be a NAT or a transparent route.

In a switched network with NAT to the LAN, some users on the LAN can have public IP addresses by adding them to this table as follows: Set Subnet to the user's public IP address, set Subnet Mask to 255.255.255.255, leave Next Hop Gateway empty and select IP Routing.

On the user's PC, set the IP address to the public IP address and the Subnet Mask to 255.255.255.255 (or 255.255.255.252 if 255.255.255.255 is not accepted) and Default Gateway to the IP address of the SmartShare, as shown on the LAN configuration menu (e.g. 192.168.2.1).

Remember to configure the Bandwidth Distributor with the added public IP addresses.

The default configuration is: Disabled

User Groups Denied Access to WAN

Local users in the defined address ranges are denied access to the WAN. Attempts to connect to the WAN will be rejected by the SmartShare.

The default configuration is: (empty)

System menu

Download Firmware

The SmartShare firmware can be upgraded from the firmware server at SmartShare Systems or any other firmware server. Firmware upgrade is a two step process. First, enter the URL of the firmware to be downloaded, and click the Download Firmware button. Second, when the firmware has been downloaded, checked for validity and is ready for installation, you can choose to cancel the upgrade or to proceed with the installation of the downloaded firmware.

Install License Key

Features of the SmartShare can be changed by installing different license keys. Enter the new license key and click the Install New License button. After the license key has been validated the SmartShare must be rebooted to activate the new feature set.

Trial Mode

If a trial license is installed, the SmartShare can operate in a trial mode where the model type and optional features can be changed. This can be used for demo or test purposes.

An ongoing trial can be stopped at any time, and the SmartShare will revert to normal operation.

As long as there is trial time remaining, new trials can be started.

When the trial expires, the SmartShare will reboot and revert to normal operation. The available trial time is controlled by the installed license, and additional trial time can be installed with additional licenses.

Restore Factory Defaults

Press this button if you wish to restore the factory default configuration.

Reboot System

Press this button if you wish to reboot the SmartShare. Rebooting the system does not clear the configuration.

Managers configuration menu

Multiple users can manage and configure the SmartShare.

The following can be configured for each manager:

- User Name (required).
- Password. Password for access to the web management interface.
- Community. SNMP Community for access to the SNMP agent. If not set, access to the SNMP agent will not be allowed.
- First and last IP address (optional). If set, the manager is only allowed management access if he connects from a PC within the specified IP address range.
- Manager Level. This determines how much the manager has access to do.

The following Manager Levels are available:

- Blocked. No access.
- User. Access to the Status page only.
- Installer. Full access.

The factory default administrator user name is: **admin** and password: **admin**
The factory default community is: (empty)

Logout menu

Log out and return to the login page.

Using the Serial Port

The serial port can be used with any terminal emulator, such as Hyperterm or Tera Term Pro, as a fallback solution if the LAN connection has been lost.
The speed is: 115200 8N1 (115200 baud, 8 bits, No parity, 1 stop bit).

The following commands are available:

- ? – Show help.
- info – Show configuration information.
- reboot – Reboot the SmartShare.
- restore – Restore configuration to factory default.
- license – Show hardware MAC and license ID.
- license=xxxxx – Install new license key.
- password bypass – Enable factory default administrator user name: **admin** and password: **admin** for 5 minutes.

The serial port is not password protected.

Security Considerations

Physical Access

The SmartShare should be installed in a locked patch panel. Anyone with physical access to the SmartShare can power it off, disconnect it or change the configuration via the Serial port.

Password Protection

The SmartShare configuration menu is password protected. Keep your password safe.

Firewall

The SmartShare firewall prevents potential intruders on the Internet from accessing computers on the local network.
The firewall does not prevent users on the local network from downloading virus or other malware from the Internet to their computers. Users on the local network should protect their computers with anti-virus software.
The firewall does not prevent intruders connected on the local network from accessing other computers on the local network. Switches and wireless access points in the local network should prevent intruders and other users on the local network from accessing each other's computers. For further information, please refer to the chapter about protecting local users from each other.

Protecting Local Users from Each Other

When installing and configuring the local network infrastructure, i.e. switches and wireless access points, it should be considered if the local network should be open (where all local users can connect to each other and share files etc.) or protected (where all local users are separated from each other, and each user only has access to the Internet and local servers).
User separation has different names, depending on equipment and vendor. In switches, look for "source-port filters" (HP ProCurve terminology), "Private VLANs" (Cisco terminology) or similar. In wireless access points, look for "AP isolation", "client isolation" or similar.
User separation does not affect the SmartShare, and the SmartShare works equally well with both open and protected networks.

Troubleshooting and FAQ

Q: After the SmartShare was installed, some of the computers on the local network can no longer access the Internet.
A: This is probably because the computers still have the old configuration from the previous Internet router. In Microsoft Windows, start a Command Prompt (Start -> Run; cmd.exe), and run the command **`ipconfig /release`** and then run the command **`ipconfig /renew`**.

Q: There is no connectivity from the LAN to the WAN after the LAN has been configured on the SmartShare.
A: The LAN can not use the same IP address range as the WAN. Verify that the configuration doesn't conflict.

Q: After powering on the SmartShare, the WAN connection to the ISP is not established.
A: First, verify that everything is correctly connected. It may take a few minutes for the WAN connection to the ISP to stabilize; if it isn't established after a few minutes, verify that the configuration in the WAN menu is correct. If it still doesn't work, disconnect the SmartShare and use a laptop to verify that the connection from the ISP works.

Q: Users with peer-to-peer applications have problems accessing the Internet.
A: Configure the peer-to-peer application to use fewer simultaneous flows (a.k.a. connections or sessions).

Q: The administrator password for the SmartShare is lost.
A: Use the Serial port to enable the default username and password for 5 minutes, then login via the web and set a new password. Refer to "Using the Serial Port".

Q: The SmartShare can not be accessed any more.
A: Use the Serial port to restore the factory default settings. Refer to "Using the Serial Port".

Q: Some of the computers on the local network can not access the Internet.
A: If a device with a DHCP server is wrongly connected to the LAN, the computers on the LAN may get an incorrect configuration from the unauthorized DHCP server. Most routers and wireless access points have a DHCP server on their LAN ports. Run the command **`ipconfig`** on a computer having access problems. If it shows an IP address outside the range configured in the SmartShare built-in DHCP server, a device with a DHCP server is wrongly connected to the LAN. Locate the device and disconnect it from the LAN.

Q: A user needs a public IP address, but the SmartShare is in NAT Routing mode.
A: Public IP addresses can be added using the "Additional LAN Subnets" feature.

Q: The SmartShare has blocked access for a peer-to-peer user.
A: The SmartShare does not block access for peer-to-peer users. However, the peer-to-peer user may have exceeded the number of allowed concurrent flows accepted by the SmartShare Flow Manager, and it has determined to start limiting the number of flows for this user, in order to protect the other users. Ask the peer-to-peer user to wait for three hours until the flows have been released.

Power Consumption

	DT models	RM models
Typical	12 Watt	24 Watt
Maximum	15 Watt	35 Watt
Typical annual power consumption	105 kWh	210 kWh

The consumption at the primary side of the power supply, i.e. at the 110-240V plug, is shown in the table above. The annual cost of electricity for the SmartShare can be estimated by multiplying the price of electricity (per kWh) with the typical annual power consumption of the installed SmartShare model.

LED Indicators

The two LEDs for each **LAN**/**WAN**/**Ext1**/**Ext2** Ethernet port indicate as follows:

LINK/ACT = Off	No connection.
LINK/ACT = On, 10/100 = Off	10Mbit link to other device established.
LINK/ACT = On, 10/100 = On	100Mbit link to other device established.
LINK/ACT = Blink	Link is active with transmissions.

The **POWER** LED indicates as follows:

POWER = Off	Power is off.
POWER = Orange Light	Power is on.

The **STATUS** LED indicates as follows:

STATUS = Green Light	The SmartShare is booting.
STATUS = Green Blink Slow	Data connection to ISP is established. Download Limiter is ready.
STATUS = Green Blink Fast	Data connection to ISP is established. Download Limiter is active.
STATUS = Red Blink Slow	Connection to ISP is down or not established yet.
STATUS = Red Blink Fast	(Not used.)
STATUS = Red Light	Internal System Error.
STATUS = Red and Green	Internal System Error.

Glossary

ATL	Anti Terror Logger (or Anti Terror Logging)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	Differentiated Services Code Point
FTP	File Transfer Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LED	Light Emitting Diode
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAPT	Network Address and Port Translation
NTP	Network Time Protocol
QOS	Quality Of Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPI	Stateful Packet Inspection
TOS	Type Of Service
WAN	Wide Area Network