SHDTU-is

G.SHDSL.bis Ethernetmodem

Software-Handbuch

AddSecure GmbH
Breite Straße 10
D-40670 Meerbusch
Telefon: +49 (0)2159/ 693 75-0
Fax: +49 (0)2159/ 922 430 0
E-Mail: info.digicomm@addsecure.com

Dokument Revision: 21-01

Weitere Informationen zu unseren Produkten finden Sie unter www.addsecure.de.

Rechtliche Informationen

Die Inhalte dieses Dokuments werden ohne Gewähr zur Verfügung gestellt. Sofern nicht gesetzlich vorgeschrieben werden keinerlei Garantien, weder ausdrücklich noch impliziert, insbesondere keine stillschweigende Garantie der Marktgängigkeit oder Eignung für einen bestimmten Zweck gewährt im Hinblick auf die Genauigkeit und Zuverlässigkeit oder die Inhalte dieses Dokuments. Die AddSecure GmbH behält sich das Recht vor, dieses Dokument jederzeit und ohne vorherige Ankündigung zu überarbeiten oder zurückzuziehen.
Die AddSecure GmbH haftet keinesfalls für eventuelle Datenverluste bzw. entgangene Einnahmen oder jedwede spezielle, zufällige und Folgeschäden sowie für indirekte Schäden unabhängig von deren Ursache.

Weitere Informationen über die AddSecure GmbH finden Sie auf folgender Website:
https://www.addsecure.de

Inhalt

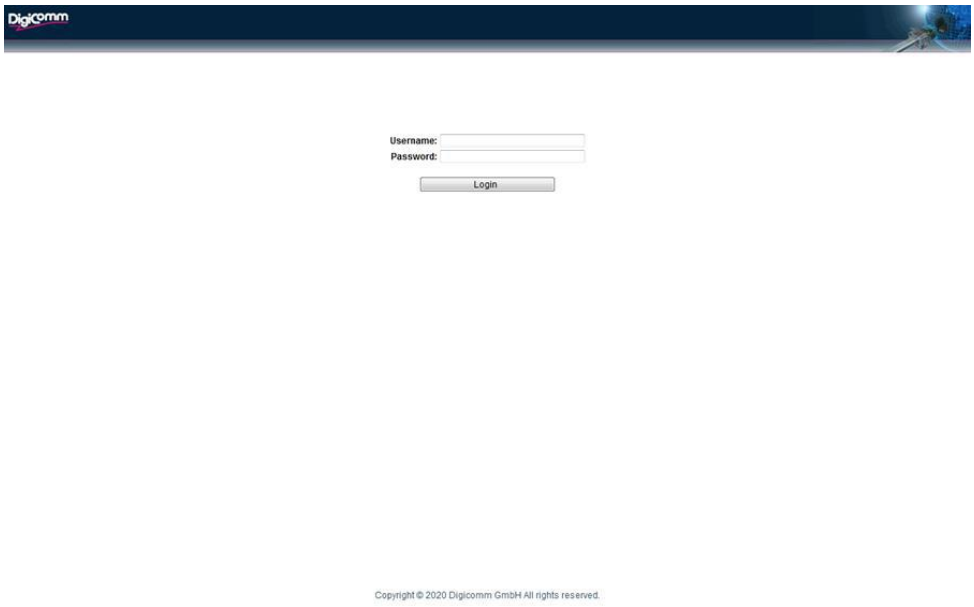
Bitte beachten Sie: Dies ist ein Handbuch für die SHDTU-Serie.
Bitte prüfen Sie, welches Modell Sie verwenden ggf. können Screenshots oder Einstellungen abweichen.

1. Login/ Home

1.1 Login

Geben Sie in Ihrem Web-Browser die IP des SHDTU's ein um zur Anmeldeseite zu gelangen.
Standardmäßig erreichen Sie die SHDTU's über folgende IP-Adressen:

192.168.0.1 Master
192.168.0.2 Slave

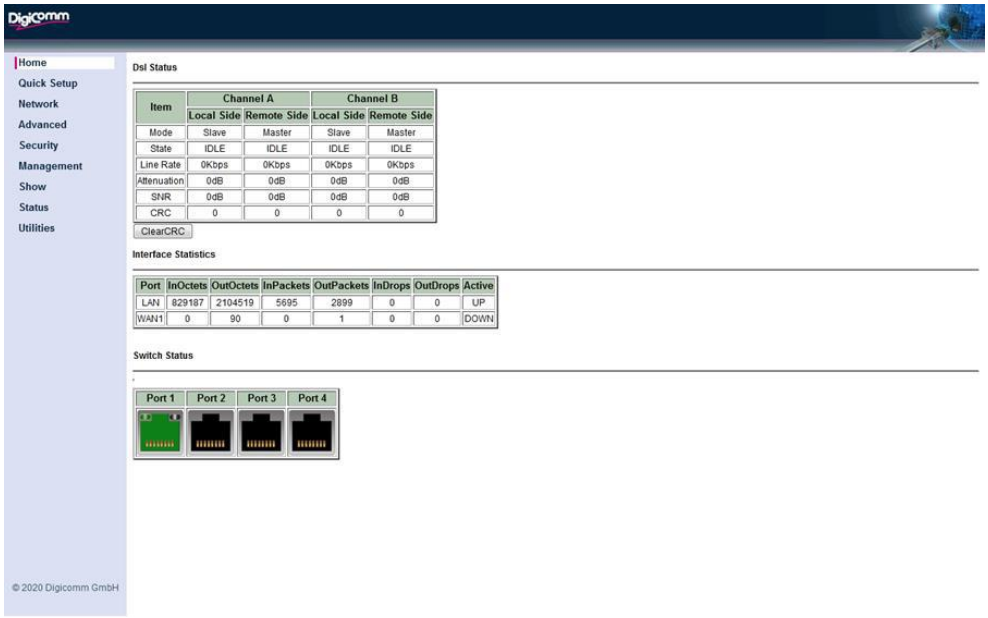


Standard Passwort

Username: root
Passwort: root

Hinweis: Wir empfehlen das Standard Passwort abzuändern.

1.2 Home



Im Home Menü finden Sie alle konfigurierbaren Optionen und das Statusmenü.

SHDSL Status

Mode:	Zeigt die Konfiguration des Gerätes auf der SHDSL-Seite an (Master oder Slave).
State:	Zeigt die aktuelle synchronisierte Datenübertragungsrate über SHDSL an.
Line Rate:	Zeigt die aktuelle synchronisierte SHDSL-Leitungsrate an.
Attenuation:	Zeigt die aktuelle Dämpfung auf der SHDSL-Seite an. Dieser Wert darf 30 dB nicht übersteigen. Optimal ist ein möglichst niedriger Wert.
SNR:	Zeigt das aktuelle Signal-Rausch-Verhältnis der Leitungen an. Optimal ist ein möglichst hoher Wert. Ein Wert unter 5 dB weist auf eine möglicherweise instabile Übertragung hin.
CRC:	Fehlerzähler für verworfene Datenpakete.

Interface Statistics

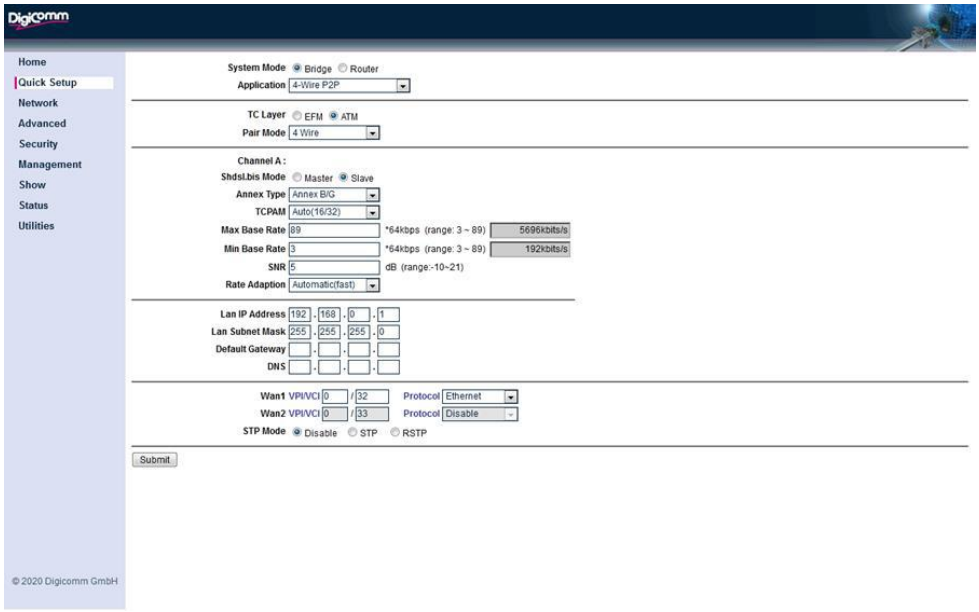
Port:	Deklaration der Schnittstelle - LAN oder WAN.
InOctets:	Zähler für empfangene Bytes/ Oktetts.
OutOctets:	Zähler für gesendete Bytes/ Oktetts.
InPackets:	Zähler für eingehende Datenpakete.
OutPackets:	Zähler für ausgehende Datenpakete.
InDrops:	Zähler für eingehende, verworfene Datenpakete.
OutDrops:	Zähler für ausgehende, verworfene Datenpakete.
Active:	Zeigt an, ob die Schnittstelle verbunden ist (UP oder DOWN)

Switch Status

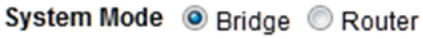
Port 1 bis 4:	Zeigt an, zu welchen Ports auf der LAN-Seite eine Verbindung aufgebaut wurde. GRÜN = verbunden / SCHWARZ = nicht verbunden/ GRAU= abgeschaltet.

2. Quick Setup

Die Funktion „Quick Setup“ (Schnellinstallation) leitet Sie Schritt für Schritt durch die Einrichtung des SHDTUs. Dieses SHDTU lässt sich als Bridge oder als Router konfigurieren. In den folgenden Abschnitten wird die Einrichtung als Bridge oder Router erläutert.



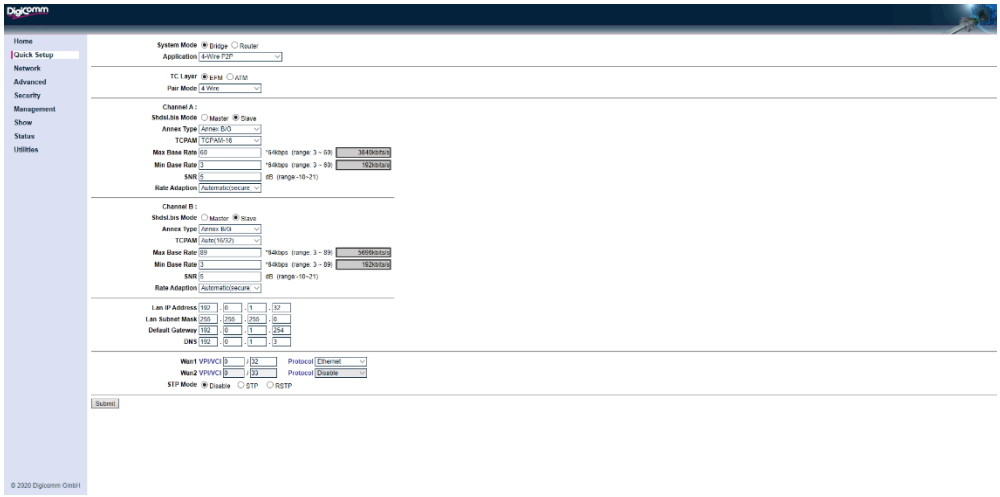
2.1 System Mode



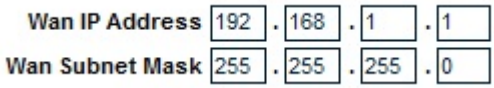
Im Abschnitt „System Mode“ (Systemmodus) legen Sie fest, ob dieses SHDTU als Bridge oder als Router verwendet werden soll.

Im „Bridge-Modus“ hingegen kann auch ein externes Gerät, beispielsweise Ihr Computer oder ein separater Router die Verbindung zum Netzwerk herstellen. Das SHDTU hat dabei lediglich die Aufgabe, sich Ihre Einstellungen für VCI, VPI und Kapselung zu merken. Die ISP-Daten sowie die zugewiesene IP-Adresse werden über Ihren separaten Router oder Ihren Computer im PPP-Modus gesteuert.

Im „Router-Modus“ führt das SHDSL-Modem alle Funktionen aus, die eine Verbindung mit einem anderen Netzwerk ermöglichen: darunter sämtliche technische Einstellungen (VCI, Kapselung, usw.) und darüber hinaus die Verbindung des SHDTU in das Netzwerk mithilfe Ihres Benutzernamens und Passwortes.



Wenn Sie als System Mode die Option „Router“ auswählen, werden weitere Einstellungsmöglichkeiten angezeigt (siehe Screenshot oben).



Geben Sie bei der Verwendung im Router-Modus die WAN-Port-Informationen für das SHDTU ein.

2.2 SHDSL.bis Mode

Es gibt zwei SHDSL.bis-Modi: Master und Slave. Klicken Sie auf „Master“ oder „Slave“, um den Betriebsmodus einzustellen.

Die Master/ Slave Einstellung kann pro WAN konfiguriert werden.

2.3 TC Layer

Wählen Sie zwischen den Übertragungsschichten ATM oder EFM aus.

Wir empfehlen EFM auszuwählen, da Sie hier einen höheren TC-PAM Wert auswählen können und eine einfachere Konfiguration durchführen können.

2.4 Pair mode

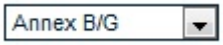
Über die Einstellung „Pair Mode“ können Sie festlegen, wie viele Drähte für eine SHDSL.bis-Verbindung verwendet werden sollen.

SHDTU- 06-is / 05-is	(2-Draht-Betrieb) ermöglicht nur die Auswahl von zwei Drähten.
SHDTU-09-is SHDTU-08-is SHDTU-08-is-SFP	(4-Draht-Betrieb) ermöglicht die Auswahl von 2 oder 4 Drähten.
SHDTU- 10-is	(8-Draht-Betrieb) ermöglicht die Auswahl von 2, 4 oder 8 Drähten.

Folgende Modi stehen zur Verfügung:

2-Wire (2-Draht):	In diesem Modus ist nur ein SHDSL-Paar aktiv.
4-Wire (4-Draht):	EFM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit und eine Redundanz zu erzielen. ATM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit zu erzielen. Falls eines der beiden Paare ausfällt, führt dies auch zum Ausfall des anderen Paares.
8-Wire (8-Draht):	EFM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit und eine Redundanz zu erzielen. ATM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit zu erzielen. Falls eines der beiden Paare ausfällt, führt dies auch zum Ausfall des anderen Paares.
Auto-Fall-Back:	(Automatisches Fallback) Nur für den ATM-Modus verfügbar. In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit und Redundanz zu erzielen.
Multi-Link:	Jede SHDSL-Leitung fungiert als unabhängiges 2-Draht-Paar. Wird für die gleichzeitige Verbindung zu zwei Remote-Geräten mit 2-Draht-Betrieb verwendet.

2.5 Annex Type

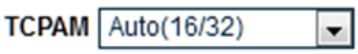


Es gibt verschiedene Annex Typen aus denen Sie auswählen können:

Annex A, Annex B, Annex A/F oder Annex B/G.

Standardmäßig ist Annex B/G ausgewählt.

2.6 TC-PAM



Standardmäßig ist TCPAM extended ausgewählt. Diese Funktion steht nur im EFM-Modus zur Verfügung.

Für die Funktion „TC-PAM“ stehen verschiedene Optionen zur Auswahl:
„Auto“, „TC-PAM-16“, „TC-PAM-32“, „TC-PAM-4“, „TC-PAM-8“, „TC-PAM-64“, „TC-PAM-128“ und TC-PAM-Extend.

Bei Auswahl der Option „Auto“ legt das System für die Funktion „TC-PAM“ automatisch einen Wert zwischen 16 und 32 fest. Diese Option steht nur zur Verfügung, wenn es sich beim Annex-Typ um „Annex A/F“ oder „Annex B/G“ handelt.

Wenn sich der TC-PAM Layer im ATM Modus befindet:

SHDSL.bis SHDTU (VPN Router)	Annex A	Annex B	Annex A/F	Annex B/G	Master	Slave
Auto			●	●	●	●
TCPAM-16	●	●	●	●	●	●
TCPAM-32			●	●	●	●
TCPAM-4						
TCPAM-8						
TCPAM-64						
TCPAM-128						
TCPAM-Extend						

Bitte beachten Sie: TC-PAM 4/8/64/128/ Extend wird im ATM-Modus nicht unterstützt.

Wenn sich der TC-PAM Layer im EFM Modus befindet:

SHDSL.bis SHDTU (VPN Router)	Annex A	Annex B	Annex A/F	Annex B/G	Master	Slave
Auto			●	●	●	●
TCPAM-16			●	●	●	●
TCPAM-32			●	●	●	●
TCPAM-4			●	●	●	
TCPAM-8			●	●	●	
TCPAM-64			●	●	●	
TCPAM-128			●	●	●	
TCPAM-Extend						●

2.7 Max / Min Base Rate

Max Base Rate : Maximale SHDSL Datenrate
Min Base Rate: Minimale SHDSL Datenrate

2.8 SNR

Über den Menüpunkt SNR können Sie den Mindest -SNR-Wert einstellen.

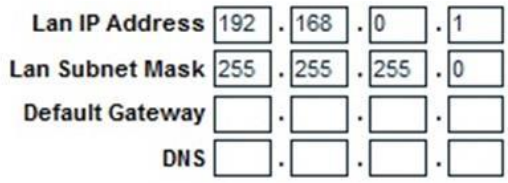
2.9 Rate Adaption

Standardmäßig ist Secure ausgewählt.

Zur Anpassung der Datenrate stehen folgende Optionen zur Verfügung:

- Fixed (feste Datenrate)
- Automatic (fast) – Das Gerät versucht sich mit max. Geschwindigkeit zu synchronisieren.
- Automatic (secure) – Das Gerät achtet bei der Synchronisierung auf maximale Stabilität der Leitung.

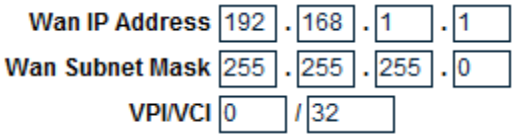
2.10 LAN



LAN IP Address: Geben Sie hier die IP Adresse ein, die dem Gerät zugeordnet werden soll.
LAN Subnet Mask: Geben Sie hier die Subnet Maske ein.
Default Gateway: Geben Sie hier das Default Gateway ein.
DNS: Geben Sie hier den DNS-Bereich ein.

2.11 WAN

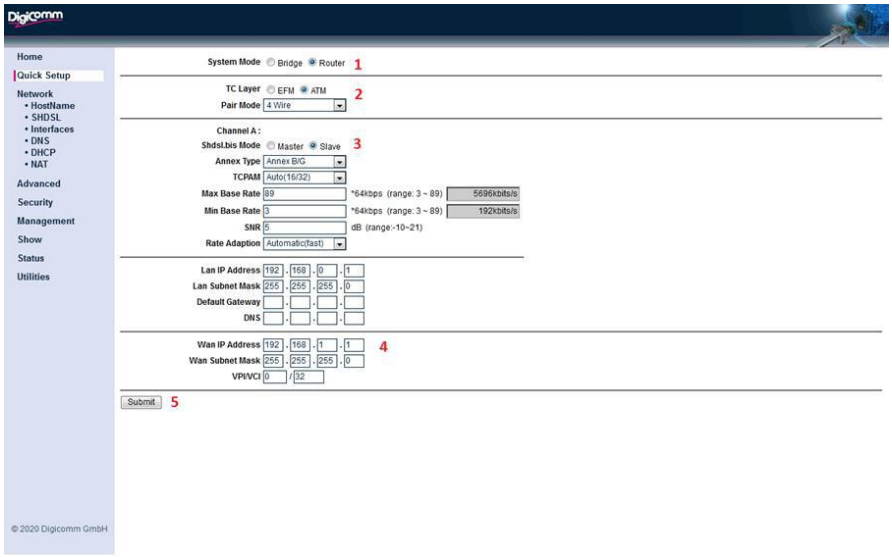
Nur im Router Modus einstellbar



WAN IP Address: Geben Sie hier die IP Adresse des WAN 1 Netzwerkes ein.
WAN Subnet Mask: Geben Sie hier die Subnet Maske des WAN 1 Netzwerkes ein.
VPI/VCI: WAN 1 VPI/ VC im ATM-Modul

2.12 Beispiel für ein „Quick Setup“

Konfigurieren Sie das Gerät im Router Modus /ATM und als Slave.



Schritt	Einstellung	Menüpunkt
1	Wählen Sie bei „System Mode“ „Router“ aus	○ Bridge ◉ Router
2	Wählen Sie beim „TC-Layer“ „ATM“ aus Wählen Sie beim „Pair Mode“ 4-Draht (4 Wire) aus	○ EFM ◉ ATM 4 Wire
3	Wählen Sie beim „SHDSL.bis Mode“ Slave aus	○ Master ◉ Slave
4	Geben Sie die LAN und WAN IP-Adressen und Subnet Masken ein	
5	Klicken Sie auf den “Submit” Button. Sie werden zu einer Übersichtsseite weitergeleitet. Klicken Sie dann auf den Button „Apply“, um die Einstellungen zu speichern.	Submit Apply

3 Network

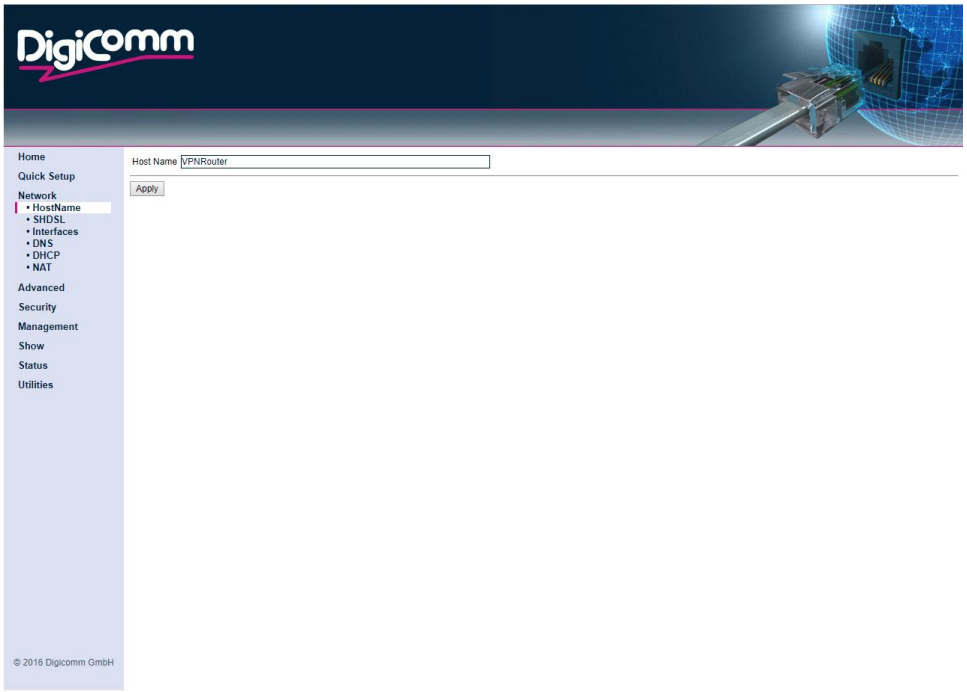
Im Abschnitt „Network“ (Netzwerk) lassen sich folgende Funktionen festlegen:

1. Hostname
2. SHDSL
3. Interfaces (Schnittstellen)
4. DNS
5. DHCP
6. NAT

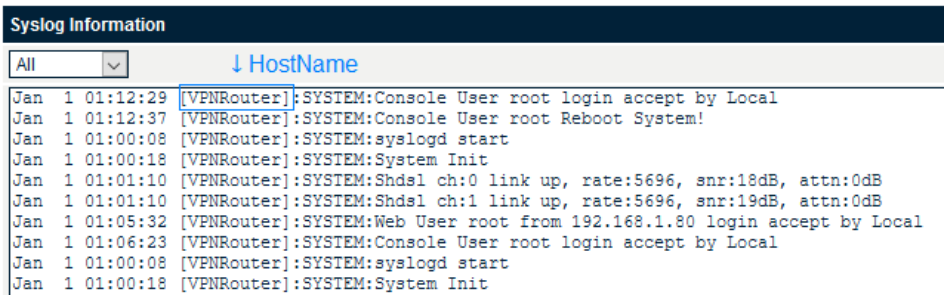
3.1 HostName

Host Name: Hier können Sie einen Host Namen vergeben.
Der Standard Name lautet „VPNRouter“.

Geben Sie den Hostnamen des Routers ein und klicken Sie auf „Apply“, um die Änderungen zu übernehmen.



Der HostName wird im Syslog wie folgt angezeigt:

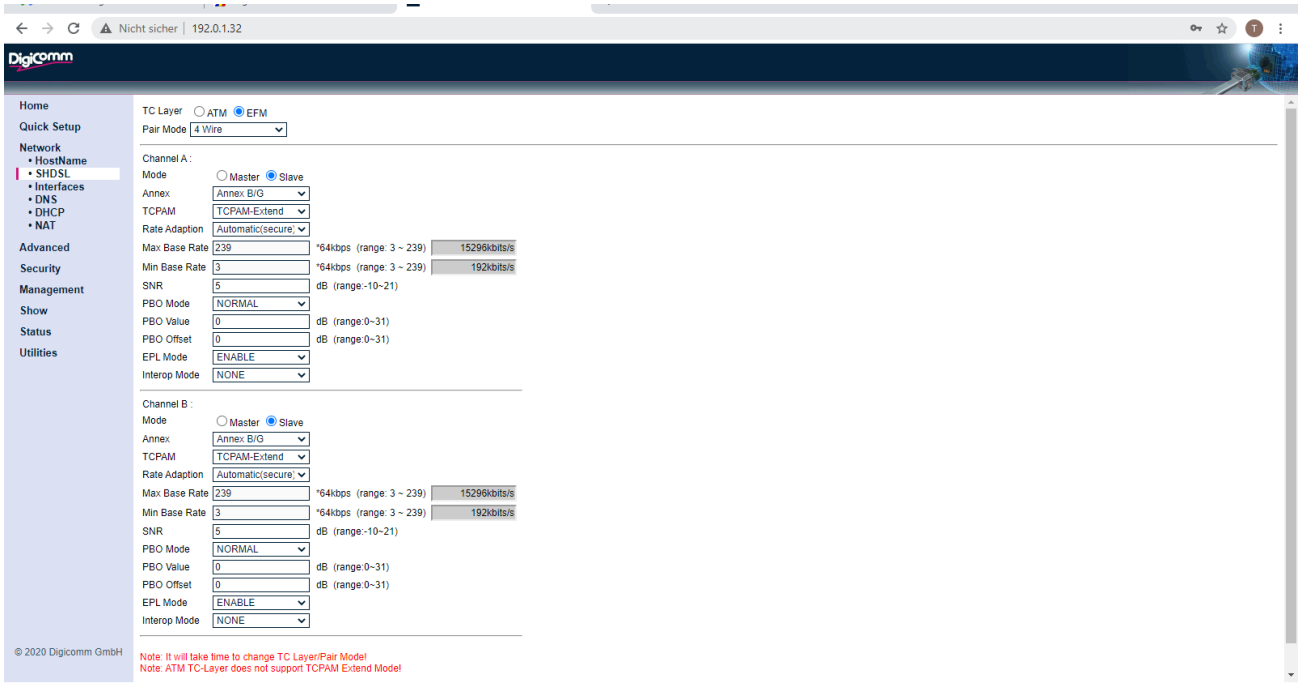


Der Host Name wird in der CLI Eingabeaufforderung wie folgt ausgewiesen: („HostName“#)

```
G.SHDSL.Bis-4W, Chip:PEF22628V1.2, PHY-FW:1.1-1.9.0__001_eLP, IDC-FW:1.9.0
MCSU 1853-0044-1052EAE2/1851-0044-1052EAE2, MAC 00:03:79:04:B7:A2
Bridge Mode, IP 192.168.1.1/255.255.255.0 Gateway
Bis as STU-R, PAIR-2, Annex B/G

Welcome to VPN Router Configuration Tool
UserName : root
Password : ****
VPNRouter#        ← Hostname
VPNRouter#
VPNRouter#show
VPNRouter/show#system
 Model Name          : SHDTU-09(is)
 Host Name           : VPNRouter
 HW MCSU             : 185300441052EAE2
 SW MCSU             : 185100441052EAE2
 Software Version    : 105
 DSL ChipName        : PEF22628V1.2
 DSL Phy Fw Version  : 1.1-1.9.0__001_eLP
 DSL IDC Fw Version  : 1.9.0
 DSL Physical Pairs  : 2
 Mac                 : 00:03:79:04:B7:A2
 SerialNo            : BKLX43FA0013
 Current   Time      : 2019/01/01 15:46:34
 System Up Time      : 0 days 14 hours 46 mins 40 secs
VPNRouter/show#
```

3.2 SHDSL



SHDSL Parameter

TC Layer	Übertragungstechnik ATM oder EFM
Pair Mode	Unterstützt 2-Draht, 4-Draht, 8-Draht, „Multi-Link“ oder „Auto Fall Back“. „Multi-Link“ und „Auto Fall Back“ wird nur bei Geräten unterstütz die mindestens mit 2 oder mehr DSL Paaren betrieben werden

Folgende Modi stehen zur Verfügung:

2-Wire (2-Draht):	In diesem Modus ist nur ein SHDSL-Paar aktiv.
4-Wire (4-Draht):	EFM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit und eine Redundanz zu erzielen.

	ATM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit zu erzielen. Falls eines der beiden Paare ausfällt, führt dies auch zum Ausfall des anderen Paares.
8-Wire (8-Draht):	EFM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit und eine Redundanz zu erzielen.
	ATM-Modus: In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit zu erzielen. Falls eines der beiden Paare ausfällt, führt dies auch zum Ausfall des anderen Paares.
Auto-Fall-Back:	Nur für den ATM-Modus verfügbar. In diesem Modus werden zwei Paare gebündelt, um eine höhere Übertragungsgeschwindigkeit und Redundanz zu erzielen.
Multi-Link:	Jede SHDSL-Leitung fungiert als unabhängiges 2-Draht-Paar. Wird für die gleichzeitige Verbindung zu zwei Remote-Geräten mit 2-Draht-Betrieb verwendet.
SHDTU- 06-is / 05-is	(2-Draht-Betrieb) ermöglicht nur die Auswahl von zwei Drähten.
SHDTU- 09-is SHDTU-08-is SHDTU-08-is-SFP	(4-Draht-Betrieb) ermöglicht die Auswahl von 2 oder 4 Drähten.
SHDTU- 10-is	(8-Draht-Betrieb) ermöglicht die Auswahl von 2, 4 oder 8 Drähten.
Mode	Stellen Sie beim Gerät entweder Master (STU-C) oder Slave (STU-R) ein.
Annex	Es gibt 4 Annex Typen. Annex A(Amerika), Annex B(Europa), Annex A/F (Amerika) und Annex B/G(Europa).
TC-PAM	Unterstützt wird ”Auto”, “TC-PAM-16”, “TC-PAM-32”, “TC-PAM-4”, “TC-PAM-8”, “TC-PAM-64”, “TC-PAM-128” im Master Betrieb STU-C„ TC-PAM-Extend” für den Slave Betrieb STU-R.
Rate Adaption	Unterstützt Fixed, Automatic (fast) und Automatic (secure) Bei Automatic (fast) – versucht das Gerät mit der maximalen Geschwindigkeit zu verbinden. Automatic (secure) – versucht das Gerät mit der maximalen Stabilität die Verbindung aufzubauen.
Max Base Rate	Maximale SHDSL Geschwindigkeit
Min Base Rate	Die minimale SHDSL Geschwindigkeit
SNR	(Signalrauschabstand) Hier legen Sie die SNR-Margin fest. Wenn ein Wert von 0 eingetragen wird, akzeptiert das SHDTU alle SNR-Werte.
PBO Mode	Power Back Off Mode, Normal oder Forced
PBO Value	Der PBO-Wert kann im Bereich von 0~31 dB festgelegt werden.
PBO Offset	Das PBO Offset kann im Bereich von 0~31 dB festgelegt werden.
EPL Mode	Ethernet Private Line (EPL) bietet eine Point-to-Point Ethernet Virtual Connection (EVC) zwischen einem Paar dedizierter Benutzer-Netzwerkschnittstellen (UNIs) mit einem hohen Maß an Transparenz. Mit „Enable“ können Sie diese Funktion aktivieren und mit „Disable“ wieder deaktivieren.
Interop Mode	Diese Funktion ermöglicht Ihnen die Aktivierung oder Deaktivierung der G.SHDSL-Version für das SHDTU durch Auswahl von „NONE“ oder „GSPN“ (GlobalSpan).

Die Einstellungen Annex A und Annex B werden für die Verbindung mit älteren G.SHDSL-Chips verwendet, die nur TCPAM-16 unterstützen. Der Parameter „Inter Mode“ wird verwendet, um die Kompatibilität mit älteren G.SHDSL-Chips zu ermöglichen.
Da der ältere Chip den EFM-Modus nicht unterstützt, können Annex A und Annex B im EFM-Modus nicht ausgewählt werden.

Für G.SHDSL.bis wird empfohlen, Annex A / F und Annex B / G zu konfigurieren.

TC-PAM 4/8/64/128 ist ein proprietärer Anbieter von DSL-Chips. Der proprietäre TC-PAM-Modus wird im ATM-Modus nicht unterstützt. Beim STU-C (Master) können Sie TC-PAM 4, 8, 64 oder 128 einstellen beim STU-R (Slave) jedoch nicht. Für STU-R (Slave) wird der TC-PAM-Modus des STU-C (Master) übernommen. Wir empfehlen TC-PAM-Extend auszuwählen.

Die Maximale- und Minimale Datenübertragungsrate ist vom TC-PAM Wert und der Annex Einstellung abhängig. Bitte sehen Sie sich dazu die folgende Tabelle an:

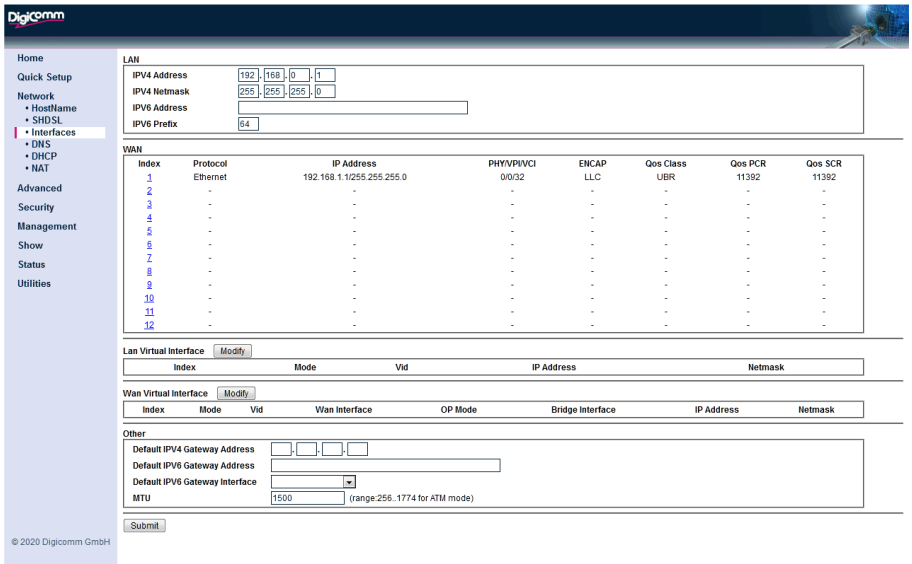
TCPAM Mode	Annex A Annex B	Annex A/F Annex B/G
TCPAM-Auto	-	3 ~ 89
TCPAM-16	3 ~ 36	3 ~ 60
TCPAM-32	-	12 ~ 89
TCPAM-4	-	1 ~ 39
TCPAM-8	-	2 ~ 79
TCPAM-64	-	3 ~ 199
TCPAM-128	-	3 ~ 239
TCPAM-Extend	-	3 ~ 239

TC-PAM-Extend ist nur im Slave-Modus möglich.

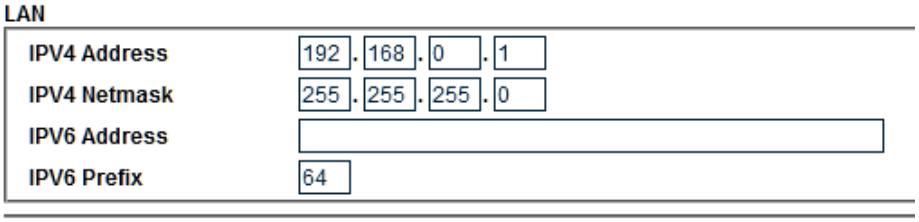
3.3 Interfaces (Schnittstellen)

Über die Funktion „Interfaces“ können Sie die LAN- und WAN-Einstellungen, sowie das Default Gateway nach Abschluss der Ersteinrichtung ändern. Wenn Sie Änderungen vornehmen, müssen Sie anschließend das SHDTU neu starten, damit diese Änderungen auch wirksam werden. Dies kann einige Minuten dauern.

Hinweis: Wenn Sie auf „Submit“ geklickt haben, werden die Einstellungen vorübergehend gespeichert. Es öffnet sich eine Übersichtsseite. Hier klicken Sie auf „Apply“ um die Einstellungen zu übernehmen.



3.3.1 Interfaces / LAN (LAN Schnittstelle)



LAN Parameter

IPV 4 Address LAN IPV4 Adresse. Die Standard Adresse ist die 192.168.0.1 (Master)
IPV 4 Netmask LAN IPV4 Subnetmask
IPV 6 Address LAN IPV6 Adresse
IPV 6 Prefix LAN IPV6 prefix

3.3.2 Interfaces / WAN (WAN Schnittstelle)

Im ATM-Modus können Sie bis zu 12 WAN Schnittstellen konfigurieren.

ATM Qos Class

Das SHDTU unterstützt UBR, CBR, VBR-rt und VBR-nrt.

Bei UBR (Unspecified Bit Rate) handelt es sich um den einfachsten Service der ATM Netzwerke. Es gibt allerdings keinerlei Garantie. Dies ist ein grundlegender Service für die Übertragung von Internet-Traffic über das ATM-Netzwerk.

CBR (Constant Bit Rate) wird von Verbindungen genutzt, die eine statische Bandbreite benötigen, die während der gesamten Verbindungsdauer zur Verfügung steht. Diese Bandbreite wird durch die Peak Cell Rate (PCR) definiert. Anhand der PCR des CBR-Traffic werden dem VC bestimmte Slots in der Schedule-Tabelle zugewiesen. Der ATM sendet immer eine einzelne Zelle während des zugewiesenen Slots der CBR-Verbindung.

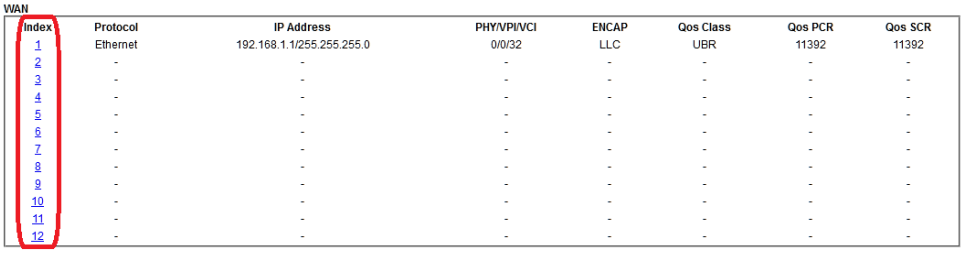
VBR-rt (Variable Bit Rate real-time) ist für Echtzeit-Anwendungen vorgesehen, beispielsweise für komprimiertes Voice-over-IP und Videokonferenzen, bei denen es auf eine strikte Beschränkung von Verzögerungen und Verzögerungsabweichungen ankommt. VBR-rt wird durch die Peak Cell Rate (PCR), Substained Cell Rate (SCR) und die Maximum Burst Rate (MBR) definiert.

VBR-nrt (Variable Bit Rate non-real-time) ist für Nicht-Echtzeit-Anwendungen vorgesehen, z.B. für FTP, E-Mail-Versand und Webbrowsing.

ATM Qos Class/PCR/SCR

PCR (Peak Cell Rate) in Kbit/s: Die maximale Datenrate für die Übertragung von Daten, Audio- und Video-Dateien. PCR und MBS eignen sich zur Verringerung der Latenz und nicht zur Erhöhung der Bandbreite.

SCR (Substained Cell Rate): Die dauerhafte Datenrate für die Übertragung von Daten, Audio- und Video-Dateien. Bei der SCR handelt es sich um die tatsächliche Bandbreite eines VC und nicht um die durchschnittliche Übertragungsrate über einen längeren Zeitraum hinweg.



WAN

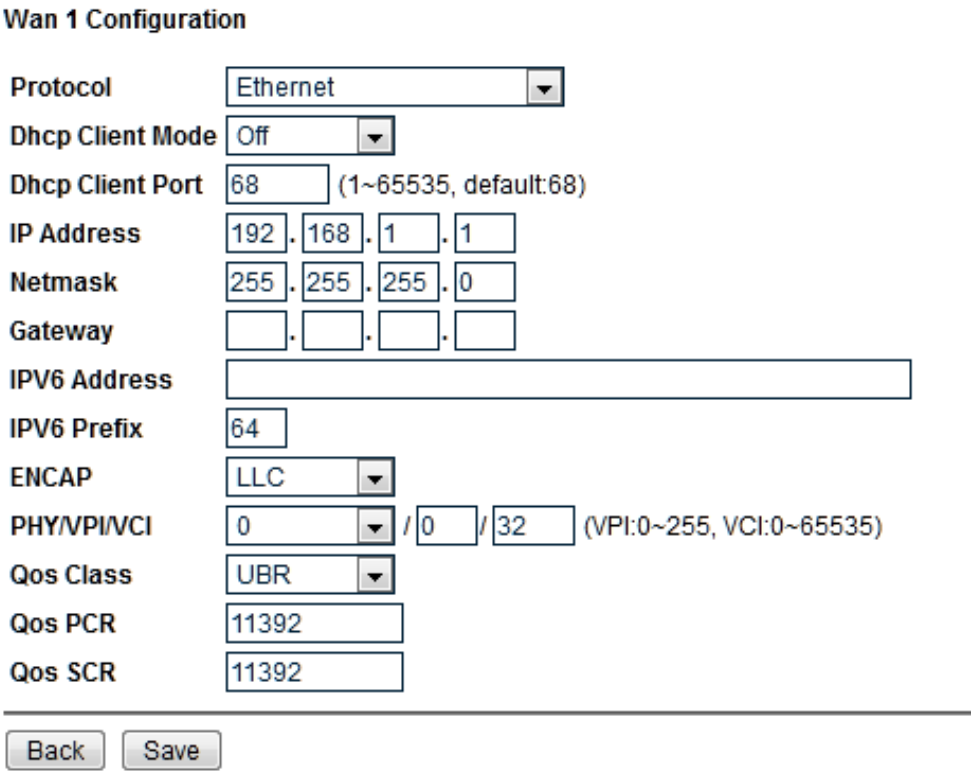
Index	Protocol	IP Address	PHY/VPI/VCI	ENCAP	Qos Class	Qos PCR	Qos SCR
1	Ethernet	192.168.1.1/255.255.255.0	0/0/32	LLC	UBR	11392	11392
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-

Der Index 1-4 der konfigurierbaren WAN Schnittstelle im EFM Modus, ist von der Anzahl der zur Verfügung stehenden SHDSL Leitungen abhängig.

WAN (EFM Mode)

Index	Protocol	IP Address	PHY/VPI/VCI	ENCAP	Qos Class	Qos PCR	Qos SCR
1	Ethernet	-/-	-	-	-	-	-

Klicken Sie auf den „Index-Link“ (Hier auf der Abbildung auf die 1) um die WAN-Konfigurationsseite aufzurufen.



Wan 1 Configuration

Protocol	Ethernet
Dhcp Client Mode	Off
Dhcp Client Port	68 (1~65535, default:68)
IP Address	192 . 168 . 1 . 1
Netmask	255 . 255 . 255 . 0
Gateway	. . .
IPV6 Address	
IPV6 Prefix	64
ENCAP	LLC
PHY/VPI/VCI	0 / 0 / 32 (VPI:0~255, VCI:0~65535)
Qos Class	UBR
Qos PCR	11392
Qos SCR	11392

Back Save

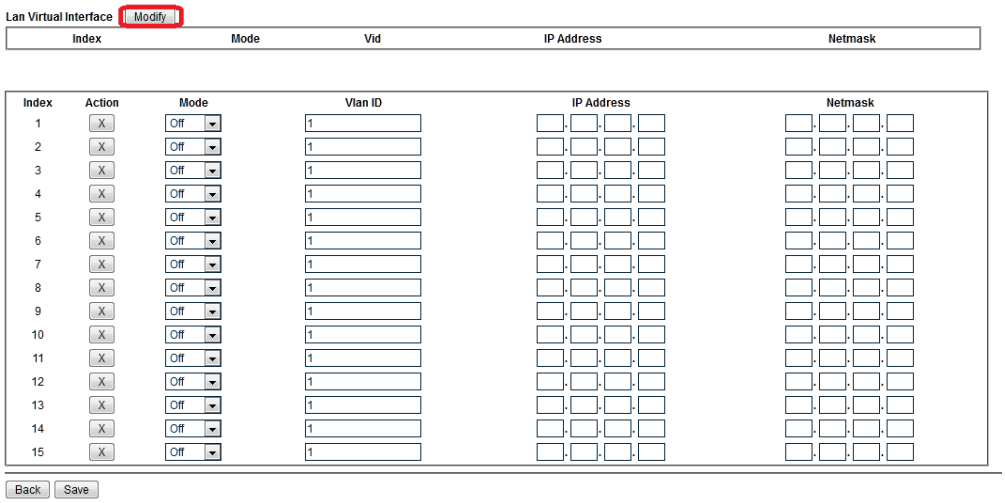
WAN Parameter

Protocol	Folgende Einstellungen können vorgenommen werden: Disable- WAN ist deaktiviert Ethernet – WAN als Ethernet im ATM Modus IP im ATM Modus PPP im ATM Modus PPP über Ethernet
DHCP Client Mode	OFF – DHCP Client Mode ist deaktiviert ON- DHCP Client Mode ist aktiviert
IP Address	Geben Sie die IP Adresse ein

Netmask	Geben Sie die Subnetmaske ein
Gateway	Geben Sie die Gateway IP Adresse ein
IPV6 Address	Geben Sie die statische IPv6 Adresse ein
IPV6 Prefix	Geben Sie den statischen IPv6 prefix ein
Encap	LLC oder VC Mux (nur im ATM-Modus möglich)
PHY/VPI/VCI	Geben Sie die PVC Einstellungen ein (nur im ATM-Modus möglich)
Qos Class	ATM Qos Class, UBR, CBR, VBR-RT, VBR-NRT
Qps PCR	ATM Qos Peak Cell Rate, unit in kbps
Qos SCR	ATM Qos Sustained Cell rate, unit in kbps

Hinweis: Klicken Sie auf „Submit“ und die Einstellungen werden vorübergehend gespeichert. Es öffnet sich eine Übersichtsseite. Hier klicken Sie auf „Apply“ um die Einstellungen zu übernehmen.

3.3.3 Interfaces / LAN Virtual Schnittstelle



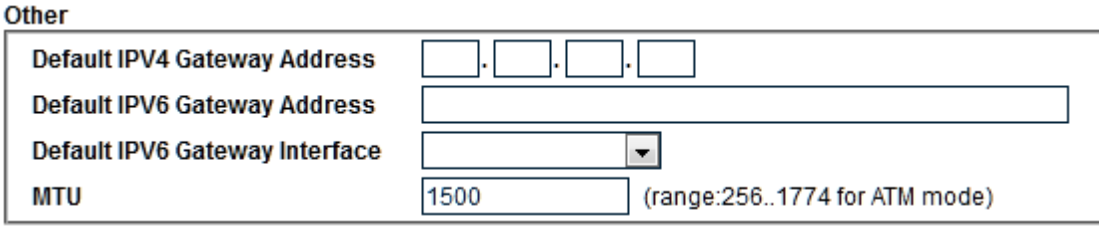
LAN Virtual Interface Parameter

Action	Klicken Sie auf den X Button um den Eintrag zu löschen
Mode	Off/ On (Aus oder An) Deaktiviert/ Aktiviert den Eintrag
VLAN ID	VLAN ID im Bereich von 1 bis 4094
IP Address	Geben Sie die IP Adresse ein
Netmask	Geben Sie die Subnet Maske ein

Hinweis: Wenn Sie auf „Submit“ geklickt haben, werden die Einstellungen vorübergehend gespeichert. Es öffnet sich eine Übersichtsseite. Hier klicken Sie auf „Apply“ um die Einstellungen zu übernehmen.

3.3.4 Weitere Schnittstellen Einstellungen

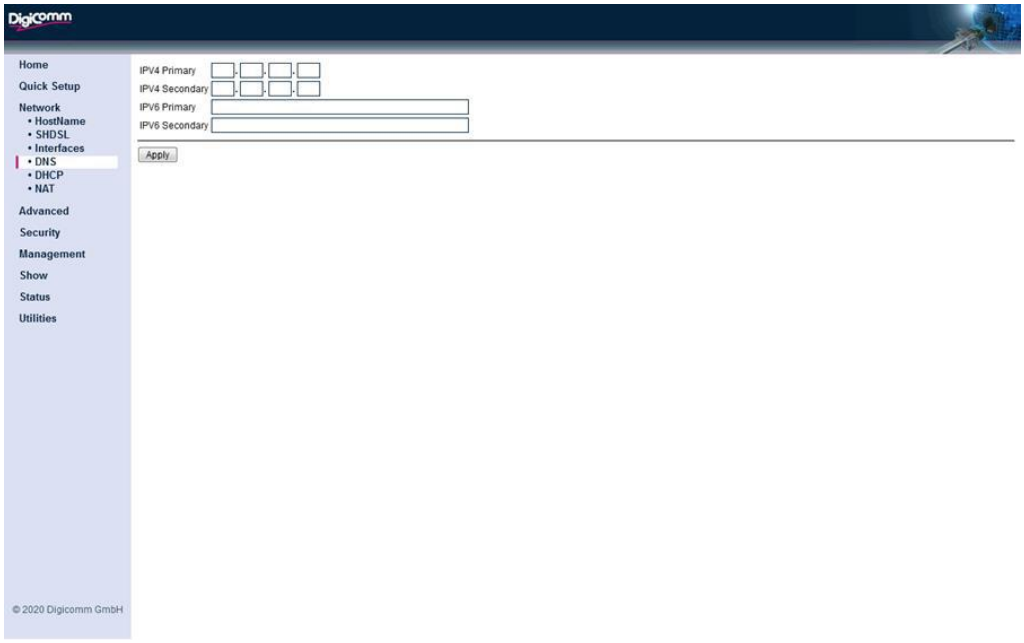
Weitere Parameter



Default IPV4 Gateway Address	Geben Sie die Standard Gateway IPV4 Adresse ein
Default IPV6 Gateway Address	Geben Sie die Standard Gateway IPV6 Adresse ein

Default IPV6 Gateway Interface	Wählen Sie die Standard Gateway Schnittstelle für IPV6 aus (LAN oder WAN1 –WAN 12)
MTU	Geben Sie die maximale Paketgröße für das für das Gerät an

3.4 DNS



DNS Parameter

IPV4 Primary	DNS IPV4 primäre Adresse
IPV4 Secondary	DNS IPV4 sekundäre Adresse
IPV6 Primary	DNS IPV6 primäre Adresse
IPV6 Secondary	DNS IPV6 sekundäre Adresse

Hier lassen sich zwei DNS-Adressen speichern, eine für den primären und eine weitere für den sekundären Bereich.

Bei dem Domain Name Service (DNS) handelt es sich um ein System zur Identifizierung von Servern im Netzwerk anhand von Namen statt ihrer IP-Adressen. Da die gesamte Kommunikation im Netzwerk über IP-Adressen läuft, muss der Name jedes Servers in eine IP-Adresse umgewandelt werden. Diese Aufgabe übernimmt der Domain Name Server.

3.5 DCHP

Das DHCP (Dynamic Host Configuration Protocol) ist ein Kommunikationsprotokoll, das Netzwerkadministratoren die zentrale Verwaltung und automatische Zuordnung von IP-Adressen innerhalb des Netzwerks eines Unternehmens ermöglicht.

Die Funktion „DHCP“ verfügt über drei Modi: „Disable“, „Server“ und „Relay“.

1. Disable: Deaktivieren des DHCP-Servers.

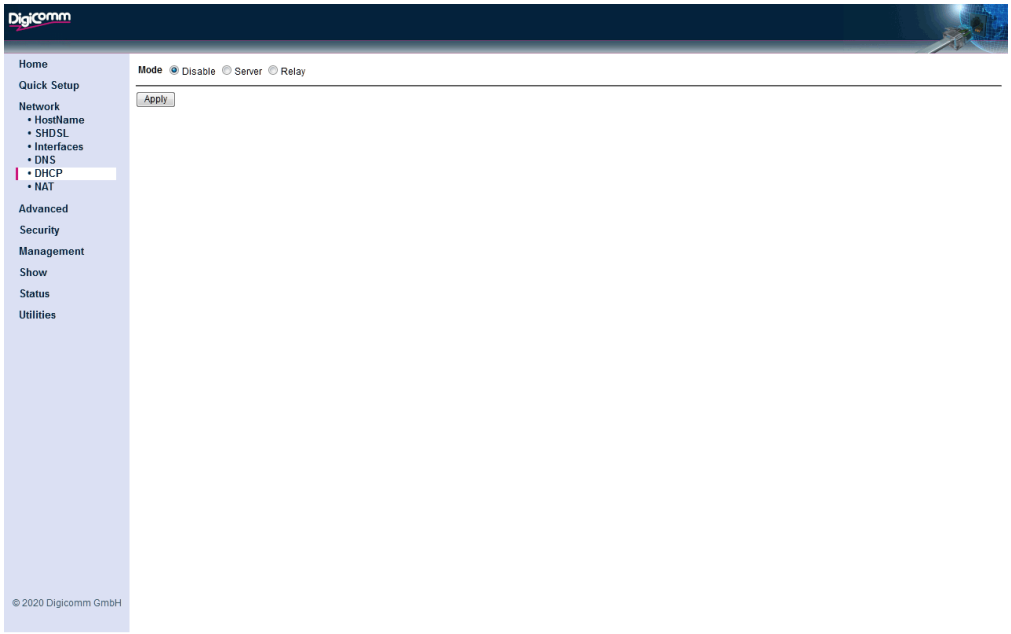
2. Server: Aktivieren des DHCP Servers und Zuweisen von IP-Adressen.

3. Relay: Aktivieren des DHCP Relay und Zuweisen von IP-Adressen.

Stellen Sie als erstes sicher, dass Sie „Server“ als Modus ausgewählt haben. Wählen Sie anschließend einen DHCP-Server aus (in diesem Konfigurationssystem stehen fünf DHCP-Server zur Verfügung) und konfigurieren Sie dessen Parameter, indem Sie auf die entsprechende Zahl klicken.

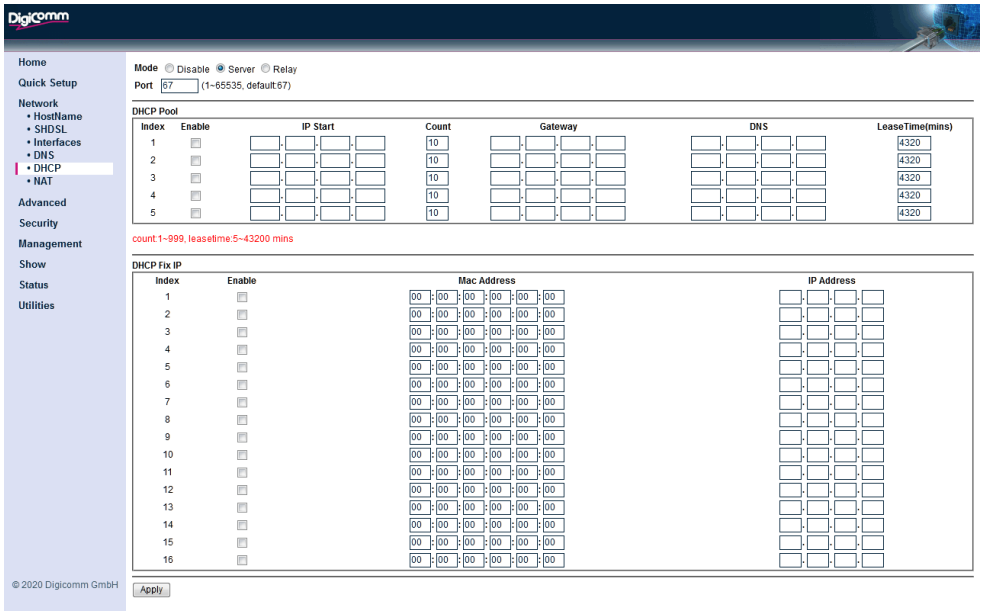
3.5.1. DHCP/ Deaktiviert

Wählen Sie „Disable“ aus um den DHCP Port zu deaktivieren.



3.5.2. DHCP/ Server

Wählen Sie “Server” aus, um den DHCP Server zu aktivieren.



DHCP Server Parameter

Port DHCP Server Daemon Listen Port

DHCP Pool Parameter

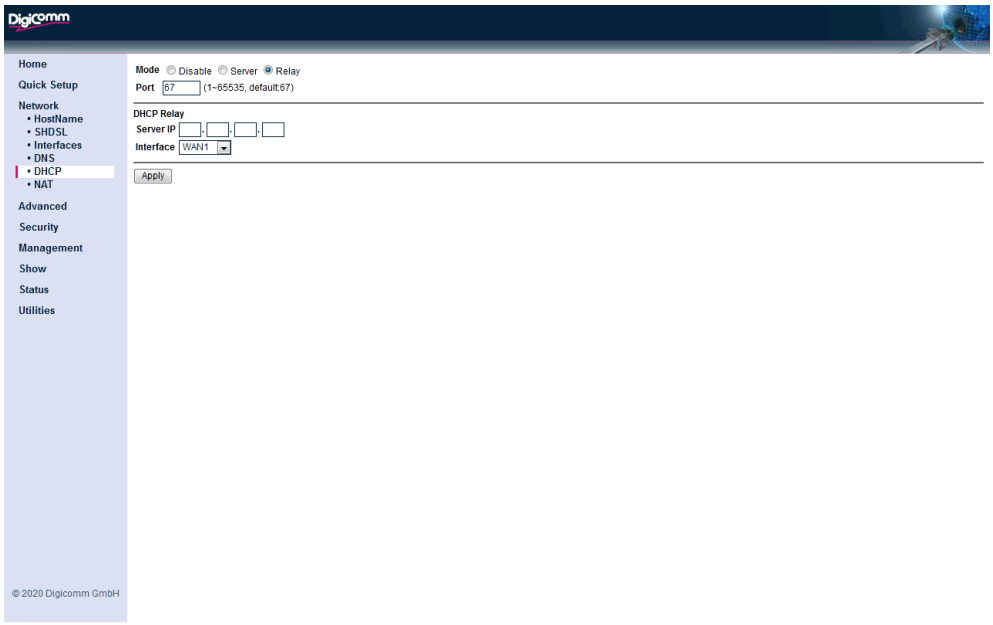
Enable	Eintrag aktivieren/ deaktivieren
IP Start	Start IP Adresse des DHCP Clients
Count	Anzahl der IP Adressen des DHCP Clients
Gateway	Gateway für DHCP Client
DNS	DNS für DHCP Client
Lease Time	Die Anzahl der Minuten die die IP-Adresse des DHCP-Clients verwendet werden kann

DHCP Fix IP Parameter

Enable	Eintrag aktivieren/ deaktivieren
MAC Address	Host MAC Adresse
IP Address	Host feste IP Adresse

3.5.3. DHCP/ Relay

Wählen Sie den Modus „Relay“ aus. Anschließend geben Sie die IP-Adresse des DHCP-Servers ein und weisen einen WAN-Port zu.



DHCP Parameter

Port	DHCP Relay Daemon Listen Port
Server IP	DHCP Server IP
Interface	DHCP Relay uplink Schnittstelle

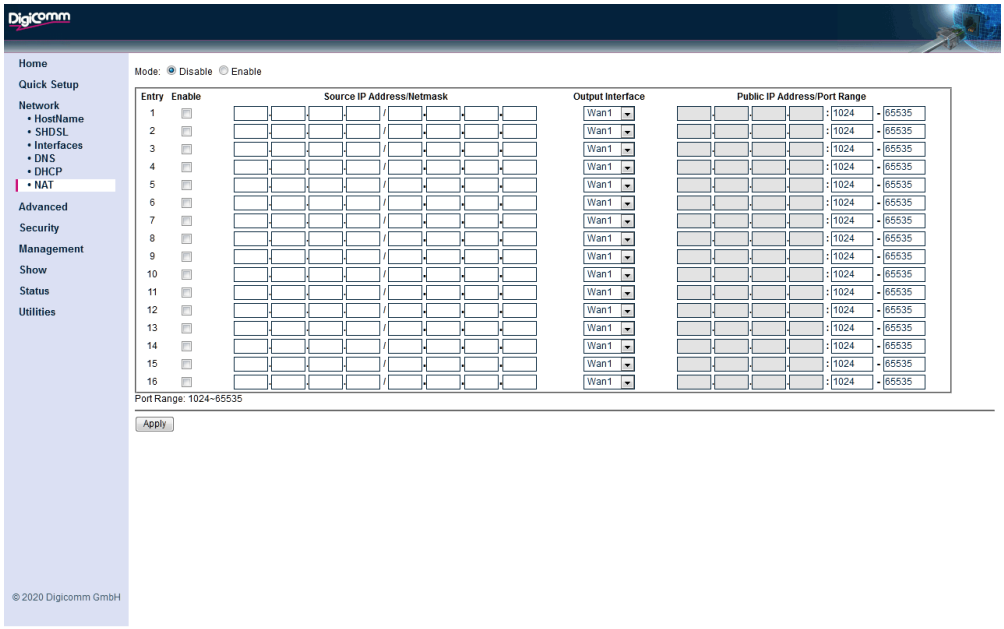
3.6 NAT (Network Address Translation)

Hinweis: Bitte beachten Sie, dass NAT nur im „Router-Modus“ zur Verfügung steht.
Entscheiden Sie zuerst, ob Sie die Option „NAT“ aktivieren oder deaktivieren möchten.

Mit NAT (Network Address Translation) bezeichnet man eine Reihe von Verfahren für die Übersetzung einer IP-Adresse im Intranet, beispielsweise in einem Unternehmensnetzwerk, in eine öffentliche IP-Adresse.

Falls Sie diese aktivieren möchten, klicken Sie im Bereich „Mode“ auf die Schaltfläche „Enable“.

In der SHDTU Konfiguration lassen sich gleichzeitig sechzehn NAT-Regeln abspeichern. Durch die Angabe von IP-Adresse und Netzmaske können Sie eine IP-Gruppe einrichten. Anschließend lässt sich diese Gruppe einem Output-WAN-Port zuweisen. Falls Sie eine NAT Regel aktivieren möchten, klicken Sie auf das jeweilige Kontrollkästchen und anschließend auf „Apply“, um die Änderungen zu übernehmen.



NAT Allgemeine Einstellungen

Mode	NAT aktivieren/ deaktivieren

NAT Entry Einstellungen

Enable	Eintrag aktivieren/ deaktivieren NAT Regeleintrag
Source IP Address/Netmask	Lokale/Private IP Adresse/ Subnetmaske für das NAT
Output Interface	WAN 1-12 Öffentliche IP als Ausgangsschnittstelle
Public IP Address / Port	Die globale/ Öffentliche IP Adresse/ Port für NAT

4 Erweitertes Menü (Advanced)

Das Menü „Advanced“ bietet den Zugriff auf neun Funktionen:

1. VLAN
2. MSTP
3. QinQ
4. Switch
5. Static Route
6. QoS
7. RIP/ OSPF
8. Virtual Server
9. DMZ
10. DDNS
11. IGMP
12. Dot1x

4.1 VLAN

VLAN steht nur im Bridge-Modus zur Verfügung.

Die Option „VLAN“ (Virtual Local Area Network) ermöglicht die Aufteilung eines physischen Netzwerks in mehrere logische Netzwerke. Die Geräte in einem logischen Netzwerk gehören zu einer Gruppe. Ein Gerät kann zu mehr als einer Gruppe gehören. In einem VLAN kann ein einzelnes Gerät nicht direkt mit anderen Geräten kommunizieren, die nicht zu seiner Gruppe gehören.

Bei MTU (Multi-Tenant Unit)-Anwendungen ist ein VLAN unverzichtbar, um die Isolierung und Sicherheit der einzelnen Teilnehmer zu gewährleisten. Ist ein VLAN richtig konfiguriert, verhindert es den Zugriff eines Teilnehmers auf die Netzwerkressourcen eines anderen im gleichen LAN.

Ein VLAN verbessert auch die Netzwerkleistung durch die Beschränkung der Übertragungen an eine kleinere und besser zu verwaltende, logische Broadcast Domain. In einer herkömmlichen Switch-basierten Umgebung werden alle Übertragungspakete über die jeweiligen einzelnen Ports gesendet. In einem VLAN beschränkt sich die Übertragung auf eine spezifische Broadcast Domain.

Im Bridge Modus stehen zwei VLAN Typen zur Auswahl „802.1Q Tag-Based VLAN“ und „Port Based VLAN“.

4.1.1 Port-Based VLAN

Portbasierte VLANs sind VLANs, bei denen die Paketweiterleitungsentscheidung auf der Ziel-MAC-Adresse und dem zugehörigen Port basiert.

Bei Verwendung des portbasierten VLAN wird der Port einem bestimmten VLAN zugewiesen, unabhängig von dem Benutzer oder System, das an den Port angeschlossen ist. Dies bedeutet, dass alle an den Port angeschlossenen Benutzer Mitglieder im selben VLAN sein sollten. Der Netzwerkadministrator führt normalerweise die VLAN-Zuweisung durch. Die Portkonfiguration ist statisch und kann ohne manuelle Neukonfiguration nicht automatisch in ein anderes VLAN geändert werden.

So gelangen die mit dieser Methode weitergeleiteten Pakete nicht in andere VLAN-Domänen im Netzwerk. Nachdem einem VLAN ein Port zugewiesen wurde, kann der Port nicht an Geräte in einem anderen VLAN senden oder von diesem empfangen.

4.1.2 802.1Q Tag-Based VLAN

Klicken Sie auf die Option „802.1Q Tag-Based VLAN“, um das SHDTU zu konfigurieren.

Bei 802.1q werden die VLAN-Daten direkt in das Ethernet-Paket geschrieben. Jedes Paket ist mit einer VLAN ID (Virtual LAN ID) versehen, die als „Tag“ bezeichnet wird. So lassen sich VLANS über mehrere Switches hinweg konfigurieren. Beachten Sie, dass VLAN-Tags von H/W und/oder S/W entfernt werden können.

Bei 802.1q werden dem Ethernet-Frame 4 Bytes hinzugefügt, von denen 12 Bits für die VLAN-ID verwendet werden. Theoretisch sind bis zu 4096 VLANs pro Netzwerk möglich.

Ein Ethernet-Paket mit einer VLAN-ID wird als getaggtes Paket bezeichnet. Demnach wird ein Ethernet-Paket ohne VLAN-ID als nicht getaggtes Paket bezeichnet. In der Regel sind alle Pakete nicht getaggt, sofern sie nicht vor ihrem Eintreffen am Switch-Port durch den Adapter getaggt werden.

Regeln für aus- und eingehenden Datenverkehr:

Die Regeln für den ausgehenden Datenverkehr legen fest, welche Frames über einen Port gesendet werden können. Grundlage hierfür ist die Egress List des zugeordneten VLAN. In jedem VLAN legt eine Egress List die Ports fest, über die Frames weitergeleitet werden können. Gleichzeitig gibt sie an, welche Frames als getaggt und welche als nicht getaggt übertragen werden.

Mithilfe von Regeln für den eingehenden Datenverkehr kann nicht erwünschter Traffic an einem Port herausgefiltert werden. Bei aktiviertem Ingress Filtering ermittelt ein Port anhand der Engress List des dem Frame zugeordneten VLAN, ob ein Frame verarbeitet werden kann.

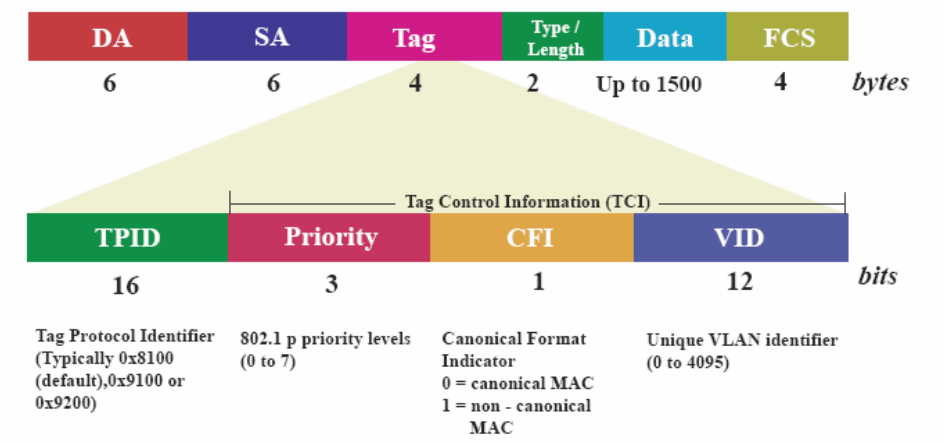
Wird an einem Switch-Port ein nicht getaggtes Paket empfangen, schreibt der Switch gemäß der PVID (Port VLAN) Port-Definition eine VLAN-ID in den Header des Frames. Normalerweise ist bei den meisten Switches die PVID-Standardeinstellung aller Ports = 1. Ein getaggter Frame wird beim Empfang an einem Switch-Port erkannt. Eine VID legt die Mitglieder einer Port-Gruppe fest. Ein Paket kann nur dann über einen Mitglieds-Port übertragen werden, wenn dieser Teil einer VID-Port-Gruppe ist. Die unterschiedlichen VID-Gruppen sind untereinander nicht sichtbar.

VID: Bei der (Virtual LAN ID) handelt es sich um eine Zahl zwischen 1 und 4094.

PVID: Die (Port VID) ist ein nicht getaggtes Mitglied eines Standard-VLAN zwischen 1 und 4094.

Link Type: „Access“ bedeutet, dass der Port nicht getaggte Pakete empfangen oder senden kann.

„Trunk“ bedeutet, dass der Port getaggte Pakete empfangen oder senden kann.



TCI (Tag Control Information field) einschließlich der Benutzerpriorität, CFI (Canonical Format Indicator) und VLAN-ID.

TPID (Tag Protocol Identifier) definierter Wert von 8100H (hexadezimal). Besitzt der Frame einen EtherType gleich 8100H, trägt dieser Frame das Tag IEEE 802.1Q/802.1P.

Das Feld „Priority“ bestimmt mit acht Prioritätsstufen ($2^3 = 8$) die Benutzerpriorität. IEEE 802.1P definiert die Funktion für diese 3 Benutzerprioritätsbits (siehe folgende Tabelle).

CFI (Canonical Format Indicator) ist für Ethernet-Switches immer auf null gesetzt. CFI wird aus Kompatibilitätsgründen zwischen einem Ethernet-Netzwerk und einem Token-Ring-Netzwerk verwendet. Wird ein Frame mit einem auf 1 gesetzten CFI an einem Ethernet-Port empfangen, darf dieser Frame nicht unverändert an einen nicht getaggten Port weitergeleitet werden.

VID (VLAN-ID) ist die Identifikation des VLAN, welche hauptsächlich durch den Standard 802.1Q verwendet wird. Mit einer Breite von 12 Bit ermöglicht er eine Identifikation von 4096 (2^{12}) VLANs. Von den 4096 möglichen VIDs wird eine VID von 0 zur Identifikation der Prioritätsframes verwendet und der Wert 4095 (FFF) ist reserviert. Somit sind maximal 4094 VLAN-Konfigurationen möglich.

Die Werkseinstellung des SHDTU hat standardmäßig ein VLAN mit der VID=1.

Ein Port wie LAN1 bis 4, DSL oder Sniffing kann nur eine PVID besitzen, jedoch so viele VIDs, wie das SHDTU in seiner VLAN-Tabelle speichern kann.

Ports in der gleichen VLAN-Gruppe nutzen die gleiche Frame Broadcast Domain, wodurch sich die Netzwerkleistung aufgrund des geringeren Broadcast-Verkehrs erhöht. VLAN-Gruppen können jederzeit durch Hinzufügen, Verschieben oder Ändern von Ports ohne erneute Verkabelung geändert werden.

Bevor dem SHDTU ein VLAN zugewiesen werden kann, muss zunächst jeder Port der/ den teilnehmenden VLAN-Gruppe(n) zugewiesen werden. Standardmäßig werden alle Ports dem VLAN1 als nicht getaggte Ports zugewiesen. Fügen Sie einen Port als getaggten Port hinzu, wenn über diesen der Datenverkehr von einem oder mehreren VLANs übertragen werden soll, und eventuell zwischengeschaltete Netzwerkgeräte am Host oder dem anderen Endpunkt der Verbindung eine Unterstützung für VLANs bieten. Anschließend weisen Sie auf den anderen VLAN-fähigen Netzwerkgeräten entlang des Pfads, über den dieser Datenverkehr an das gleiche bzw. die gleichen VLAN(s) übertragen wird, die Ports entweder manuell oder dynamisch mithilfe von GVRP zu. Falls allerdings ein Port dieses VPN-Routers eine Verbindung zu einem oder mehreren VLANs herstellen soll, jedoch keines der zwischengeschalteten Netzwerkgeräte und auch nicht der Host am anderen Endpunkt der Verbindung eine Unterstützung für VLANs bietet, müssen Sie diesen Port dem VLAN als nicht getaggten Port hinzufügen.

Hinweis: VLAN-getaggte Frames können durch ein VLAN-taugliches oder ein nicht VLAN-taugliches Netzwerk geleitet werden.

Die VLAN-Tags müssen entfernt werden, bevor die Frames an einen Endknoten-Host übertragen werden, der kein VLAN-Tagging unterstützt.

VLAN-Klassifizierung – Wenn ein VPN-Router einen Frame empfängt, klassifiziert er ihn mithilfe von einem von zwei möglichen Verfahren. Falls es sich um einen nicht getaggten Frame handelt, weist der VPN-Router den Frame einem verbundenen VLAN zu (anhand der Standard-VLAN-ID des Empfangs-Ports). Handelt es sich jedoch um einen getaggten Frame, nutzt der VPN-Router die getaggte VLAN-ID zur Identifizierung der Port Broadcast Domain des Frames.

Port Overlapping – Mithilfe dieser Option kann der Zugriff auf die von verschiedenen VLAN-Gruppen gemeinsam genutzten Netzwerkressourcen wie Dateiserver oder Drucker freigegeben werden.

Untagged VLANs – Nicht getaggte (oder statische) VLANs dienen normalerweise dazu, das übertragene Datenvolumen zu verringern und die Sicherheit zu erhöhen. Eine Gruppe von Netzwerkbenutzern, die einem VLAN zugeordnet sind, bilden eine Broadcast Domain, die von anderen auf dem VPN-Router konfigurierten VLANs getrennt ist. Datenpakete werden nur zwischen Ports übertragen, die dem gleichen VLAN zugewiesen sind. Nicht getaggte VLANs können verwendet werden, um Benutzergruppen oder Subnetze manuell zu isolieren.

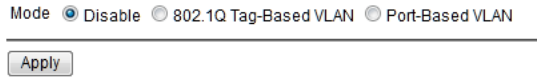
PVID – Nicht getaggten Frames zugewiesene VLAN-ID, die über die Schnittstelle empfangen wurden.

Falls eine Schnittstelle nicht Mitglied von VLAN 1 ist und Sie deren PVID diesem VLAN zuordnen, wird die Schnittstelle automatisch VLAN 1 als nicht getaggtes Mitglied hinzugefügt. Für alle anderen VLANs muss zuerst eine Schnittstelle als nicht getaggtes Mitglied konfiguriert werden, bevor Sie deren PVID dieser Gruppe zuweisen können.

Link Type – Konfiguriert den Port für den Empfang der Frame-Typen: „UnTag“ bedeutet, dass der Port ausschließlich nicht getaggte Frame-Typen empfangen oder senden kann. „Tag“ bedeutet, dass der Port ausschließlich getaggte Frame-Typen empfangen oder senden kann.

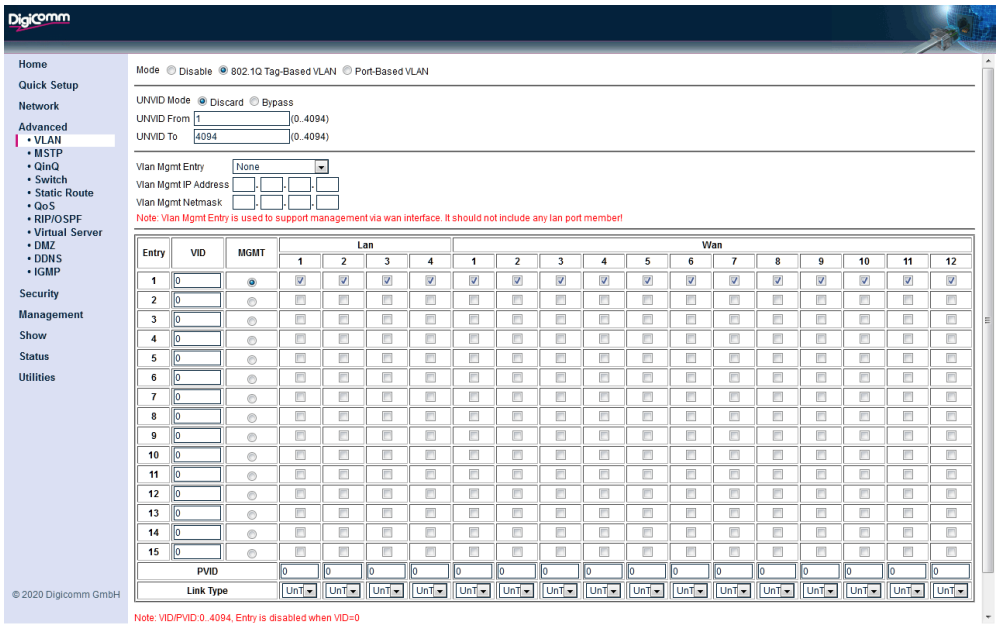
4.1.3. VLAN/ Disable

Klicken Sie die Option „Disable“ an, um das VLAN zu deaktivieren.



4.1.4. VLAN/ Tag-Base für den Bridge Modus

Klicken Sie die Option „802.1Q Tag-Based VLAN“ an, um das Tag basierende VLAN zu aktivieren.



VLAN UNVID Parameter

Mode	Discard - Paket mit unbekannter VID verwerfen Bypass - Weiterleiten eines unbekannten VID Paketes
UNVID From To	UNVID Bereich von/ bis

VLAN Mgmt Parameter

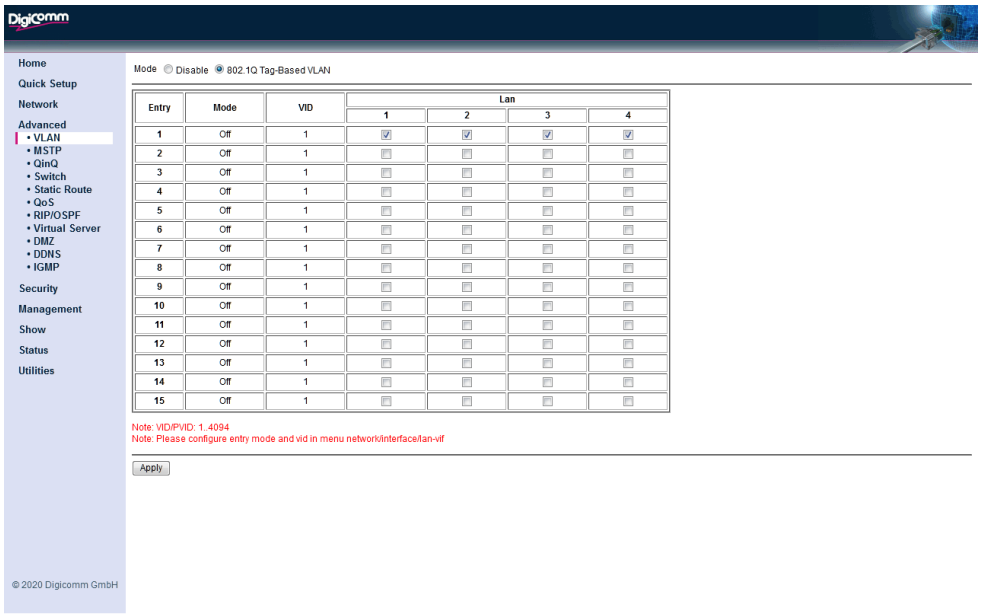
VLAN Mgmt Eintrag	None – Wenn Sie None aus wenn kein Vlan mgmt Eintrag vorhanden ist. Oder wählen Sie VLAN1 bis 15 VLAN für den Eintrag für mgmt
VLAN MgmT IP Address	Geben Sie die IP Adresse des VLAN mgmt Eintrages ein
VLAN Mgmt Netmask	Geben Sie die Subnetmaske des VLAN mgmt Eintrages ein
VID	0 bis 4095, bei 0 ist der Eintrag deaktiviert

PVID	0 bis 4094
Link Type	Tag/Untag

Hinweis: Der "Vlan Mgmt-Eintrag" wird verwendet, um die Verwaltung über die WAN-Schnittstelle zu unterstützen. Es sollte kein LAN-Port-Mitglied enthalten!

4.1.5. VLAN/Tag-Base für den Router Modus

Klicken Sie die Option „802.1Q Tag-Based VLAN“ an, um das Tag basierende VLAN zu aktivieren.

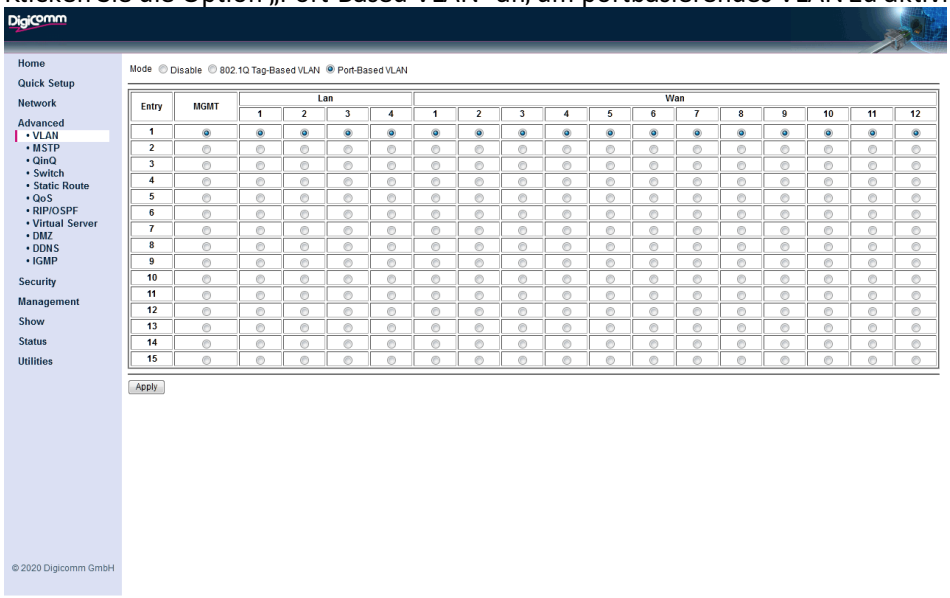


Im Router-Modus wird Tag-Base-VLAN nur auf der LAN- / Switch-Seite angewendet. Es ist eine Verbindung zur virtuellen LAN-Schnittstelle. Der Modus und die VID des VLAN-Eintrags werden im LAN-Eintrag für die virtuelle Schnittstelle definiert (siehe 3.3.3). Das VLAN definiert nur die Portmitglieder des VLAN-Eintrags.

Für den VLAN-Eintrag ist das LAN-Ausgangspaket mit Tags versehen.

4.1.6 Portbasierendes VLAN

Klicken Sie die Option „Port-Based VLAN“ an, um portbasierendes VLAN zu aktivieren.



Das portbasierte VLAN erlaubt nur einen MGMT Eintrag als LAN-Schnittstelle (3.3.1).
Jeder Port darf nur Mitglied eines VLAN-Eintrages sein.
Bei Verwendung des portbasierten VLAN wird der Port einem bestimmten VLAN zugewiesen, unabhängig von dem Benutzer oder System, das an den Port angeschlossen ist. Dies bedeutet, dass alle an den Port angeschlossenen Benutzer Mitglieder im selben VLAN sein sollten. Der Netzwerkadministrator führt normalerweise die VLAN-Zuweisung durch. Die Portkonfiguration ist statisch und kann ohne manuelle Neukonfiguration nicht automatisch in ein anderes VLAN geändert werden.

So gelangen die mit dieser Methode weitergeleiteten Pakete nicht in andere VLAN-Domänen im Netzwerk. Nachdem einem VLAN ein Port zugewiesen wurde, kann der Port nicht an Geräte in einem anderen VLAN senden oder von diesem Port Daten empfangen.

4.2 MSTP

Hinweis: MSTP ist nur im Bridge Modus verfügbar

STP (Spanning-Tree Protokoll) definiert in IEEE 802.1D, ist ein Link Management Protokoll das eine „Pfadredundanz“ bietet und gleichzeitig unerwünschte Schleifen im Netzwerk verhindert. Damit ein Ethernet-Netzwerk ordnungsgemäß funktioniert, darf zwischen zwei Stationen nur ein aktiver Pfad vorhanden sein.

Mehrere aktive Pfade zwischen Stationen verursachen Schleifen im Netzwerk. Wenn in der Netzwerktopologie eine Schleife vorhanden ist, besteht die Möglichkeit, dass Nachrichten dupliziert werden. Wenn Schleifen auftreten, werden bei einigen Switches Stationen auf beiden Seiten des Switches angezeigt. Diese Bedingung verwirrt den Weiterleitungsalgorithmus und ermöglicht die Weiterleitung doppelter Frames. Um „Pfadredundanzen“ bereitzustellen, definiert das Spanning-Tree-Protokoll einen „Tree“ der alle Switches in einem erweiterten Netzwerk umfasst.

Das Spanning-Tree-Protokoll zwingt bestimmte redundante Datenpfade in einen Standby-Zustand (blockiert). Wenn ein Netzwerksegment im Spanning-Tree-Protokoll nicht mehr erreichbar ist oder sich die Kosten des Spanning-Tree-Protokolls ändern, konfiguriert der Spanning-Tree-Algorithmus die Spanning-Tree-Topologie neu und stellt die Verbindung durch Aktivieren des Standby-Pfads wieder her.

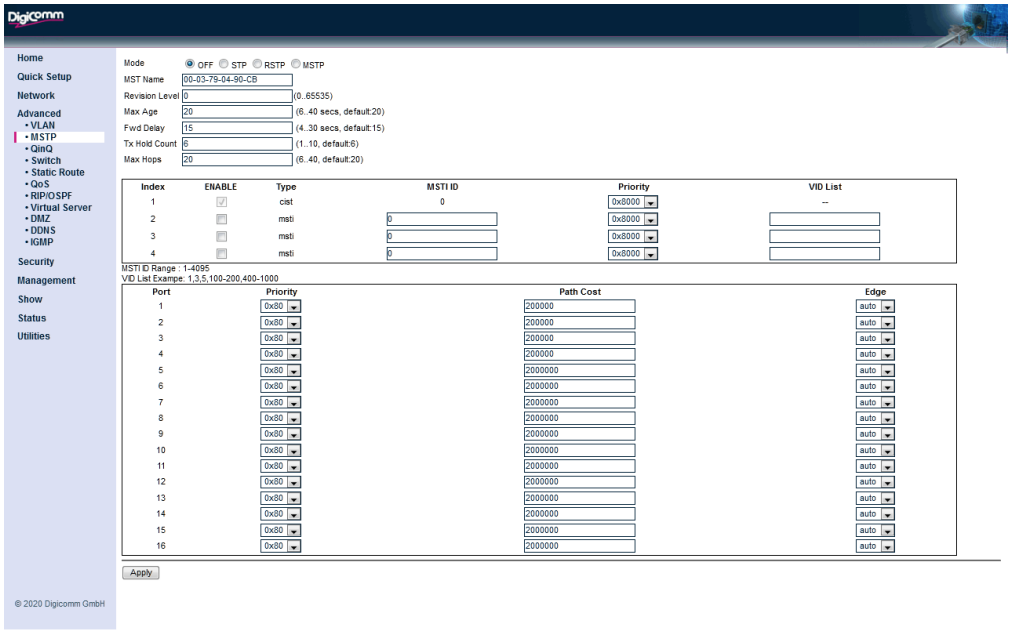
Der Betrieb des Spanning-Tree-Protokolls ist für Endstationen transparent, die nicht wissen, ob sie mit einem einzelnen LAN-Segment oder einem Switched LAN mit mehreren Segmenten verbunden sind.

RSTP (Rapid Spanning Tree Protokoll) als 802.1w. RSTP bietet eine erheblich schnellere Wiederherstellung als Reaktion auf Netzwerkänderungen oder -ausfälle und führt dazu neue Konvergenzverhalten und Bridge-Port-Rollen ein. RSTP wurde so konzipiert, dass es mit Standard-STP abwärtskompatibel ist.

MSTP (Multiple Spanning Tree Protocol) als 802.1s. MSTP definiert eine Erweiterung von RSTP, um die Nützlichkeit von virtuellen LANs (VLANs) weiterzuentwickeln.

Standardmäßig wird ein Spanning Tree, der ein oder mehrere VLANs abbildet, als Multiple Spanning Tree (MST) bezeichnet. Wenn MSTP implementiert ist, kann ein Spanning Tree für einzelne VLANs oder für Gruppen von VLANs definiert werden. Darüber hinaus kann der Administrator alternative Pfade innerhalb eines Spanning Trees definieren. VLANs müssen einer sogenannten Multiple Spanning Tree Instance (MSTI) zugeordnet werden. Switches werden zuerst einer MST-Region zugewiesen, dann werden VLANs diesem MST zugeordnet oder diesem MST zugewiesen. Ein Common Spanning Tree (CST) ist ein MST, dem mehrere VLANs zugeordnet sind. Diese Gruppe von VLANs wird als MST-Instanz (MSTI) bezeichnet. CSTs sind abwärtskompatibel mit dem STP- und RSTP-Standard. Ein MST, dem nur ein VLAN zugewiesen ist, ist ein Internal Spanning Tree (IST)

Im Gegensatz zu einigen proprietären Pro-VLAN-Spanning-Tree-Implementierungen enthält MSTP alle Spanning-Tree-Informationen in einem einzigen BPDU-Format. Dies reduziert nicht nur die Anzahl der BPDUs, die in einem LAN für die Kommunikation von Spanning Tree-Informationen für jedes VLAN erforderlich sind, sondern stellt auch die Abwärtskompatibilität mit RSTP (und damit auch mit klassischem STP) sicher.



MSTP Parameter

Mode	Aus (OFF), STP, RSTP und MSTP auswählbar
MST Name	MST Domain Name
Revision Level	MST Domain Revision Level (0 bis 65535- Standardwert 20)
Max Age	Angabe des maximalen (6 bis 40 Sekunden – Standardwert 15)
Fwd Delay	Vorwärtsverzögerungszeit einstellen (4 bis 30 Sekunden- Standardwert 15)
Tx Hold Count	Stellen Sie Tx Hold Count für die Übertragung ein (1 bis 20- Standardwert 6)
Max Hops	Die maximale Anzahl von Hops für die MST-Domäne(6 bis 40 – Standardwert 20)

MTSi Parameter

Enable	Aktivieren oder Deaktivieren des MSTI Eintrages
MSTI ID	Eintrag des MSTi ID
Priority	Eintrag der MSTi Prioritäten
VID List	Eintrag der MSTi VID Mitglieder

Port Parameter

Priority	Eintrag der Port Prioritäten
Path Cost	Geben Sie die Port Pfad Kosten ein. Standardmäßig hängen die Kosten von den physikalischen Merkmalen ab. 10 Mbps 2000000 100 Mbps 200000
Edge	Auto- Automatische Erkennung True Port ist ein Edge Port False Port ist kein Edge Port

4.3 QinQ

Hinweis: QinQ ist nur im Router Modus und „Tag-Base“ Modus verfügbar

QinQ ist eine Änderung der IEEE 802.1Q-Spezifikation, mit der mehrere VLAN-Tags in einen einzelnen Ethernet-Frame eingefügt werden können.

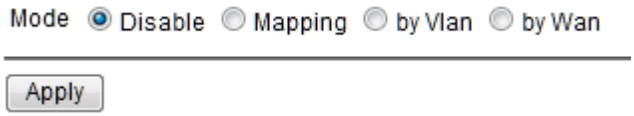
Im Gerät unterstützt QinQ die Konvertierung von Einzel-Tag-Paketen der LAN Seite in Doppel-Tag-Paketausgaben auf der WAN Seite. Der Ausgangs-S-Tag- und C-Tag-Wert hängt vom QinQ-Modus ab.

Deaktiviert	QinQ ist deaktiviert
Mapping	Sowohl S-Tag als auch C-Tag hängen vom eingehenden VID-Wert ab.

VLAN	Das C-Tag entspricht der Eingangs-VID.
WAN	Das S-Tag hängt von der Eingangs-VID ab.

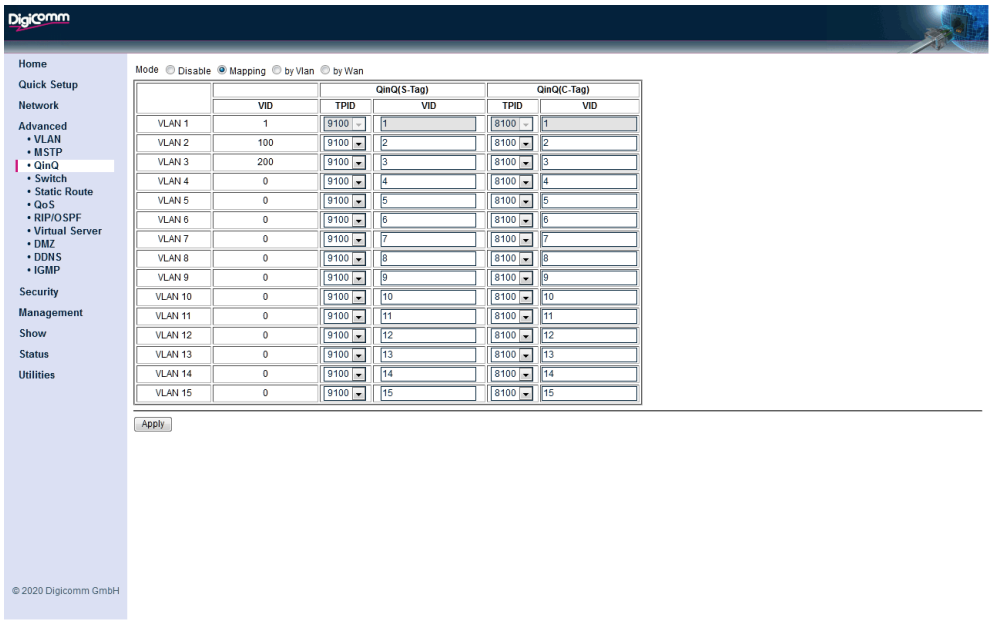
4.3.1 QinQ/ Disable

Klicken Sie auf die Option „Disable“ um QinQ zu deaktivieren



4.3.2 QinQ/ Mapping

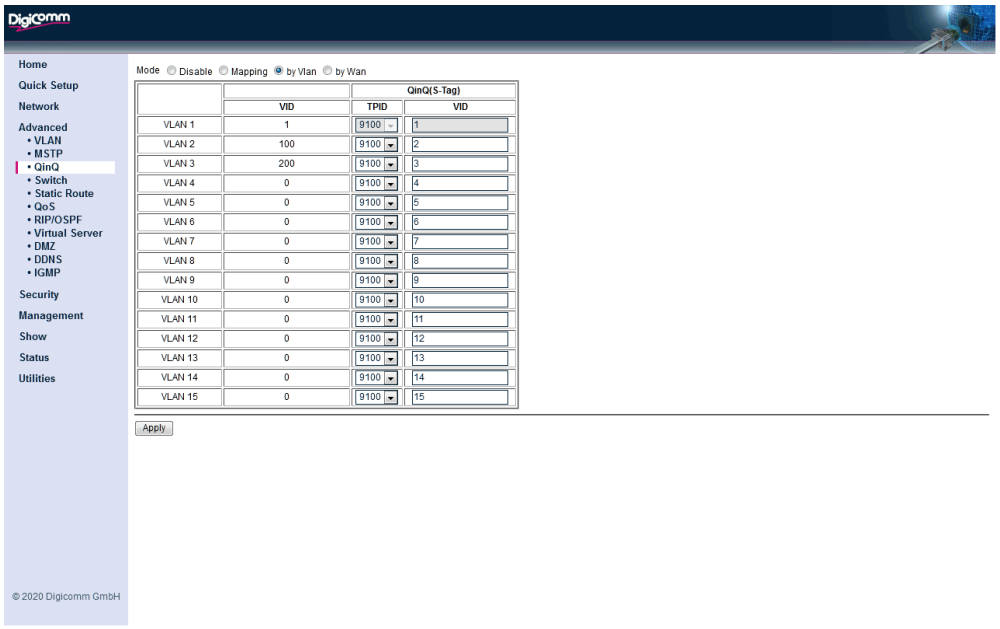
Klicken Sie auf die Option „Mapping“ um den QinQ Mapping Modus zu aktivieren



S-Tag/ TPID	Geben Sie die TPID für den S-Tag ein
S-Tag/VID	Geben Sie die VID für den S-Tag ein
C-Tag/TPID	Geben Sie die TPID für den C-Tag ein
C-Tag/VID	Geben Sie die VID für den C-Tag ein

4.3.3 QinQ/ by VLAN

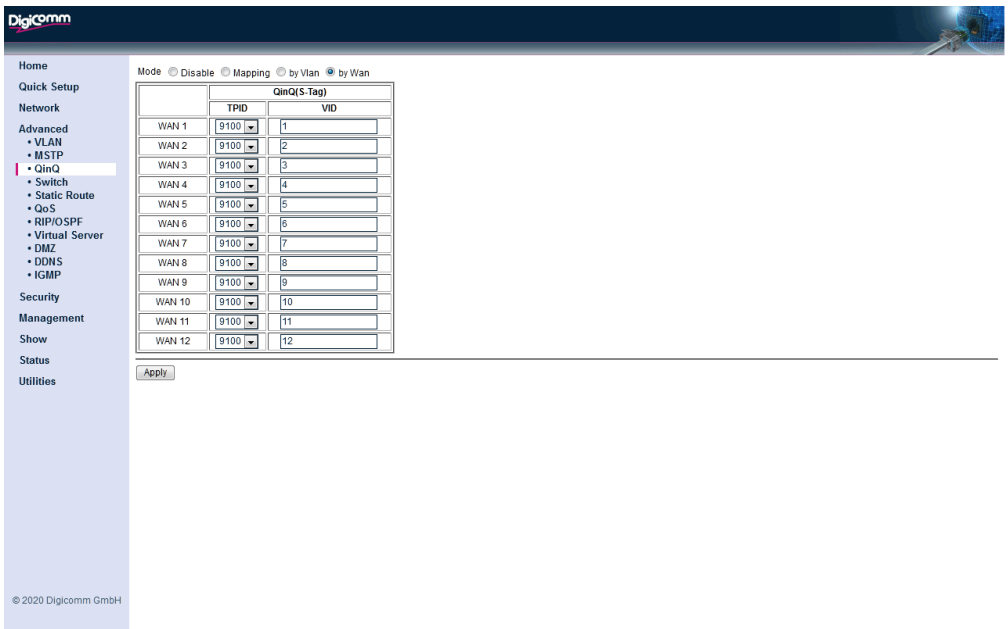
Klicken Sie auf die Option „by Vlan“ um den VLAN Modus im QinQ zu aktivieren.



S-Tag/ TPID Geben Sie die TPID für den S-Tag ein
S-Tag/ VID Geben Sie die VID für den S-Tag ein

4.3.4 QinQ/ by WAN

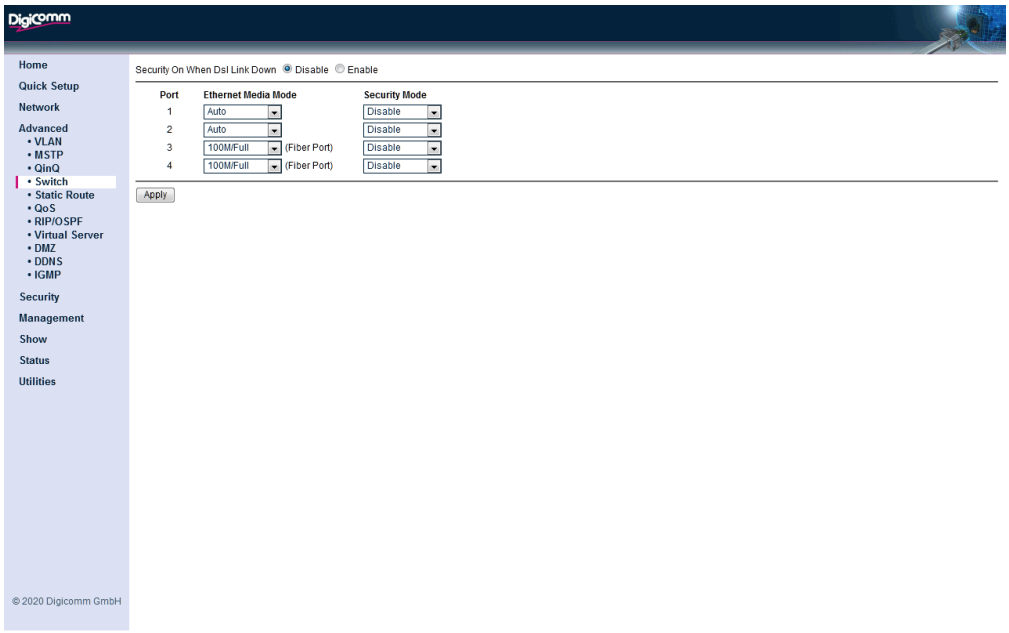
Klicken Sie auf die Option „by WAN“ um den WAN Modus im QinQ zu aktivieren.



S-Tag/TPID Geben Sie die TPID für den S-Tag ein
S-Tag/VID Geben Sie die VID für den S-Tag ein

4.4 Switch

Der Switch ermöglicht die Steuerung der Ethernet- / SFP-LAN-Ports des SHDTU.
Sie können die Geschwindigkeit / Duplex einstellen oder die Ports deaktivieren.

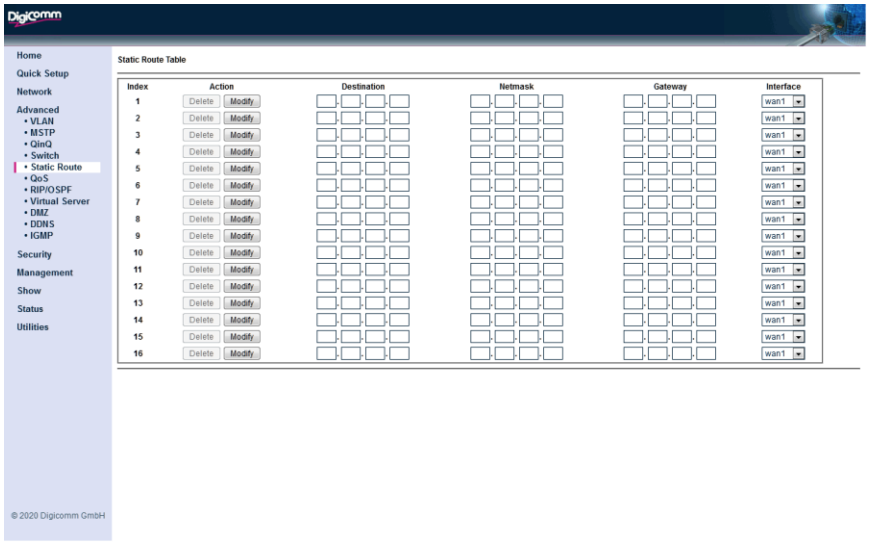


Security On When DSL Link Down	Deaktiviert –Wenn alle DSL-Links ausgefallen sind passiert nichts. Aktiviert- Wenn alle DSL-Verbindungen unterbrochen sind, sperren sie die Switch-Ports. Wenn der Sicherheitsmodus aktiviert ist und die Verbindung hergestellt ist.
Ethernet Media Mode	Automatisch (Auto), 100M/Full, 100M/Half/, 10M/Full, 10M/Half, Deaktiviert
Security Mode	Deaktiviert- Wenn alle DSL-Links ausgefallen sind passiert nichts. Aktiviert- Port ist gesperrt, wenn die Portverbindung unterbrochen ist

Hinweis: Wenn der Port gesperrt ist, wird der Port heruntergefahren, selbst wenn die Verbindung wiederhergestellt wurde. Der Benutzer muss zuerst den Sperrstatus auf der Seite Status / Switch aufheben.

4.5 Static Route

Hinweis: Static Route ist nur im Router Modus verfügbar.



Bei der Funktion „Static Route“ handelt es sich um einen spezifischen Pfad im Router zu einem bestimmten Subnetz. Eine „Static Route“ wird von Ihrem Netzwerkadministrator manuell installiert.

Im Vergleich zur dynamischen Weiterleitung bieten statische Routen Vorteile wie auch Nachteile.

Vorteile von statischen Routen:

- Einfachere Konfiguration von statischen Routen
- Kein Overhead im Routing-Protokoll erforderlich
- Zuverlässige Sicherheit bei begrenzter IP-Maske

Nachteile von statischen Routen:

- Änderungen am Netzwerk nur durch manuelle Konfiguration der Route möglich
- Kein automatisches Routing bei einem Netzwerkausfall
- Trotz sehr einfacher Konfiguration könnten bei großen und komplexen Netzwerken Probleme auftreten.

Es ist wichtig, dass der entsprechende Netzwerkadministrator umfassende Kenntnisse über statische Routen besitzt. Obwohl diese Art von Routen in großen Netzwerken unter Umständen nicht sehr effektiv ist, sind sie trotzdem in Netzwerken jeder Größe sehr nützlich. Selbst wenn Sie eine dynamische Route eingerichtet haben, gibt es Fälle, für die immer noch eine statische Route erforderlich ist.

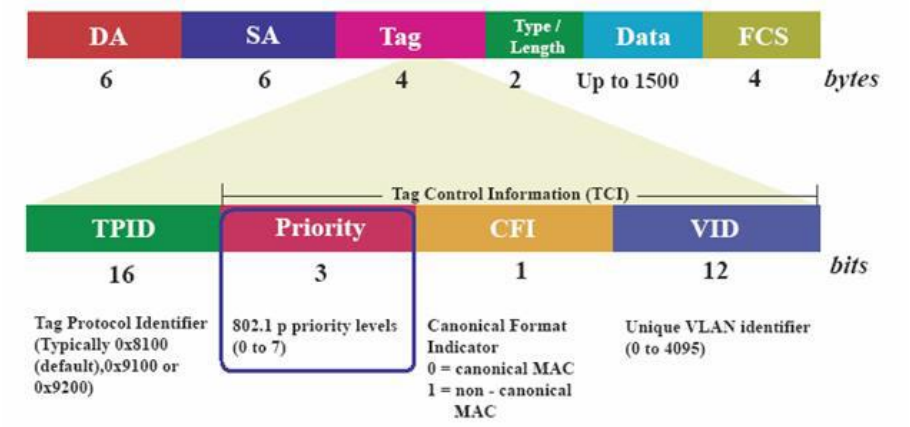
4.6 QoS

Mit „QoS“ (Quality of Service) bezeichnet man die Fähigkeit eines Netzwerks zur Weiterleitung von Daten mit minimaler Verzögerung, auch als „Class of Service“ (CoS) bekannt, sowie die zur Steuerung der Bandbreitennutzung verwendeten Verfahren. Ohne QoS besteht bei einer Überlastung des Netzwerks für jedes Datenpaket eine gleich hohe Wahrscheinlichkeit, dass es verworfen wird. Dies kann zu einer schlechteren Netzwerkleistung führen und zur Folge haben, dass ein Netzwerk für die Übertragung zeitkritischer Anwendungen wie Video-on-Demand als nicht tauglich gekennzeichnet wird.

Mithilfe von QoS (Quality of Service) wird entschieden, welchen PCs Priorität für die Übertragung über das SHDTU eingeräumt wird, sobald die Bandbreite erschöpft oder vollständig belegt ist.

Qos Mode

Disable	Qos ist deaktiviert
WRR	Qos plant nach der WRR-Methode (Weighted Round Robin)
WFQ	Qos plant nach der WFQ-Methode (Weighted Fail Queue)
WRR+SP	Die 1. und 2. Warteschlange werden mit strikter Priorität gesendet. Wenn die 1. und 2 Warteschlange leer ist wird die andere Warteschlange per WRR gesendet.
WFQ+SP	Die 1. und 2. Warteschlange werden mit strikter Priorität gesendet. Wenn die 1. und 2 Warteschlange leer ist wird die andere Warteschlange per WFQ gesendet.



Der 3-Bit-PCP-Wert (Priority Code Point) bietet acht verschiedene Dienstklassen. Die empfohlenen Verwendungen sind in der folgenden Tabelle aufgeführt:

PCP Value	Priority Level	Traffic Type
1	0 (Low)	Background
0	1 (Default)	Best Effort
2	2	Excellent Effort
3	3	Critical applications
4	4	Video
5	5	Video (Low latency and jitter)
6	6	Internetwork control
7	7 8High)	Network Control

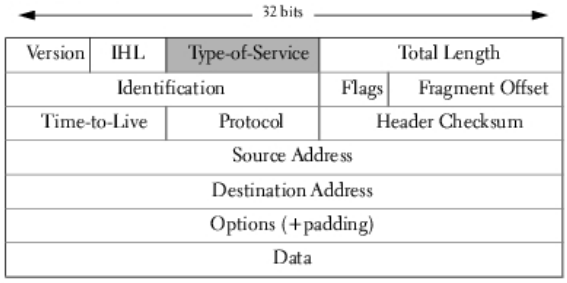
IP DSCP

Bei „Differentiated Services“ (DiffServ) handelt es sich um ein Class of Service (CoS)-Modell zur Verbesserung von Best-Effort-Internet Services anhand der Differenzierung von Traffic nach Benutzern, Serviceanforderungen und anderen Kriterien. Die Datenpakete werden speziell markiert, sodass Netzwerkknoten mittels Prioritäts-Warteschlangenverarbeitung oder Bandbreitenzuordnung unterschiedliche Service-Level anbieten können, die sich jeweils für die Wiedergabe von Video, Sprachanrufen oder andere verzögerungsempfindliche Anwendungen eignen.

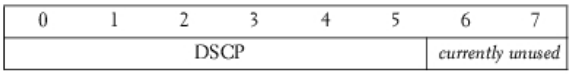
„DiffServ“ definiert im IP-Header ein neues Feld „DS“ (Differentiated Services), das das Feld „Type of Service“ (ToS) ersetzt. Das Feld „DS“ enthält ein nicht verwendetes 2-Bit-Feld sowie ein DSCP-Feld mit 6-Bit, das bis zu 64 Service-Level definieren kann.

Die folgende Abbildung zeigt ein Beispiel für ein DS-Feld:

Ethernet packet header



Type-of-Service Octet for DSCP



Das Gerät bietet eine Zuordnungstabelle von 64 DSCP-Werten zu acht Ausgangswarteschlangen / -klassen. Basierend auf der Shaping-Einstellung für die Ausgangswarteschlange bietet es verschiedene Arten der Prioritäts- / Bandbreitensteuerung für die Weiterleitung.

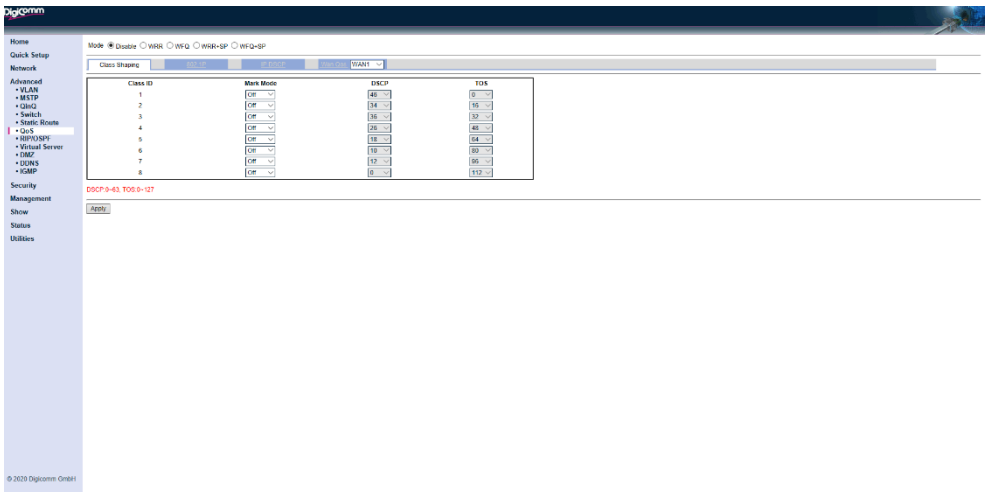
Qos Classify Rule Priority

Das Gerät bietet 3 Klassifizierungsmethoden (802.1P, DSCP und Benutzerregel). Wenn ein Eingangspaket alle Klassifizierungsmethoden trifft, erhalten Sie ein anderes Ergebnis. Das Endergebnis entscheidet anhand der Prioritätsregel.

User Rule >8021.P>DSCP

Beispiel: Ein Eingangspaket, klassifiziert nach Benutzerregel als Klasse 2, klassifiziert nach COS als Klasse 1 und klassifiziert nach DSCP als Klasse 3. Schließlich entscheidet die Benutzerregel, dass das Paket in Klasse 2 klassifiziert wird.

4.6.1 QoS/Class Shaping

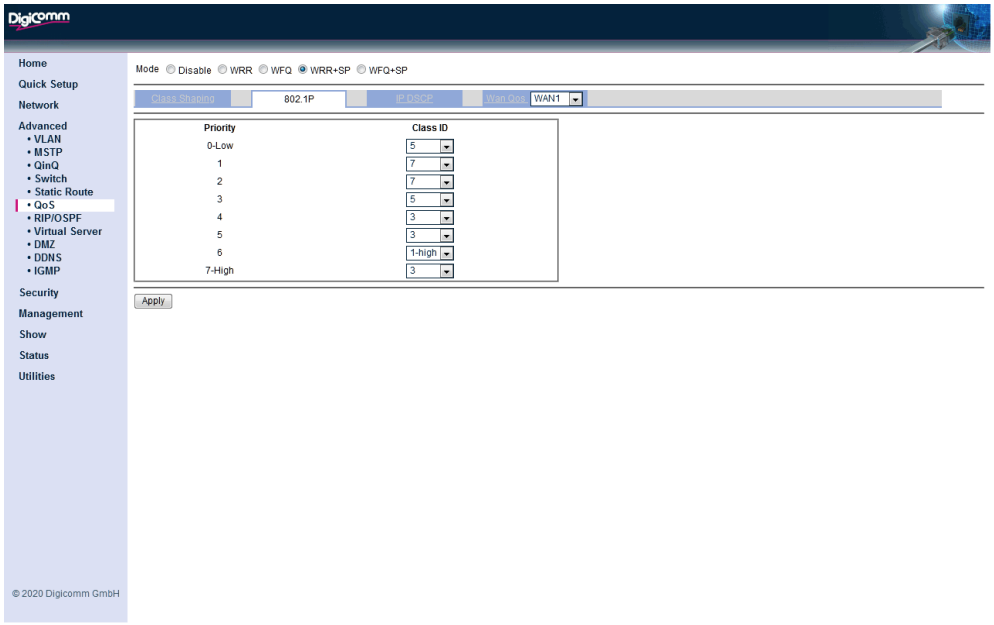


Mark Mode	Off (Aus)	Klassifizierung der Pakete ist deaktiviert.
	DSCP	Tragen Sie den Klassifizierungswert in das DSCP Feld ein um die Position in der Warteschleife zu Kennzeichnen.

	TOS	Tragen Sie den Klassifizierungswert in das TOS Feld ein um die Position in der Warteschleife zu Kennzeichnen
Weight		Der Gewichtungswert für WRR / WFQ

4.6.2 QoS/802.1 P

Stellen Sie 802.1P / PCP des Pakets auf Warteschlangen- / Klassenzuordnungsregeln ein.



4.7 RIP/OSFP

Hinweis: RIP/OSFP ist nur im Router Modus verfügbar.

RIP (Routing Information Protocol)

Das RIP (Routing Information Protocol) ist ein dynamisches Routing-Protokoll, das in lokalen und Weitverkehrsnetzwerken verwendet wird. Es ist ein sehr einfaches Protokoll, das auf Distanzvektor-Routing-Algorithmen basiert. Als solches wird es als IGP (Interior Gateway Protocol) klassifiziert. Der VPN-Router unterstützt Version 1 (RFC1058) und Version 2 (RFC2453).
Es kann die angegebene Schnittstelle (LAN, WAN1 bis WAN12) auf "passiven Modus" setzen. Auf der Schnittstelle im passiven Modus werden alle empfangenden Pakete wie gewohnt verarbeitet und RIP sendet weder Multicast- noch Unicast-RIP-Pakete.

OSFP (Open shortest Path First)

Verbindungsstatus über verfügbare Router und erstellt so eine Topologiekarte des Netzwerks. Die Topologie wird der Internetschicht als Routing-Tabelle zur Verfügung gestellt. So lassen sich Datagramme nur anhand der in den IP-Paketen erkannten Ziel-IP-Adresse weiterleiten. OSPF unterstützt Netzwerke mit Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6). Es bietet als Adressierungsmodelle Variable Length Subnet Masking (VLSM) und Classless Inter-Domain Routing (CIDR).
OSPF erkennt Veränderungen in der Topologie, beispielsweise den Ausfall eines Links, und bündelt den Traffic innerhalb von Sekunden in einer neuen schleifenfreien Weiterleitungsstruktur. Es berechnet den kürzesten Pfad für jede einzelne Route mithilfe eines Verfahrens, das auf dem Dijkstra-Algorithmus basiert, einem Algorithmus zur Berechnung des kürzesten Pfads. OSPF erkennt Veränderungen in der Topologie, beispielsweise den Ausfall eines Links. Die OSPF-Routing-Richtlinien für die Erstellung einer Routing-Tabelle werden durch die Verbindungskosten beeinflusst (externe Metriken), die den einzelnen Routing-Schnittstellen zugeordnet sind. Bei den Kostenfaktoren kann es sich um die Entfernung eines Routers (Round-Trip-Time) handeln, den Datendurchsatz eines Links oder die Verfügbarkeit und Zuverlässigkeit eines Links, die als einfache Zahl ohne Maßeinheit ausgedrückt wird. Daraus ergibt sich ein dynamischer Prozess der

Lastverteilung im Datenverkehr zwischen Routen mit gleichen Kosten.

Die OSPF-Routing-Richtlinien für die Erstellung einer Routing-Tabelle werden durch die Verbindungskosten beeinflusst (externe Metriken), die den einzelnen Routing-Schnittstellen zugeordnet sind. Bei den Kostenfaktoren kann es sich um die Entfernung eines Routers (Round-Trip-Time) handeln, den Datendurchsatz eines Links oder die Verfügbarkeit und Zuverlässigkeit eines Links, die als einfache Zahl ohne Maßeinheit ausgedrückt wird. Daraus ergibt sich ein dynamischer Prozess der Lastverteilung im Datenverkehr zwischen Routen mit gleichen Kosten.
Ein OSPF-Netzwerk kann in Routing-Bereiche strukturiert oder unterteilt werden, um seine Verwaltung zu vereinfachen und eine optimale Ressourcen-Nutzung und Verteilung des Datenverkehrs zu gewährleisten Identifiziert werden die Bereiche anhand von 32-Bit-Zahlen, die ganz einfach in Dezimalschreibweise oder oft auch Oktett-basiert als Dezimalzahlen mit einem Punkt als Trennzeichen, ähnlich der Schreibweise von IPv4-Adressen, notiert werden.

Vereinbarungsgemäß stellt der Bereich 0 (null) oder 0.0.0.0. den Kern- oder Backbonebereich eines OSPF-Netzwerks dar. Die Identifizierung anderer Bereiche kann frei gewählt werden. Oft wählen Administratoren die IP-Adresse eines Haupt-Routers in einem Bereich als die Identifikation für diesen Bereich aus. Jeder zusätzliche Bereich muss eine direkte oder virtuelle Verbindung zum OSPF-Backbonebereich haben. Solche Verbindungen werden über einen sogenannten Bereichsgrenzenrouter (Area Border Router, ABR) gehalten. Ein ABR pflegt separate Verbindungsstatusdatenbanken für alle der von ihm abgedeckten Bereiche. Zudem speichert er zusammengefasst Routen für alle Bereiche des Netzwerks.

Im Gegensatz zu anderen Routing-Protokollen verwendet OSPF kein TCP/ IP Übertragungsprotokoll wie UDP oder TCP. Stattdessen kapselt es seine Daten in IP Datagrammen mit der Protokollnummer 89 ein. Dies ist ein Unterschied zu anderen Routing Protokollen, beispielsweise dem Routing Information Protocol (RIP) und dem Border Gateway Protocol (BGP). Das OSPF implementiert eigene Funktionen zur Fehlererkennung und Korrektur.

Protokollnachrichten

Hallo

Hallo-Nachrichten werden oft als Begrüßung verwendet, um einem Router die Erkennung benachbarter Router in Netzwerken und an lokalen Links zu ermöglichen. Diese Nachrichten dienen dazu, Beziehungen zwischen benachbarten Geräten herzustellen (sogenannte „Adjacencies“) und Schlüsselparameter im Hinblick auf die Verwendung von OSPF im autonomen System oder Bereich auszutauschen.

Datenbankbeschreibung

Nachrichten zur Datenbankbeschreibung enthalten Beschreibungen der Topologie des autonomen Systems oder Bereichs. Sie übermitteln die Inhalte der Link-State Database (LSDB) für den Bereich von einem Router zum nächsten. Für die Übermittlung einer umfangreichen LSDB sind unter Umständen mehrere Nachrichten erforderlich. Das sendende Gerät muss hierfür als Master festgelegt sein und die Nachrichten in Folge versenden. Der Slave (Empfänger der LSDB-Informationen) antwortet mit Bestätigungen.

Anforderung des Verbindungsstatus

Mithilfe dieser Nachrichten fordert ein Router aktualisierte Informationen über einen Teil der LSBD von einem anderen Router an. Die Nachricht gibt präzise an, zu welchen Links das Gerät, das die Anforderung versendet, weitere Informationen benötigt.

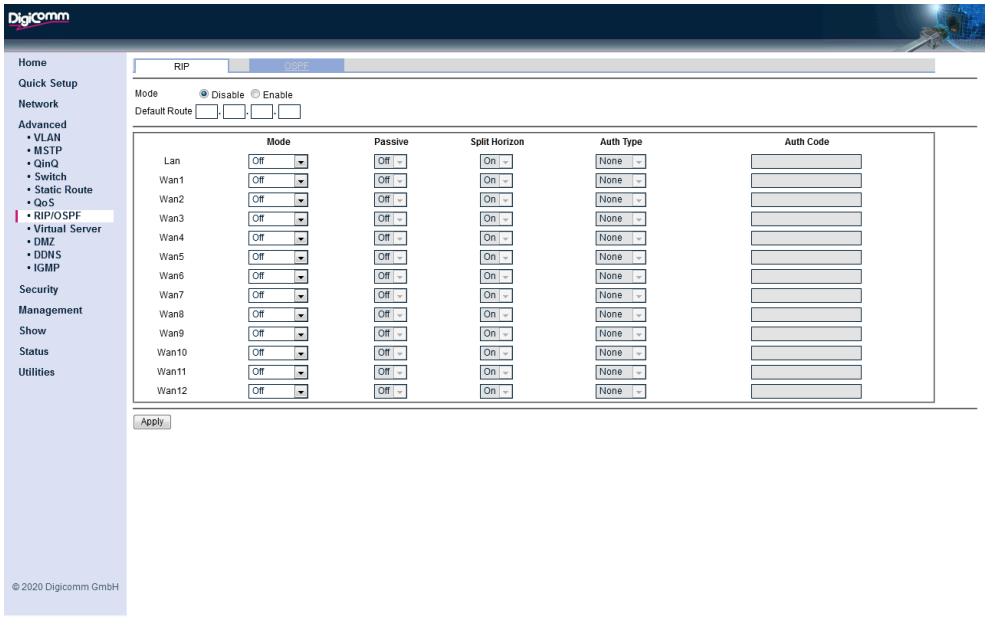
Aktualisierung des Verbindungsstatus

Diese Nachrichten enthalten aktualisierte Informationen über den Verbindungsstatus bestimmter Links in der LSDB. Sie werden als Antwort auf eine Anforderung des Verbindungsstatus versendet und auch in regelmäßigen Abständen von Routern als Broadcast oder Multicast. Mithilfe ihres Inhalts können Router, die diese Nachrichten empfangen, ihre LSDBs aktualisieren.

Bestätigung des Verbindungsstatus

Diese Nachrichten gewährleisten die Zuverlässigkeit des Austauschprozesses, indem sie ausdrücklich den Erhalt einer Nachricht zur Aktualisierung des Verbindungsstatus bestätigen.
RIP/ OSPF ist im „Bridge-Modus“ nicht verfügbar. Anhand der folgenden Anleitung ist ein Zurücksetzen in den „Router-Modus“ möglich.
Öffnen Sie die Funktion „Quick Setup“, klicken Sie auf das Kontrollkästchen „Router“ und anschließend auf „Abschicken“.

4.7.1 RIP



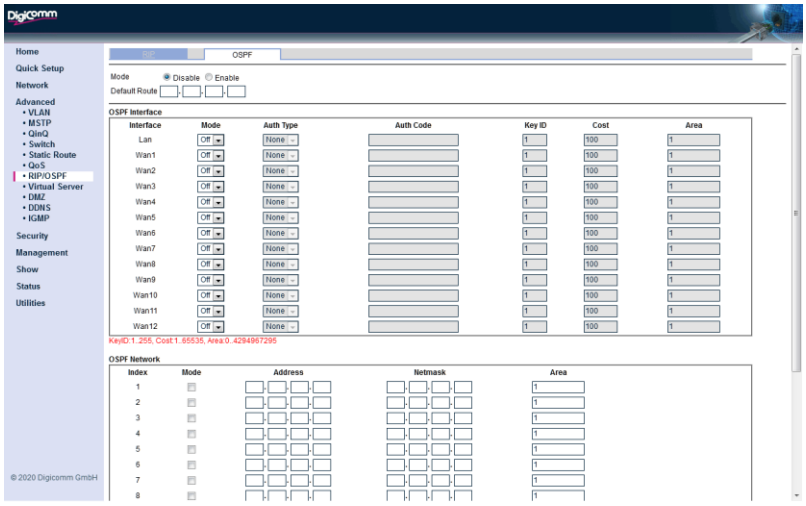
RIP Parameter

Mode	Aktivieren/ Deaktivieren RIP Protocol
Default Route	RIP verteilt die Pakete an diese Adresse, wenn der Modus aktiviert wurde.

RIP Eingabeparameter

Mode	Aus (Off)/ Version 1/ Version 2
Passive	RIP sendet keine Informationen in der Schnittstelle, wenn der Modus aktiviert ist.
Split Horizon	Wenn Split Horizon eingeschaltet ist, sendet das SHDTU keine Updates über das Interface, von welchem es die Netze gelernt hat.
Auth Type	None, Simple und MD5. Deaktiviert/ Aktiviert RIP Authentifikation.
Auth Code	RIP Authentifizierungs Code

4.7.2 OSPF



OSPF Parameter

Mode	Aktivieren/ Deaktivieren des OSPF Protokolls
Default Route	OSPF verteilt die Pakete an diese Adresse, wenn der Modus aktiviert wurde.

OSPF Schnittstellen Parameter

Mode	OSPF tauscht keine Routing-Informationen in der Schnittstelle aus, wenn der Modus ist nicht aktiviert ist.
Auth Type	None/MD5. Deaktiviert/ Aktiviert OSPF Authentifikation in der Schnittstelle
Auth Code	OSPF Authentifikations Code
Key ID	Der Schlüsselindex für die OSPF-Authentifizierung 1 bis255.
Cost	Route Path Cost 1 bis 65535
Area	Area ID, 0 bis 4294967295

OSPF Network Parameter

Mode	Wenn dieser Modus aktiviert ist, verteilt OSPF die eingetragenen Informationen
Address	Netzwerk IP Adresse
Netmask	Netzwerk IP Subnet Mask
Area	Netzwerksbereichs ID

4.8 Virtual Server

Hinweis: Virtual Server ist nur im Router Modus verfügbar

Mithilfe dieser Funktion können Sie den Zugriff auf die Server in Ihrem LAN für Benutzer über das Netzwerk erlauben. Normalerweise können Benutzer nicht über das Netzwerk auf einen Server in Ihrem LAN zugreifen. Gründe hierfür:

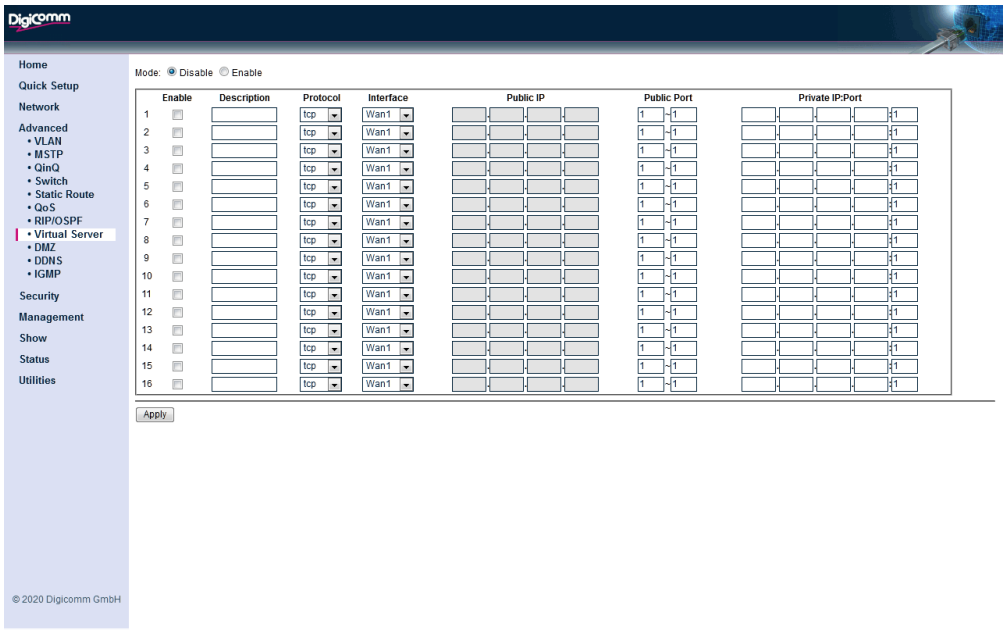
(1) Ihre Server besitzen keine gültige externe IP-Adresse.

(2) Der Versuch eines Zugriffs auf Geräte in Ihrem LAN, über die einem Benutzer im Netzwerk angezeigte IP-Adresse, wird durch die Firewall in diesem Gerät blockiert.

Für Benutzer im Netzwerk besitzen alle virtuellen Server in Ihrem LAN die gleiche IP-Adresse. Die IP-Adresse wird durch Ihren Internetanbieter zugewiesen. Normalerweise handelt es sich um eine statische Adresse, die es Benutzern im Netzwerk erleichtert, eine Verbindung zu Ihren Servern herzustellen. Im Anschluss an die Konfiguration kann jeder Benutzer im Netzwerk eine Verbindung zu Ihren virtuellen Servern herstellen.

Entscheiden Sie als erstes, ob Sie die Funktion für virtuelle Server aktivieren oder deaktivieren möchten. Falls Sie sich für die Aktivierung dieser Funktion entscheiden, müssen Sie festlegen, wie viele Server Sie verwenden

möchten (maximal: 16 Server). Sie müssen die Daten für diesen Server festlegen, beispielsweise Schnittstelle (welcher WAN Port), Protokoll (TCP oder UDP), öffentlicher Port-Bereich sowie die private IP-Adresse und deren Port-Nummer. Achten Sie darauf, das entsprechende Kontrollkästchen zu aktivieren, um die Aktivierung des ausgewählten virtuellen Servers zu ermöglichen. Klicken Sie abschließend auf die Schaltfläche „Apply“ um die Änderungen zu übernehmen.



Virtual Server Parameter

Mode Aktivieren/ Deaktivieren Virtual Server

Virtual Server Eintragsparameter

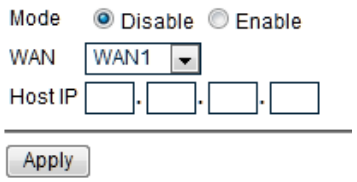
Enable	Aktivieren/ Deaktivieren den Eintrag
Description	Benutzerdefinierter Kommentar für den Eintrag
Protocol	Unterstützt ICMP/TCP/IP
Public IP	Die globale / öffentliche IP-Adresse für Internetnutzer.
Public Port	Der globale / öffentliche TCP / UDP-Port für Internetnutzer.
Private IP Port	Die IP-Adresse des lokalen / privaten Servers / Hosts und der TCP / UDP-Port

4.9 DMZ

Hinweis: DMZ ist nur im Router Modus verfügbar

In der Computersicherheit ist DMZ (entmilitarisierte Zone) ein physisches oder logisches Teilnetzwerk, das die externen Dienste eines Unternehmens enthält und einem größeren nicht vertrauenswürdigen Netzwerk, normalerweise dem Internet, aussetzt. Der Begriff wird von IT-Fachleuten normalerweise als DMZ bezeichnet. Es wird manchmal als Perimeter-Netzwerk bezeichnet. Der Zweck einer DMZ besteht darin, dem LAN (Local Area Network) einer Organisation eine zusätzliche Sicherheitsebene hinzuzufügen. Ein externer Angreifer hat nur Zugriff auf Geräte in der DMZ und nicht auf andere Teile des Netzwerks.

Wenn DMZ aktiviert ist, wird der gesamte Datenverkehr zum DMZ-WAN / IF zur Host-IP umgeleitet.



DMZ Parameter

Mode	Aktivieren /Deaktivieren DMZ
WAN/ IF	WAN eingehende Schnittstelle für DMZ Zugriff
Host IP	Host für DMZ-Umleitungsziel

4.10 DDNS

Mit DDNS (Dynamic DNS Free) kann der Benutzer einen Hostnamen erstellen, der auf das Gerät verweist und eine leicht zu merkende URL für den schnellen Zugriff bereitstellt.
Um es nutzen zu können, musste der Benutzer den Dienst bei den aufgeführten DDNS-Dienstanbietern anwenden / registrieren.

Wenn DDNS aktiviert ist, aktualisiert das Gerät die IP-Adresse auf dem DDNS-Server regelmäßig. Um es zu aktualisieren, müssen Sie den Hostnamen, den Benutzernamen und das Kennwort angeben, mit denen der der Dienst auf dem Server registriert ist.

DDNS Parameters

Mode	Aktivieren/Deaktivieren DDNS
Provider	DDNS Service Provider
Host Name	Vom Benutzer registrierter Hostname
User Name	Benutzername, mit dem der Dienst beim Anbieter registriert wird
Password	Benutzerkennwort, mit dem der Dienst beim Anbieter registriert wird

4.11 IGMP

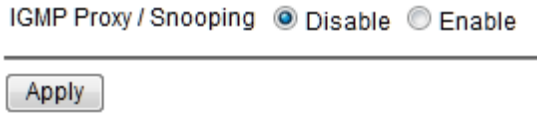
IGMP (Internet Group Management Protocol)-Proxy ermöglicht die Implementierung von Multicast-Routing. Dies funktioniert über die IGMP-Frame-Weiterleitung. Das IGMP-Proxy des SHDTUs unterstützt IGMP Version 2 (RFC2236). IGMP-Proxy ermöglicht dem System den Versand von IGMP-Host-Nachrichten im Namen des Hosts, den das System über die Standard-IGMP-Schnittstellen erkannt hat. Das System fungiert als Proxy für seine Hosts.

Das IGMP-Snooping dient zum „Abhören“ von IGMP-Netzwerkverkehr. Wie schon der Name verrät, handelt es sich bei „IGMP-Snooping“ um eine Funktion, die dem SHDTU das „Abhören“ der IGMP-Kommunikation zwischen Hosts zu diesem SHDTU ermöglicht. Hierfür werden die in ein Multicast-Netzwerk gesendeten IGMP-Pakete verarbeitet. Ist diese Funktion aktiviert, analysiert das SHDTU sämtliche IGMP-Pakete zwischen den an dieses SHDTU angeschlossenen Hosts und Multicast-Routern im Netzwerk.

Wenn das SHDTU einen IGMP-Bericht von einer Remote-Einheit an eine bestimmte Multicast-Gruppe abhört, fügt das SHDTU die Port-Nummer der Multicast-Liste dieser Gruppe hinzu. Ebenso entfernt das SHDTU den Host-Port wieder aus der Tabelle, wenn er erkennt, dass ein IGMP die Verbindung löst.

IGMP Parameter

Mode Aktivieren/ Deaktivieren IGMP Proxy/ Snooping



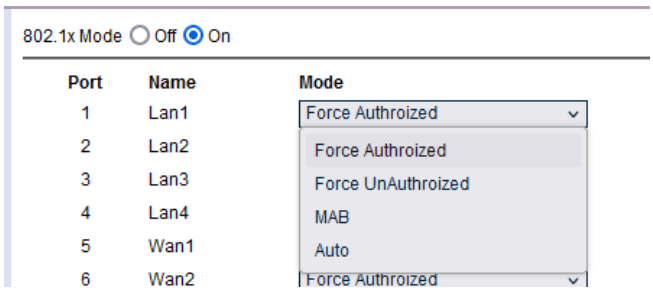
4.12 Dot1x

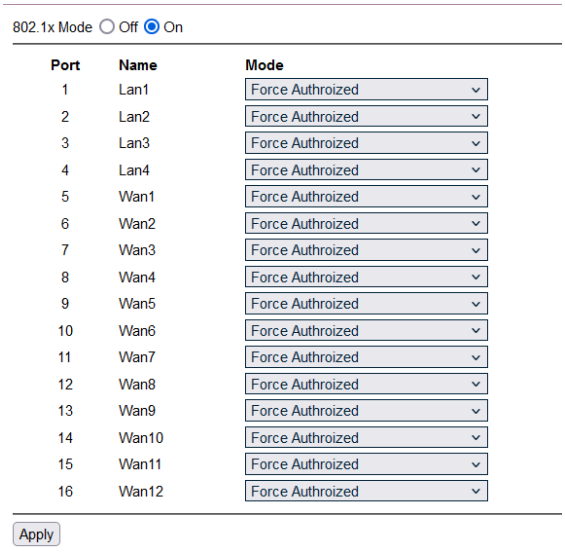
Um den nicht autorisierten Zugriff von Außenstehenden zu vermeiden, kann der 802.1x-Modus nach IEEE-Standard über Dot1x aktiviert werden. 802.1x ist eine generelle Methode bzw. eine Kontrollinstanz, die den Anwender überprüft, bevor dieser auf das LAN- oder WLAN-Netzwerk zugreift.

Der Benutzer wird am Netzwerkzugang, beispielsweise am LAN-Port, durch den Authenticator authentifiziert. Der Authenticator übermittelt die Authentifizierungsinformationen anschließend an den RADIUS-Server (auch als Authentifizierungsserver bezeichnet), der diese prüft. Der Zugriff wird daraufhin zugelassen oder abgelehnt. Für die Nutzung ist ein RADIUS-Server oder ein vergleichbares System erforderlich. Im Kapitel 6.2 „AAA“ wird der RADIUS-Server näher beschrieben.

Die Entscheidung, welche Einstellung angewendet werden soll, liegt beim Nutzer. Die Voreinstellung lautet „Force Authorized”, wodurch dem Benutzer stets Zugriff gewährt wird. Die andere Option ist „Force Unauthorized”. Hier wird selbst bei korrekten Authentifizierungsinformationen der Zugriff verweigert. Um den Zugriff auf bestimmte Benutzer zu beschränken, gibt es die Auto-Einstellung. Bei einer erfolgreichen Authentifizierung wird der Zugriff gewährt, bei einem nicht erfolgreichen Versuch wird der Zugriff verweigert. Falls das Gerät nicht über 802.1x verfügt, kann die MAB-Option (Mac-Authentication-Bypass) verwendet werden. Hierbei wird die MAC-Adresse des Gerätes verwendet, um die Art des Netzwerkzugriffs zu bestimmen.

Hinweis: Wenn 802.1x aktiviert ist, funktionieren die Ringprotokolle nicht.





5 Security

Im Menü „Security“ (Sicherheit) werden folgende Funktionen konfiguriert.

1. Firewall
2. VPN
3. OPENVPN #01
4. OPENVPN #02
5. OPENVPN #03
6. OPENVPN #04
7. OPENVPN #05
8. OPENVPN #06
9. OPENVPN #07
10. OPENVPN #08
11. OPENVPN #09
12. OPENVPN #10
13. OPENVPN Filter
14. Filter

5.1 Firewall

Eine Firewall besteht aus einer Reihe von Programmen, die den Schutz der Ressourcen eines privaten Netzwerks gegenüber anderen Netzwerken gewährleisten. Benutzer können damit verhindern, dass ein Hacker auf ihre eigenen privaten Datenressourcen zugreifen kann.

Die Firewall bietet drei verschiedene Sicherheitsstufen: Grundlegende Firewall-Sicherheit, automatische Firewall-Sicherheit und erweiterte Firewall-Sicherheit.

Xmas tree scan: Hier kann ein TCP-Frame mit gesetzten URG-, PUSH- und FIN-Flags an ein Remote-Gerät gesendet werden. Dies wird als „Xmas-Tree-Scan“ bezeichnet, da die alternierenden Bits im Byte der Flags ein- und ausgeschaltet werden, ganz ähnlich der Beleuchtung eines Weihnachtsbaums.

Null scan: Bei einem Null-Scan werden alle Flags ausgeschaltet, was zu einem Mangel an TCP-Flags führt, der in der Realität niemals auftreten kann.

SYN flood: Bei einer SYN-Flood handelt es sich um eine Variante einer Denial-of-Service (DoS)-Attacke, die zum Ziel hat, die Leistung Ihres Netzwerks zu verringern, indem neue Verbindungen angefordert werden, ohne den Vorgang zum Aufbau einer angeforderten Verbindung abzuschließen. Sobald der Puffer für diese ausstehenden Verbindungen voll ist, akzeptiert der Server keine weiteren Anforderungen und reagiert in der Folge nicht mehr.

ICMP flood: Ein Sender überträgt ein hohes Volumen an ICMP-Anforderungspaketen, um sämtliche CPU-Ressourcen auf die Verarbeitung dieser falschen Anforderungen zu konzentrieren.

UDP Flood: Eine UDP-Flood ist eine weitere Variante einer Denial-of-Service (DoS)-Attacke, die über das User Datagram Protocol (UDP) erfolgt. Ein Sender überträgt ein hohes Volumen an Anforderungen für UDP-Diagnosedienste, um sämtliche CPU-Ressourcen auf die Verarbeitung dieser falschen Anforderungen zu konzentrieren.

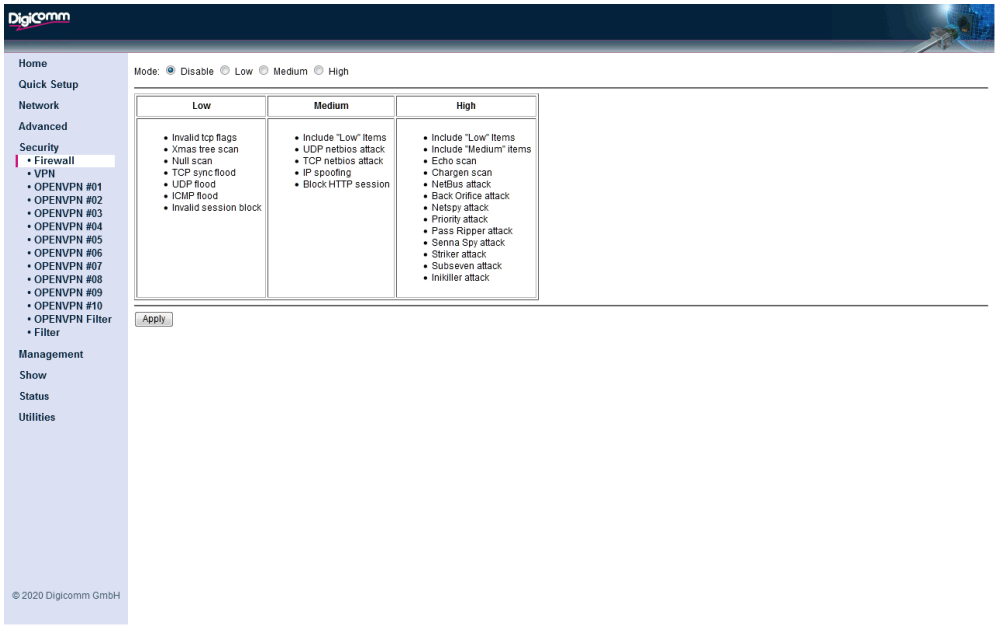
Ping of Death: Bei einer Ping-of-Death (POD)-Attacke versucht der Angreifer Ihr System zum Absturz zu bringen, indem er ein fragmentiertes Paket sendet, dessen Größe bei der Reassemblierung den maximal zulässigen Wert übersteigt.

Land attack: Die Land-Attacke hat zum Ziel, die Leistungsfähigkeit Ihres Netzwerks zu beeinträchtigen. Hierfür wird ein Paket versendet, dessen Quell- und Zieladresse identisch ist und aus Ihrem Netzwerk stammt.

IP Spoofing: Das IP-Spoofing ist ein Verfahren zum Verbergen der Identität eines Eindringlings in Ihr Netzwerk, indem es vorgibt, dass der Traffic von einem anderen Computer stammt. Dieses Verfahren wird von einem Angreifer zur Wahrung seiner Anonymität verwendet und kann auch bei einer DoS-Attacke eingesetzt werden.

Smurf attack: Eine Smurf-Attacke dient dazu, auf Seiten des angegriffenen Hosts ein hohes Volumen an Netzwerkdatenverkehr zu generieren. Es handelt sich hierbei um eine Variante einer Denial-of-Service (DoS)-Attacke. An einer Smurf-Attacke sind zwei Systeme beteiligt. Der Angreifer sendet ein Paket mit einem ICMP Echo Request (Ping) an die Netzwerkadresse eines anderen Systems. Dieses System wird als „Amplifier“ (Verstärker) bezeichnet. Die Antwortadresse für den Ping wurde gefälscht, sodass es aussieht, als käme der Ping von einer Maschine in einem anderen Netzwerk (das Angriffsziel). In der Folge wird das Angriffsziel mit einer hohen Zahl an Antworten auf den Ping überflutet. Ein einzelner Angriff generiert dabei bereits eine hohe Zahl an Antworten und der Angreifer ist in der Lage, viele Verstärker auf das gleiche Ziel anzusetzen.

Fraggle attack: Ein Fraggle-Angriff ist ebenfalls eine Variante einer Denial-of-Service Attacke, bei der ein Angreifer ein hohes Volumen an UDP Echo Traffic an IP Broadcast Adressen sendet, die alle über eine gefälschte Quelladresse verfügen. Hierfür muss der Code einer Smurf-Attacke nur leicht verändert werden.



Firewall Parameter

Mode	Disable (Deaktivieren), Low (niedrig), Medium (Mittelwert) und High (hoch) können konfiguriert werden.

5.2 VPN

Ein VPN (Virtual Private Network) bietet eine sichere Verbindung zwischen zwei Punkten über ein unsicheres Netzwerk. Diese sichere Verbindung wird als VPN-Tunnel bezeichnet. Der VPN-Router unterstützt drei wichtige Varianten von VPN: IPsec, L2TP und PPTP.

5.2.1 VPN/ IPSec

Klicken Sie auf die Option „IPSec“ um die IPSec Konfigurationsseite aufzurufen.

IPsec ist ein flächendeckend verbreiteter VPN-Sicherheitsstandard, der für TCP/ IP Netzwerke entwickelt wurde. Er setzt auf Paketebene an und authentifiziert sowie verschlüsselt alle Pakete, die über den VPN-

Tunnel versendet werden. Es spielt daher keine Rolle, welche Anwendungen auf Ihrem PC verwendet werden. Jede Anwendung ist in der Lage, VPN wie eine normale Netzwerkverbindung zu nutzen.

IPsec VPNs tauschen Informationen über logische Verbindungen aus, die man als SAs (Security Associations) bezeichnet. Bei einer SA handelt es sich ganz einfach um eine Definition von Protokollen, Algorithmen und Schlüsseln, die von zwei VPN-Geräten (Endpunkten) verwendet werden.

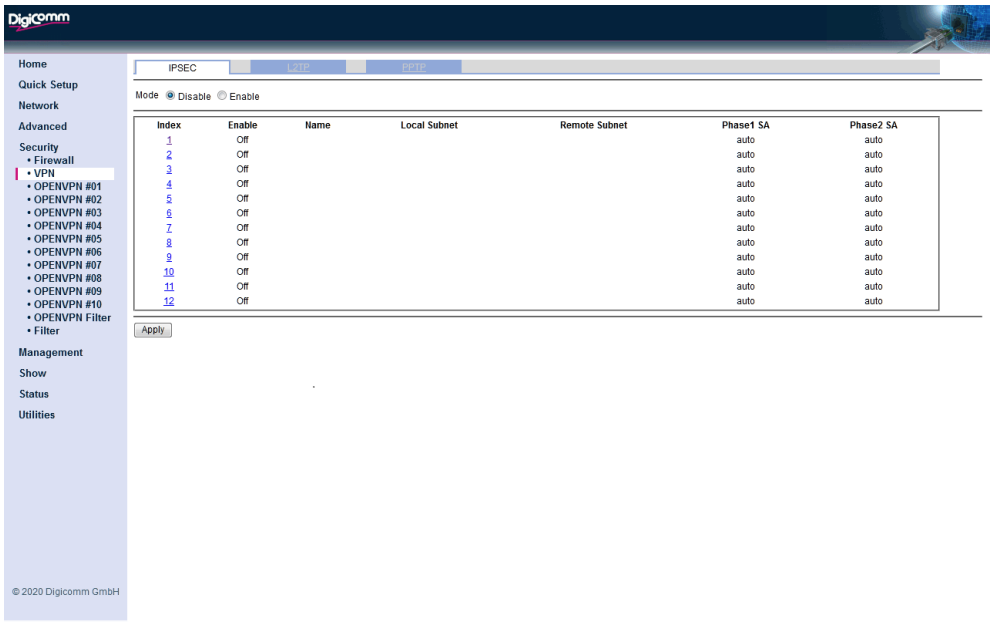
Bei IPsec sind zwei Sicherheitsmodi möglich:

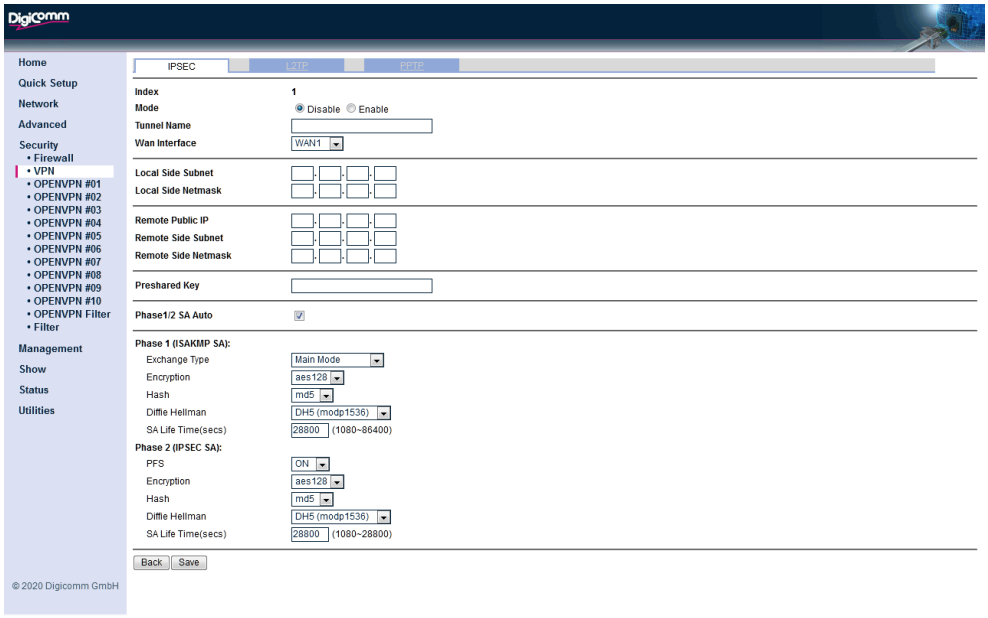
Transport-Modus: die Nutzdaten des Pakets werden mithilfe von Verschlüsselung eingekapselt, während der IP-Header unverschlüsselt (unverändert) bleibt.

Tunnel-Modus: sämtliche Daten, einschließlich des ursprünglichen IP-Headers, werden verschlüsselt und es wird ein neuer IP-Header generiert. Nur der neue IP-Header bleibt unverschlüsselt (d.h. nicht geschützt). Dieses System bietet höhere Sicherheit.

IKE (Interface Key Exchange) ist eine optionale, jedoch häufig verwendete Komponente von IPsec.

IKE bietet ein Verfahren zum Aushandeln und Generieren der Schlüssel und IDs, die von IPsec benötigt werden. Für IKE ist zur Konfiguration nur ein einzelner Schlüssel erforderlich. Darüber hinaus unterstützt IKE die Verwendung von Zertifikaten für die Authentifizierung der Identität eines Remote-Benutzers oder Gateways. Wird IKE nicht verwendet, ist eine manuelle Eingabe aller Schlüssel und IDs (SPIs) erforderlich und es können keine Zertifikate verwendet werden. Dies wird als „Manueller Schlüsselaustausch“ bezeichnet.





IPSec Parameter

Mode Aktivieren /Deaktivieren IPSec

IPSec Einstellungs-Parameter

Mode	IPSec Aktivieren/ Deaktivieren
Tunnel Name	Hier können Sie einen Namen für den Tunnel vergeben
WAN Interface	WAN-Schnittstelle für die IPSec-Verbindung
Local Side Subnet	Die lokale Netzwerk Subnet IP Adresse
Local Side Netmask	Die lokale Netzwerk Subnet Maske
Remote Public IP	Die IP-Adresse der öffentlichen Netzwerkschnittstelle
Remote Side Subnet	Die IP-Adresse des Subnetzes der Remote Seite
Remote Side Netmask	Die Subnet IP-Adresse der Remote Seite
Preshared Key	Vordefinierter Schlüssel der beiden Seiten bekannt ist (Verschlüsselungsverfahren)
Phase 1/ 2 SA Auto	Phase 1&2 SA aktivieren oder deaktivieren

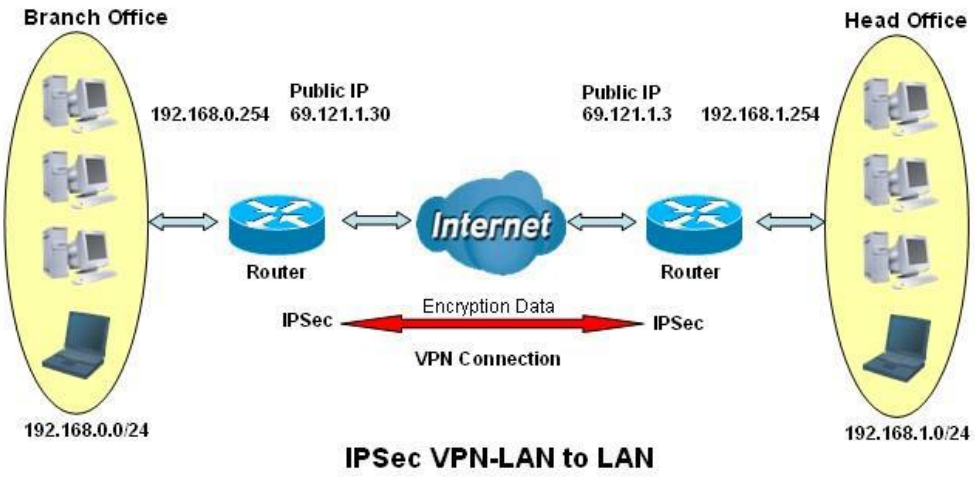
IPSec Einstelllungen Phase 1 Parameter

Exchange Type	Wählen Sie zwischen Main Modus oder Aggressive
Encryption	Unterstützt 3des, aes128, aes192 und aes256
Hash	Unterstützt DH2, 5, 14, 15, 16, 17 und 18
SA Life Time	1080 Sekunden bis zu 86400 Sekunden

IPSec Einstelllungen Phase 2 Parameter

PFS	PFS Aktivieren/ Deaktivieren
Encryption	Unterstützt 3des, aes128, aes192 und aes256
Hash	Unterstützt DH2, 5, 14, 15, 16, 17 und 18
SA Life Time	1080 Sekunden bis zu 86400 Sekunden

Beispiel: Konfigurieren einer IPSec LAN-zu-LAN-VPN-Verbindung



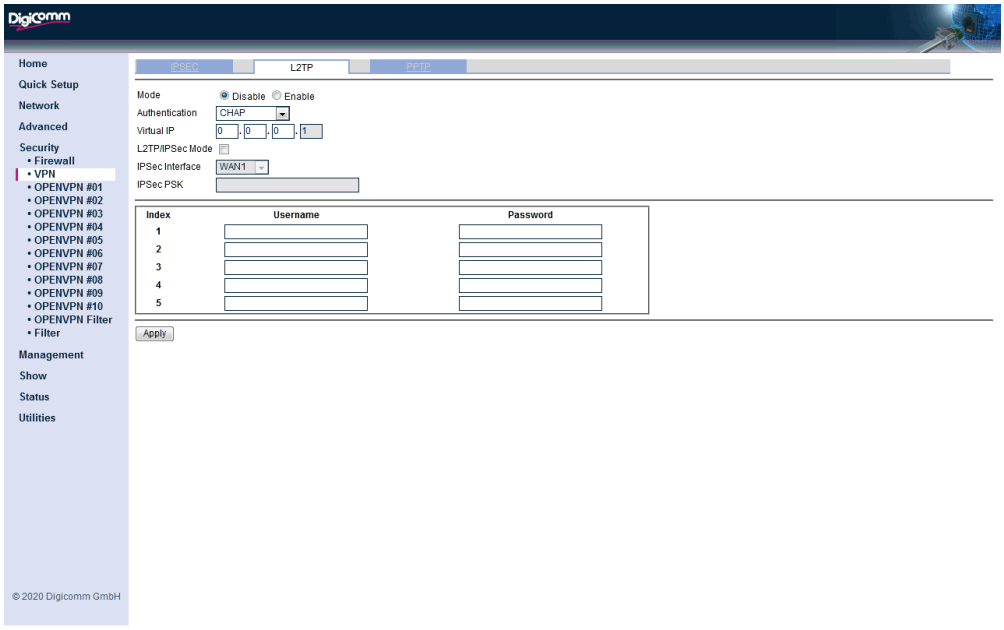
	Außenstelle	Zentrale
Local Side Subnet/Netmask	192.168.0.0./24	192.168.1.0./24
WAN Interface	69.1.121.30	69.1.121.3
Remote Side Subnet/Netmask	192.168.1.0/24	192.168.0.0/24
Remote Public IP	69.1.121.3	69.1.121.30
Preshared Key	12345678	12345678
Hash/Encryption	MD5/AES128	MD5/AES128

5.2.2. VPN/ L2TP (Layer 2 Tunneling Protocol)

Klicken Sie auf die Option „L2TP“ um die VPN/ L2TP Konfigurationsseite aufzurufen.

Bei L2TP (Layer 2 Tunneling Protocol) handelt es sich um ein Tunneling-Protokoll zur Unterstützung von VPNs. Das Protokoll selbst bietet keine Funktionen für Verschlüsselung oder die Gewährleistung der Vertraulichkeit. L2TP ermöglicht die Übertragung einer PPP-Session über mehrere Links und Netzwerke.

PPP wird für die Kapselung der IP-Pakete verwendet, die von einem PC oder mobilen Gerät des Benutzers an den Internetanbieter gesendet werden, und L2TP erweitert diese Session über das Internet.



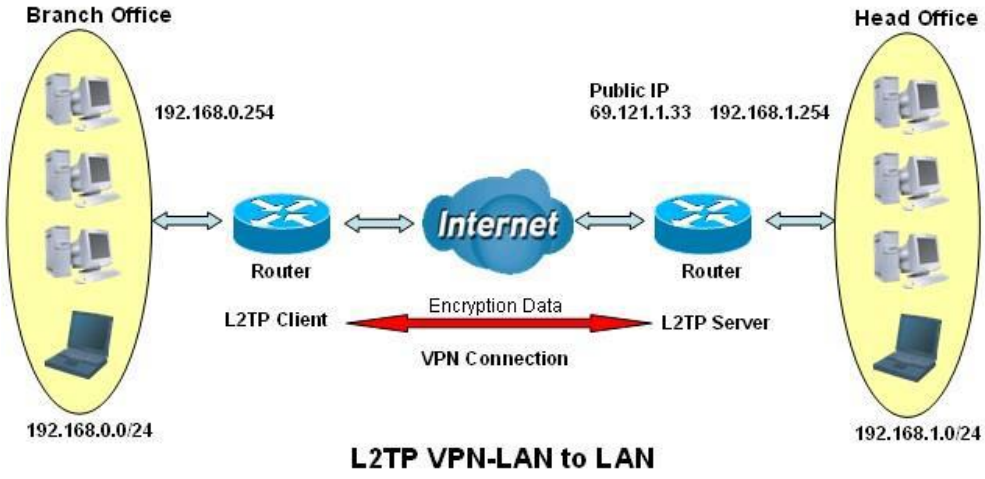
L2TP Parameter

Mode	L2TO Aktivieren/ Deaktivieren
Authentication	Unterstützt PAP, CHAP, MS-CHAP und MS-CHAPV2
Virtual IP	Die virtuelle IP-Startadresse für die Verbindung
L2TP/ IPSec Mode	Aktivieren / Deaktivieren Sie die Verbindung mit der IPSec-Kombination
IPSec Interface	WAN-Schnittstelle für IPSec
IPSec PSK	Pre-Shared Key für IPSec

L2TP Einstellungs-Parameter

Username	L2TP Account/ Username
Password	L2TP Account/ Password

Die Zweigstelle stellt einen L2TP VPN-Tunnel zum Hauptsitz her, um zwei private Netzwerke über das Internet zu verbinden. Die entsprechenden Router sind in der Zentrale und in der Aussenstelle installiert. Beide Netzwerke müssen sich in einem unterschiedlichen Subnetz mit LAN-zu-LAN-Anwendung befinden. Die Funktionen von Pre-Shared Key, VPN und Sicherheitsalgorithmus müssen auf beiden Seiten identisch eingerichtet sein.



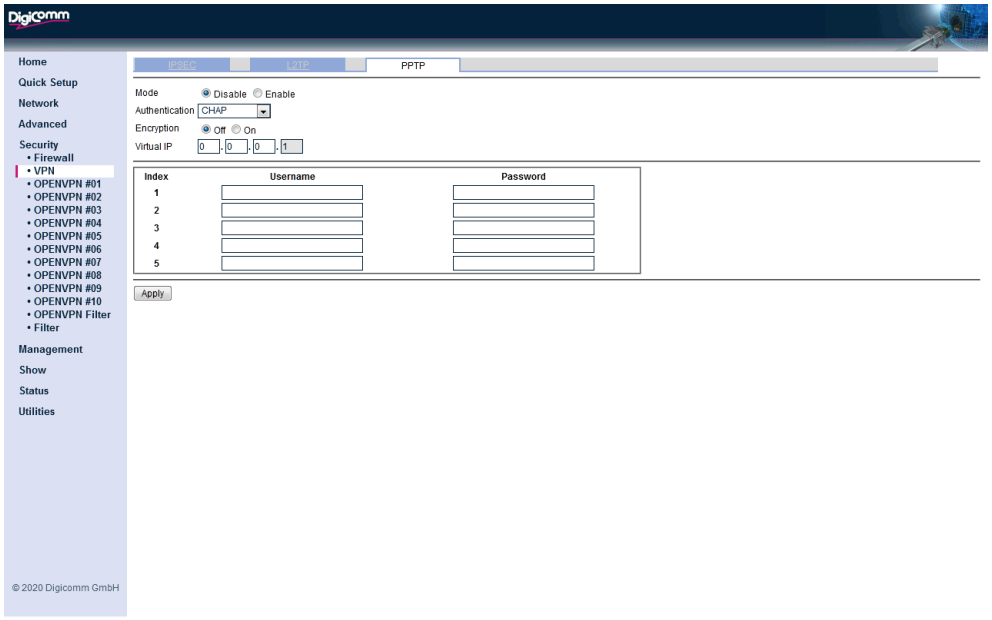
L2TP VPN-LAN to LAN

5.2.3. VPN/ PPTP

Klicken Sie auf die Option „PPTP“ um die VPN/ PPTP Konfigurationsseite aufzurufen.

Das PPTP (Point-to-Point Tunneling Protocol) ist ein privates Computernetzwerk, das mehrere Knoten über das öffentliche Internet verbindet. Da es sich beim Internet im Grunde genommen um ein offenes Netzwerk handelt, wird mithilfe des PPTP gewährleistet, dass die Nachrichten zwischen den VPN-Knoten sicher übertragen werden können. Sie können das PPTP verwenden, um über das Internet eine Verbindung zum Netzwerk Ihres Unternehmens herzustellen.

Es gibt zwei unterstützte PPTP VPN-Varianten: Remote Access und LAN-zu-LAN.



PPTP Parameter

Mode	PPTP aktivieren/ deaktivieren
Authentication	Unterstützt PAP, CHAP, MS-CHAP und MS-CHAPV2
Encryption	Verschlüsselung aktivieren/ deaktivieren
Virtual IP	Die virtuelle IP-Startadresse für die Verbindung

PPTP Einstellungs Parameter

Username	PPTP Username (Benutzername)
Password	PPTP Password (Passwort)

5.3. OpenVPN

OpenVPN ist eine VPN-Technik (Virtual Private Network). Es unterstützt das Erstellen sicherer Punkt-zu-Punkt- oder Standort-zu-Standort-Verbindungen in gerouteten oder überbrückten Konfigurationen und RAS-Einrichtungen. Es verwendet ein benutzerdefiniertes Sicherheitsprotokoll, das SSL/TLS für den Schlüsselaustausch verwendet. Es kann Netzwerkadressübersetzer (NATs) und Firewalls durchlaufen.

Mit OpenVPN können sich Peers gegenseitig mit vorab freigegebenen geheimen Schlüsseln, Zertifikaten oder Benutzernamen / Kennwörtern authentifizieren. Bei Verwendung in einer Multiclient-Server-Konfiguration kann der Server mithilfe von Signaturen und Zertifizierungsstellen ein Authentifizierungszertifikat für jeden Client freigeben. Es verwendet die OpenSSL-Verschlüsselungsbibliothek in großem Umfang sowie das TLS-Protokoll und enthält viele Sicherheits- und Steuerungsfunktionen.

5.3.1 OpenVPN/ Key

VPN-Router unterstützen die OpenVPN-Authentifizierung mit vorinstalliertem Schlüssel und Zertifikaten. Im Servermodus unterstützt der VPN-Router das Erstellen und Verwenden eines selbstsignierten Zertifikats. Der Benutzer kann auch ein CA-signiertes Zertifikat importieren und verwenden.

Erstellen Sie einen Pre-Shared Key auf dem Open VPN Server

Um einen Pre-Shared Key zu erstellen gehen Sie bitte wie folgt vor:

Schritt 1: Stellen Sie sicher, dass die Gerätezeit mit dem PC oder SNTP-Server synchronisiert ist.

Schritt 2: Aktivieren Sie OpenVPN

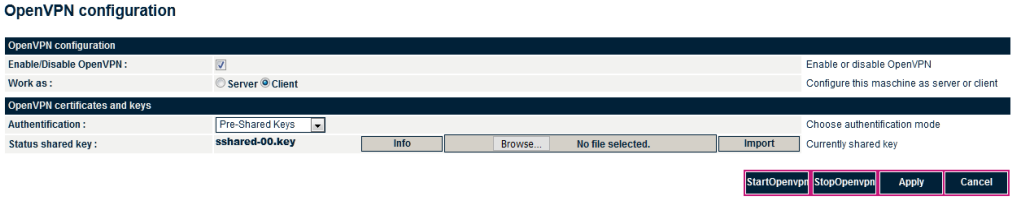
Schritt 3: Wählen Sie unter „Work as“ Server aus

Schritt 4: Wählen Sie bei „Authentication“ Pre-shared Keys aus

Schritt 5: Klicken Sie in der Zeile „Create shared key“ auf den „create-Button“ und bestätigen Sie die Aktion. Danach rufen Sie die Seite erneut auf. In der Zeile „shared key modification“ können Sie die Erstellungszeit des Keys ablesen. Klicken Sie den „Info“ Button um sich den Key anzeigen zu lassen.

Schritt 6: Klicken Sie in der Zeile „Export shared key“ den „Download“ Button. Der Key wir dann heruntergeladen.

Pre-Shared Key auf dem OpenVPN-Client



Schritt 1: Stellen Sie sicher, dass die Gerätezeit mit dem PC oder SNTP-Server synchronisiert ist.

Schritt 2: Aktivieren Sie Open VPN

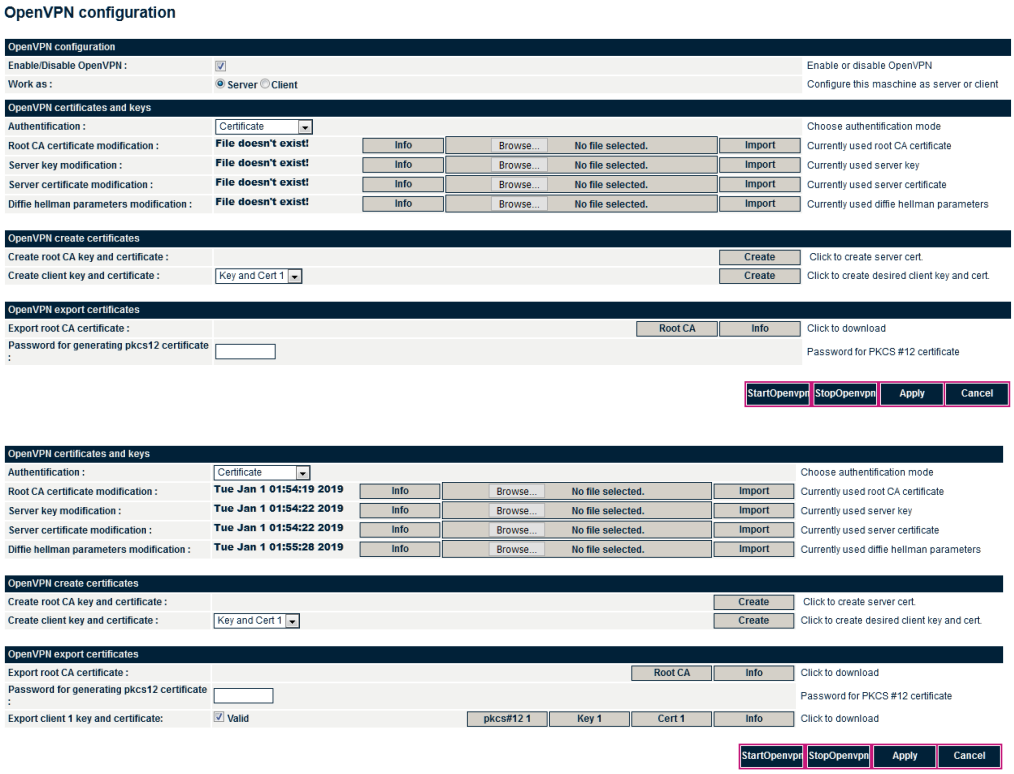
Schritt 3: Wählen Sie unter „Work as“ Client aus.

Schritt 4: Wählen Sie bei „Authentication“ Pre-shared Keys aus

Schritt 5: Klicken Sie in der Zeile „Status shared key“ auf den „Browse“ Button um die Importdatei auszuwählen. Danach klicken Sie auf „Importieren“ um den Key zu importieren.

Nach erfolgreichem Import des Keys, rufen Sie die Seite erneut auf. In der Zeile „Status shared key“ wird Ihnen die importierte Datei angezeigt. Klicken Sie den „Info“ Button um sich den Key anzeigen zu lassen.

Erstellen Sie selbstsignierte Zertifikate



Schritt 1: Stellen Sie sicher, dass die Gerätezeit mit dem PC oder SNTP-Server synchronisiert ist.

Schritt 2: Aktivieren Sie OpenVPN

Schritt 3: Wählen Sie unter „Work as“ Server aus.

Schritt 4: Wählen Sie bei „Authentication“ „Certificate“ aus.

Schritt 5: Klicken Sie in der Zeile „Create root CA key and certificate“ auf den „Create“ Button und bestätigen Sie die Aktion.

Abschließend rufen Sie die Seite erneut auf. In den Zeilen "Root CA certificate modification", "Server key modification“, Server certificate modification“ und „Diffie hellman parameters modification“, können Sie die Erstellungszeit sehen.

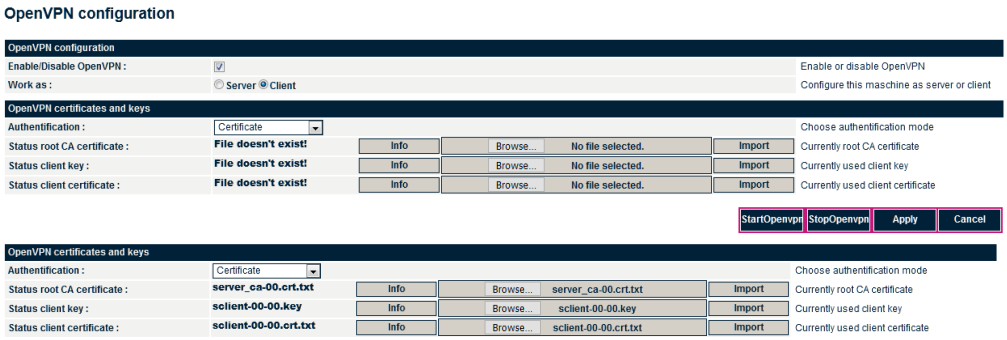
Schritt 6: Geben Sie das Passwort in der Zeile „Password for generarting pkcs 12 certificate“ ein.
Schritt 7: In Zeile „Create client key and certificate“ wählen Sie „Key and Cert 1“ aus. Klicken Sie auf den „Create“ Button und bestätigen Sie die Aktion.

Nach Abschluss wird die Zeile „Export client 1 key and certificate“ angezeigt. Klicken Sie den „Info“ Button um sich den Key anzeigen zu lassen.

Schritt 8: Aktivieren Sie in Zeile "Export client 1 key and certificate" das Kontrollkästchen "Valid" und klicken Sie auf "Pkcs # 12 1", um die pkcs12-Datei für den Client auf den PC herunterzuladen.

Selbst erstellte Zertifikate verwenden

Methode 1



Schritt 1: Stellen Sie sicher, dass die Gerätezeit mit dem PC oder SNTP-Server synchronisiert ist.

Schritt 2: Aktivieren Sie OpenVPN

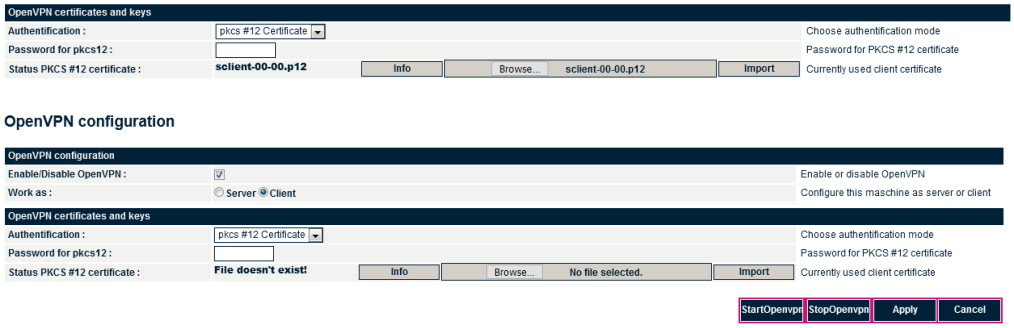
Schritt 3: Wählen Sie unter „Work as“ Client aus.

Schritt 4: Wählen Sie bei „Authentication“ „Certificate“ aus.

Schritt 5: Klicken Sie in den Zeilen „Status root CA certificate“, „Status client key“ und „Status client certificate“ auf den „Browse“ Button und wählen Sie die Importdatei aus. Klicken Sie auf „Import“ um die Datei zu importieren.

Methode 2

Import mit „pkcs#12 Certificate“.



Schritt 1: Stellen Sie sicher, dass die Gerätezeit mit dem PC oder SNTP-Server synchronisiert ist.

Schritt 2: Aktivieren Sie OpenVPN

Schritt 3: Wählen Sie unter „Work as“ Client aus.

Schritt 4: Wählen Sie bei „Authentication“ „pkcs’12 Certificate“ aus.

Schritt 5: Geben Sie das Passwort, welches Sie beim „Server“ vergeben haben in die Zeile „Passwort“ ein.

Schritt 6: Klicken Sie in der Zeile „Status PKCS#12 certificate“ auf den „Browse“ Button auf den „Browse“ Button und wählen Sie die Importdatei aus. Klicken Sie auf „Import“ um die Datei zu importieren.

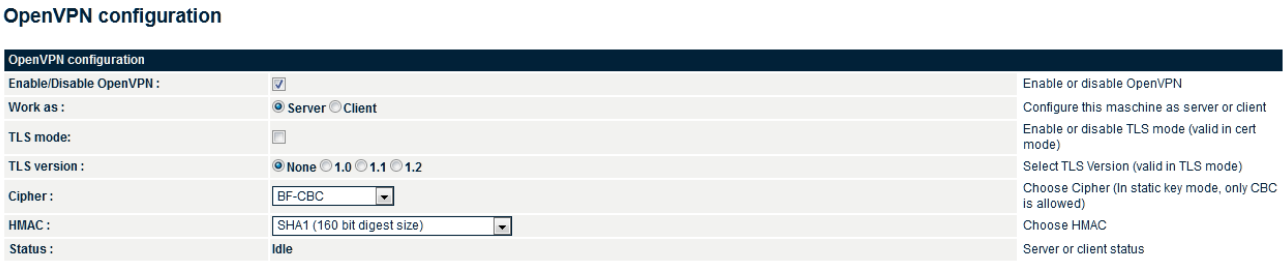
Abschließend rufen Sie die Seite erneut auf. In der Zeile "Status PKCS#12 certificate", können Sie den Dateinamen der importierten Datei sehen.

CA-signierte Zertifikate anwenden

Importieren Sie beim Server die folgenden Zertifikate: Root CA Zertifikat, Server Zertifikat, Schlüssel und Defie Hellmann Parameter.

Importieren Sie beim Client Root CA Zertifikat, Client Zertifikat und Client Key oder die pkcs#12 Datei. Am einfachsten ist es PKCS#12 zu nutzen, da dort alle Daten Root CA certificate, client certificate und clien Key Datei) in einer Datei enthalten sind.

5.3.2 OpenVPN/ Konfiguration



OpenVPN Parameter

Parameter

Aktivieren/ Deaktivieren Open VPN	Aktivieren/Deaktivieren Sie den OpenVPN Eintrag
Work as	Wählen Sie Server oder Client aus
TLS mode	Haken Sie die TLS mode an, um TLS zu aktivieren
TLS version	Wählen Sie zwischen None (ohne), 1.0, 1.1 oder 1.2 aus
Cipher	Wählen Sie eine Verschlüsselungsmethode aus
HMAC	Wählen Sie einen HMAC Algorithmus aus
Status	Hier können Sie den Status Ihrer OpenVPN Verbindung ablesen

5.3.3 OpenVPN/ Server Konfiguration

Roadwarrior Modus

Bridging Modus

OpenVPN Server Parameter

Device	OpenVPN Geräte Modus, wählen Sie TUN oder TAP aus
Protocol	Wählen Sie UDP oder TCP aus
Port	OpenVPN Port Nummer
VPN compression	Aktivieren Sie diese Option, um den Datenstrom zu komprimieren
Client mode	Wählen Sie zwischen Roadwarrior oder Bridging

Roadwarrior Parameter

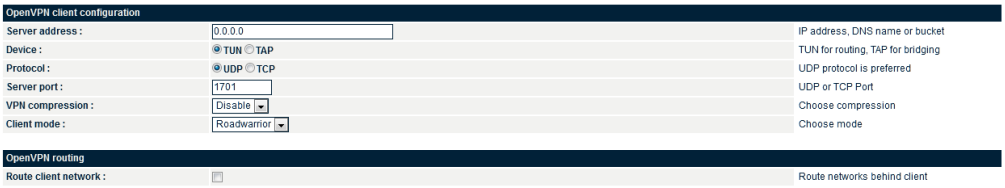
Network	Tragen Sie die IP-Adresse des OpenVPN Netzwerkes ein
Subnet mask	Tragen Sie die Open VPN Subnetmaske ein
Enable/Disable 1:1 NAT	Aktivieren Sie NAT Traversal für Open VPN
Route client network	Aktivieren Sie diese Option, um das Client Netzwerk hinzuzufügen

Bridging Parameter

OpenVPN bridge IP	Tragen Sie die IP-Adresse des lokalen OpenVPN Netzwerkes ein
Start IP address range	Tragen Sie die Startadresse des lokalen OpenVPN-IP-Pools ein
End IP address range	Tragen Sie die Endadresse des lokalen OpenVPN-IP Pools ein
Subnet netmask	Tragen Sie die Subnetmaske des lokalen OpenVPN Netzwerkes ein
Use a gateway address	Aktivieren Sie dieses Kontrollkästchen, um das Standard-Gateway für die Verbindung hinzuzufügen.
Enable/Disable 1:1 NAT	Aktivieren Sie NAT Traversal für OpenVPN

5.3.4 OpenVPN/ Client Konfiguration

Roadwarrior Mode



Bridging Mode

Client Parameter

Server Address	OpenVPN Server Adresse für die Verbindung
Device	OpenVPN Geräte Modus, wählen Sie TUN oder TAP aus
Protocol	Wählen Sie UDP oder TCP aus

Server Port	OpenVPN Port Nummer
VPN compression	Aktivieren Sie diese Option, um den Datenstrom zu komprimieren.
Client mode	Wählen Sie zwischen Roadwarrior oder Bridging

Roadwarrior Parameter

Route client network	Weiterleiten des hinter dem Client liegenden Netzwerkes

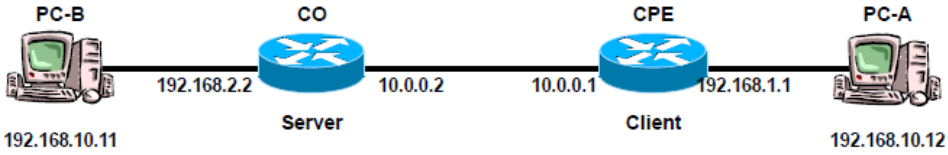
Bridging Parameter

OpenVPN bridge IP	Stellt eine Verbindung zum Internet her

5.3.5 OpenVPN Setup Beispiel

Beispiel 1: Konfiguration einer OpenVPN Bridge basierenden Verbindung

Richten Sie eine OpenVPN Bridge Verbindung ein, um PC-A und PC-B per im Bridge Modus miteinander zu verbinden.



Schritt 1	Stellen Sie sicher, dass die Master (CO) und Slave (CPE)-Zeit synchronisiert ist.
Schritt 2	Befolgen Sie die Schritte unter 5.3.1. und erstellen Sie ein selbstsigniertes Zertifikat auf dem Master(CO) und laden Sie die Client-PKCS# 12-Datei auf den Slave (CPE).
Schritt 3	Konfigurieren Sie den Slave (CPE) als OpenVPN Bridge/Client. Schauen Sie sich dazu die Abbildung an. Abschließend bestätigen Sie die Einstellung per „Apply“.
Schritt 4:	Konfigurieren Sie den Master (CO) als OpenVPN Bridge/ Server. Bitte schauen Sie sich die folgende Abbildung an und bestätigen Sie die Einstellungen mit „Apply“.
Schritt 5:	Wenn eine OpenVPN-Brige Verbindung hergestellt ist, können sich PC-A und PC-B gegenseitig anpingen.

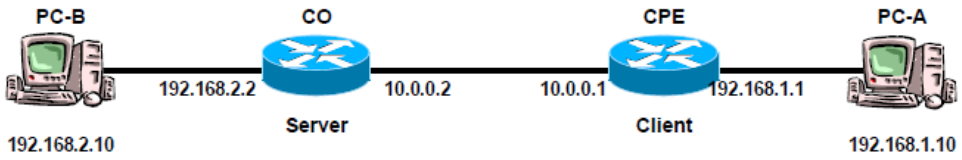
OpenVPN configuration

OpenVPN configuration		
Enable/Disable OpenVPN :	☑	Enable or disable OpenVPN
Work as :	◉ Server ○ Client	Configure this maschine as server or client
TLS mode:	☐	Enable or disable TLS mode (valid in cert mode)
TLS version :	◉ None ○ 1.0 ○ 1.1 ○ 1.2	Select TLS Version (valid in TLS mode)
Cipher :	BF-CBC	Choose Cipher (In static key mode, only CBC is allowed)
HMAC :	SHA1 (160 bit digest size)	Choose HMAC
Status :	Running	Server or client status

OpenVPN server configuration		
Device :	○ TUN ◉ TAP	TUN for routing, TAP for bridging
Protocol :	◉ UDP ○ TCP	UDP protocol is preferred
Port :	1701	Port to listen on
VPN compression :	Disable	Choose compression
Client mode :	Bridging	Choose mode
OpenVPN bridge IP :	192 . 168 . 100 . 1	Establish connection to website
Start IP address range :	192 . 168 . 100 . 2	IP address pool
End IP address range :	192 . 168 . 100 . 20	IP address pool
Subnet mask:	255 . 255 . 255 . 0	Certificate mode: Subnet mask Pre-Shared key/TUN mode: the other side IP
Use a gateway address :	☐	Set default gateway

1:1 NAT		
Enable/Disable 1:1 NAT :	☐	enable/disable 1:1 NAT

Beispiel 2: Richten Sie eine OpenVPN Router Verbindung wie folgt ein:



Schritt 1: Stellen Sie sicher, dass die Master (CO) und Slave (CPE)-Zeit synchronisiert ist.

Schritt 2: Befolgen Sie die Schritte unter 5.3.1. und erstellen Sie ein selbstsigniertes Zertifikat auf dem Master(CO) und laden Sie die Client-PKCS# 12-Datei auf den Slave (CPE).

Schritt 3: Konfigurieren Sie den Slave (CPE) als OpenVPN Roadwarrior/ Client. Schauen Sie sich dazu die Abbildung an. Abschließend bestätigen Sie die Einstellung per „Apply“.

Schritt 4: Konfigurieren Sie den Master (CO) als OpenVPN Roadwarrior/ Server. Bitte schauen Sie sich die folgende Abbildung an und bestätigen Sie die Einstellungen mit „Apply“.

OpenVPN configuration

OpenVPN configuration		
Enable/Disable OpenVPN :	☑	Enable or disable OpenVPN
Work as :	○ Server ◉ Client	Configure this maschine as server or client
TLS mode:	☐	Enable or disable TLS mode (valid in cert mode)
TLS version :	◉ None ○ 1.0 ○ 1.1 ○ 1.2	Select TLS Version (valid in TLS mode)
Cipher :	AES-256-CBC	Choose Cipher (In static key mode, only CBC is allowed)
HMAC :	SHA1 (160 bit digest size)	Choose HMAC
Status :	Connected with IP address 192.168.5.6/255.255.255.255 (p-t-p remote:192.168.5.5)	Server or client status

OpenVPN client configuration		
Server address :	10.0.0.2	IP address, DNS name or bucket
Device :	◉ TUN ○ TAP	TUN for routing, TAP for bridging
Protocol :	◉ UDP ○ TCP	UDP protocol is preferred
Server port :	1701	UDP or TCP Port
VPN compression :	Disable	Choose compression
Client mode :	Roadwarrior	Choose mode

Schritt 5: Wenn eine OpenVPN-Router Verbindung hergestellt ist, können sich PC-A und PC-B gegenseitig anpingen. Weiterhin erkennt PC-B, dass die „Source-IP“ die IP-Adresse des OpenVPN- TUN-Gerätes auf dem Master (CPE) ist. In diesem Beispiel wird es die IP-Adresse 192.168.5.6 die in der Statuszeile des CPE (Slave) angezeigt wird. PC-B unterstützt den Zugriff auf das LAN-Netzwerk von CPE(Slave) nicht.

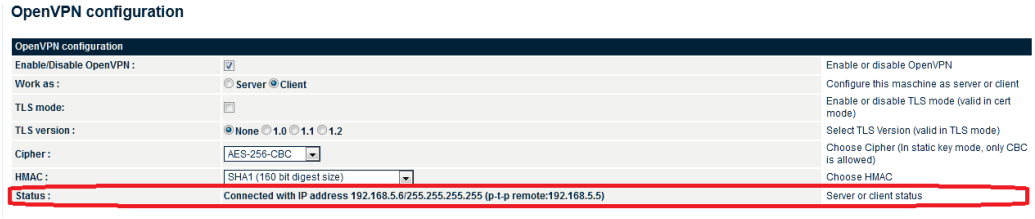
OpenVPN configuration

OpenVPN configuration		
Enable/Disable OpenVPN :	☑	Enable or disable OpenVPN
Work as :	◉ Server ○ Client	Configure this maschine as server or client
TLS mode:	☐	Enable or disable TLS mode (valid in cert mode)
TLS version :	◉ None ○ 1.0 ○ 1.1 ○ 1.2	Select TLS Version (valid in TLS mode)
Cipher :	AES-256-CBC	Choose Cipher (In static key mode, only CBC is allowed)
HMAC :	SHA1 (160 bit digest size)	Choose HMAC
Status :	Not Running	Server or client status

OpenVPN server configuration		
Device :	◉ TUN ○ TAP	TUN for routing, TAP for bridging
Protocol :	◉ UDP ○ TCP	UDP protocol is preferred
Port :	1701	Port to listen on
VPN compression :	Disable	Choose compression
Client mode :	Roadwarrior	Choose mode
Network :	192 . 168 . 5 . 0	Network for Clients
Subnet mask:	255 . 255 . 255 . 0	Certificate mode: Subnet mask Pre-Shared key/TUN mode: the other side IP

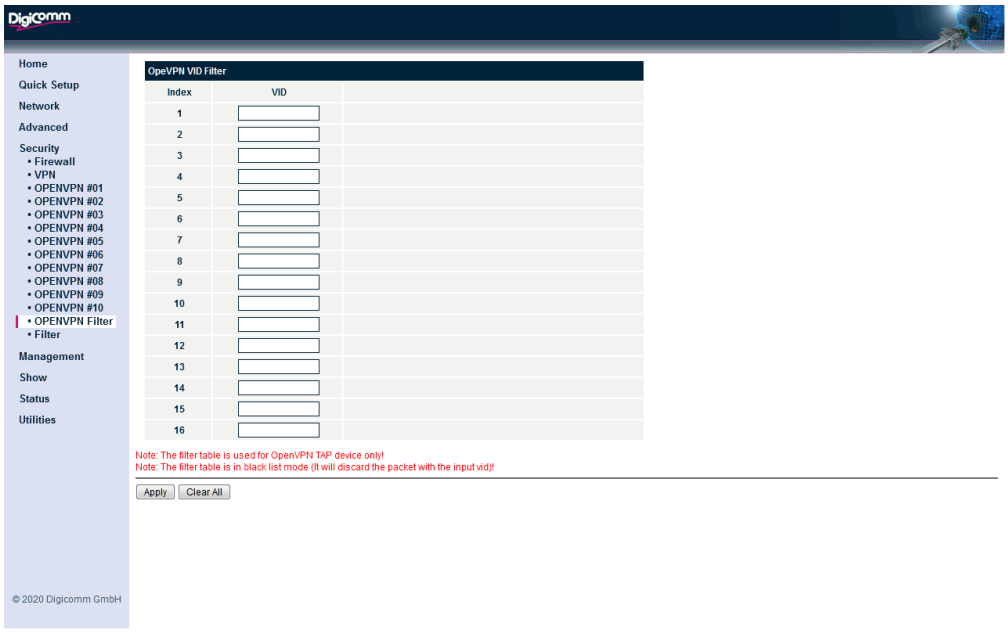
1:1 NAT		
Enable/Disable 1:1 NAT :	☐	enable/disable 1:1 NAT

OpenVPN routing		
Route client networks :	☑	Route networks behind clients
Client 1 network / netmask :	192.168.1.0 / 255.255.255.0	Network behind client



5.4 OpenVPN Filter

Der OpenVPN-Filter bietet einen VLAN-ID-Filter unter OpenVPN-TAP-Verbindung (Bridge).
Auf dem OpenVPN TAP-Gerät wird das gesamte Eingangspaket mit der übereinstimmenden VID in der Tabelle verworfen.



OpenVPN Filter Parameter

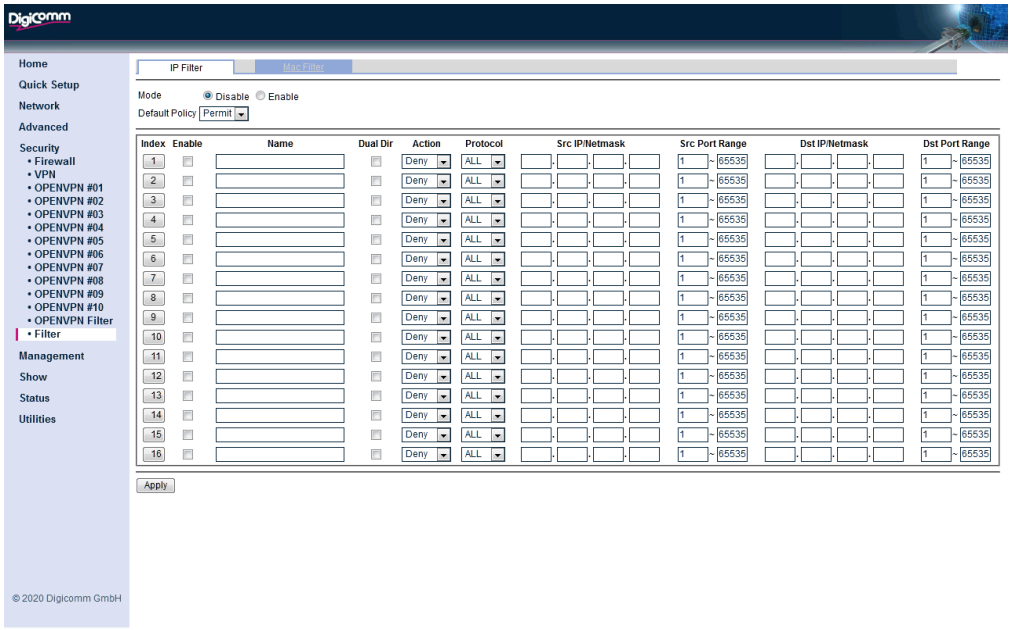
VID Die VLAN-ID, die in OpenVPN TAP Verbindung herausgefiltert werden soll

5.5 Filter

Der VPN-Router bietet eine IP-Filter- und eine MAC-Filterfunktion zum Herausfiltern des eingehenden Pakets.

5.5.1 Filter/IP Filter

Klicken Sie auf den „IP Filter“ Button um die IP Filter Einstellungen vornehmen zu können.



IP Filter Parameter

Mode	Aktivieren/ Deaktivieren Sie die globalen Filter Einstellungen
Default Policy	Deny, Permit und Reject auswählbar
	Deny Nicht übereinstimmende Pakete werden abgelehnt
	Permit Nicht übereinstimmende Pakete werden akzeptiert
	Reject Nicht übereinstimmende Pakete werden abgelehnt

IP Filter Eingabeparameter

Enable	Aktivieren/ Deaktivieren Sie die Option
Name	Vergeben Sie einen Namen (frei wählbar)
Dual Dir	Aktivieren/ Deaktivieren Sie die Regel für beide Richtungen
Action	Unterstützt die Optionen Verweigern, Zulassen und Ablehnen
Protocol	Wählen Sie aus den Optionen ALL, IGMP, TCP und UDP aus
Src IP/ Netmask	Tragen Sie die Quell-IP-Adresse/ Netzmaske hier ein
Src Port Range	Tragen Sie hier den Quellportbereich ein
Dst IP/ Netmask	Tragen Sie hier die Ziel-IP-Adresse / Netzmaske ein
Dst Port Range	Tragen Sie hier den Zielportbereich ein

Application	Protocol	Port Number	
		Start	End
HTTP	TCP	80	80
DNS	UDP	53	53
DNS	TCP	53	53
FTP	TCP	53	53
Telnet	TCP	21	21
SMTP	TCP	23	23
POP3	TCP	25	25
NEWS (NNTP)	TCP	110	110
Real Audio/ Real Video	UDP	119	119
PING	ICMP	7070	7070
H.323	TCP	N/A	N/A
T.120	TCP	1720	1720
SSH	TCP	1503	1503
NTP/ SNTP	UDP	22	22
HTTP/ HHTP Proxy	TCP	123	123

HTTPS	TCP	8080	8080
ICQ	TCP	443	443
MSN (1863)	TCP	5190	5190
MSN (7001)	TCP	1863	1863
MSB video	UDP	7001	7001
	TCP	9000	9000

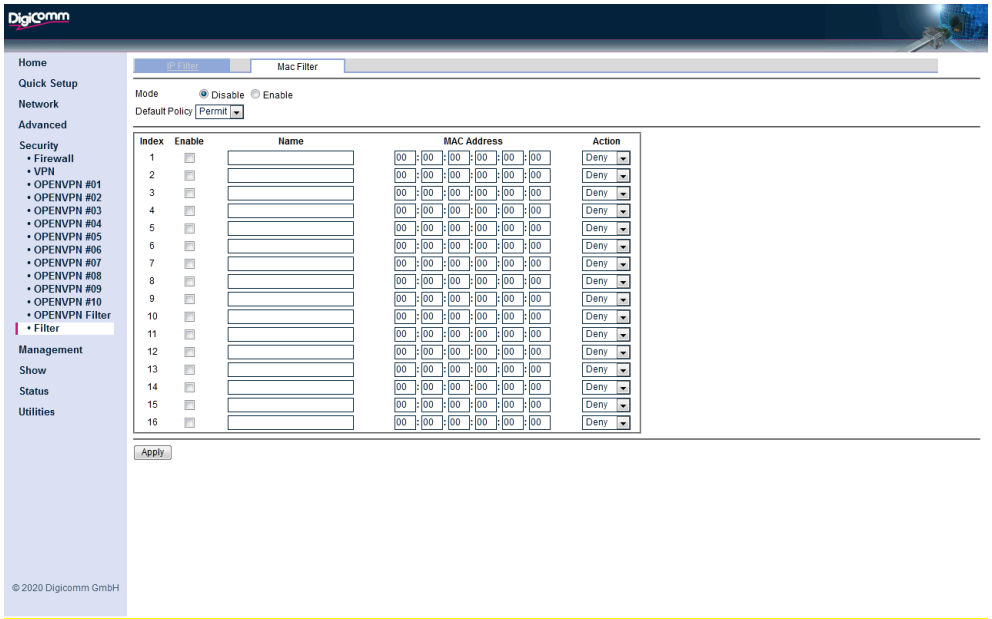
5.5.2 Filter/Mac Filter

Klicken Sie auf den Button „Mac Filter“, um auf die Konfigurationsseite zu gelangen.

In Computernetzwerken bezieht sich die MAC-Filterung auf eine Sicherheitszugriffskontrollmethode, bei der die jedem Netzwerkgerät zugewiesene 48-Bit-Adresse (XX: XX: XX: XX: XX: XX) verwendet wird, um den Zugriff auf das Netzwerk zu bestimmen.

MAC-Adressen werden jedem Netzwerkgerät eindeutig zugewiesen. Die Verwendung der MAC-Filterung in einem Netzwerk ermöglicht und verweigert den Netzwerkzugriff auf bestimmte Geräte mithilfe von schwarzen und weißen Listen. Während die Einschränkung des Netzwerkzugriffs durch die Verwendung von Listen unkompliziert ist, wird eine einzelne Person nicht durch eine MAC-Adresse identifiziert, sondern nur durch ein Gerät. Daher muss eine autorisierte Person für jedes Gerät, das sie verwenden möchte, einen White-List-Eintrag erhalten um Zugriff auf das Netzwerk zu erhalten.

Während einem drahtlosen Netzwerk ein zusätzlicher Schutz gewährt wird, kann die MAC-Filterung umgangen werden, indem eine gültige MAC-Adresse gescannt und dann der eigene MAC-Adresse in eine validierte MAC-Adresse geändert wird.



MAC Filter Parameter

Mode	Aktivieren/Deaktivieren Sie den MAC Filter
Default Policy	Deny, Permit und Reject auswählbar
	Deny Nicht übereinstimmende Pakete werden abgelehnt
	Permit Nicht übereinstimmende Pakete werden akzeptiert
	Reject Nicht übereinstimmende Pakete werden abgelehnt

MAC Filter Eingabeparameter

Enable	Aktivieren/ Deaktivieren Sie die Option

Name Vergeben Sie einen Namen (frei wählbar)
MAC Address Tragen Sie die MAC Adresse ein
Action Unterstützt die Optionen Verweigern, Zulassen und Ablehnen

6 Management

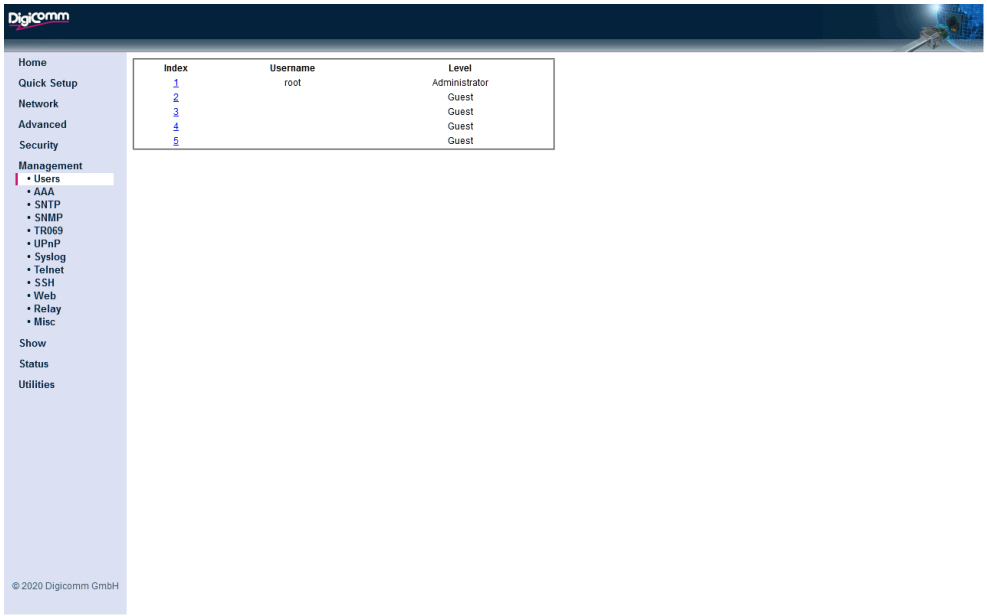
Im Management Menü können Sie folgende Punkte konfigurieren:

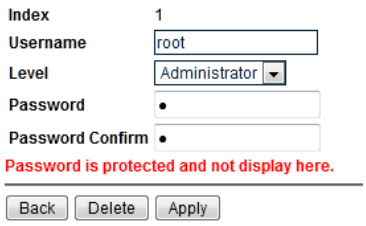
1. Users
2. AAA
3. SNTP
4. SNMP
5. TR069
6. UPnP
7. Syslog
8. Telnet
9. SSH
10. Web
11. Relay
12. Misc

6.1 Users / Nutzer

Beim SHDTU können fünf Benutzerkonten konfiguriert werden mit drei Berechtigungsstufen Administrator, Normal und Gast.

Guest User (Gast Zugriff) Zeigt nur den Status des Gerätes an.
Normal User (Normaler Zugriff) Zeigt den Status des Gerätes an und die Konfiguration kann geändert werden.
Administrator Users (Administrator Zugriff) Zeigt des Status des Gerätes an, Konfiguration kann geändert werden und Nutzer hinzugefügt oder gelöscht werden.





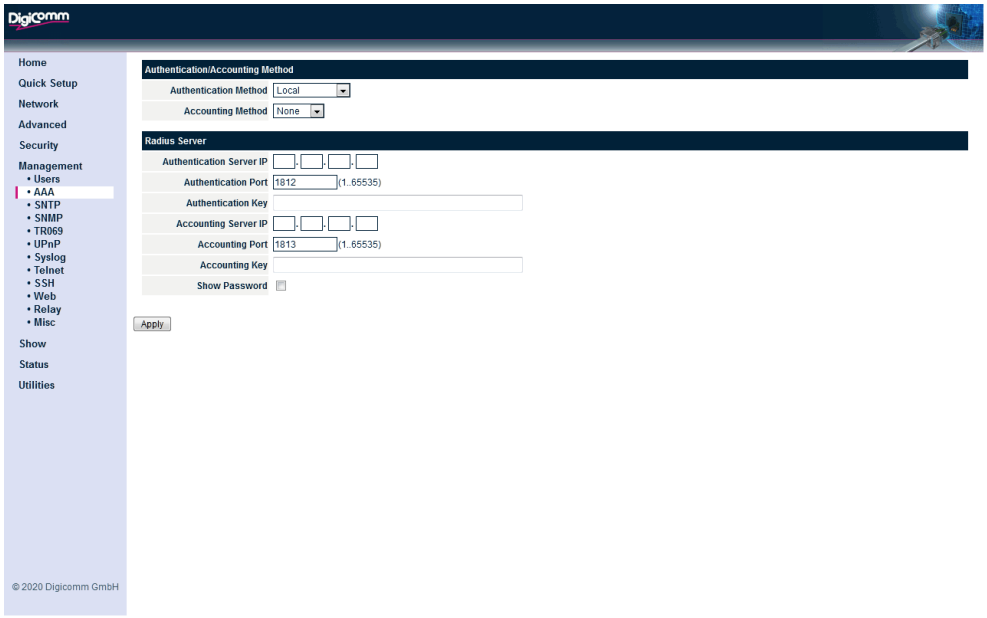
User Parameter

Username	Benutzername
Level	Benutzerberechtigungsstufe (Administrator, Normal oder Gast)
Password	Benutzerpasswort
Password Confirm	Geben Sie zur Bestätigung das Benutzerpasswort erneut ein.

6.2 AAA

Beim SHDTU wird der externe Radius-Serverauthentifizierungsdienst unterstützt.

Wenn sich ein Benutzer über CLI oder Web anmeldet, kann sich das Benutzerkonto durch einen externen Radius-Server authentifizieren.



AAA Parameter

Authentication Method

Local	Benutzer nur durch Lokal authentifizieren
Local-Radius	Authentifizieren Sie den Benutzer in der Reihenfolge Lokal, Radius
Radius-Local	Authentifizieren Sie den Benutzer in der Reihenfolge Radius, Lokal

Account Methode

None	Keine Methode ausgewählt
Radius	Wenn sich Benutzer anmelden und abmelden wir an den Radius Server eine Meldung gesendet.

Radius Server Parameter

Authentication Server IP	Tragen Sie die Adresse des Radius Authentication Servers ein
Authentication Port	Tragen Sie die Portnummer des Radius Authentifizierungsdienstes ein
Authentication Key	Tragen Sie den Schlüssel für den Radius-Authentifizierungsdienst ein
Accounting Server IP	Tragen Sie die IP Adresse des Radius Accounting Servers
Accounting Port	Tragen Sie die Portnummer des Radius Accounting Services ein
Accounting Key	Tragen Sie den Schlüssel des Radius Accounting Services ein
Show Password	Wählen Sie diese Option aus, um sich das Passwort anzeigen zu lassen.

6.3 SNTP (Simple Network Time Protocol)

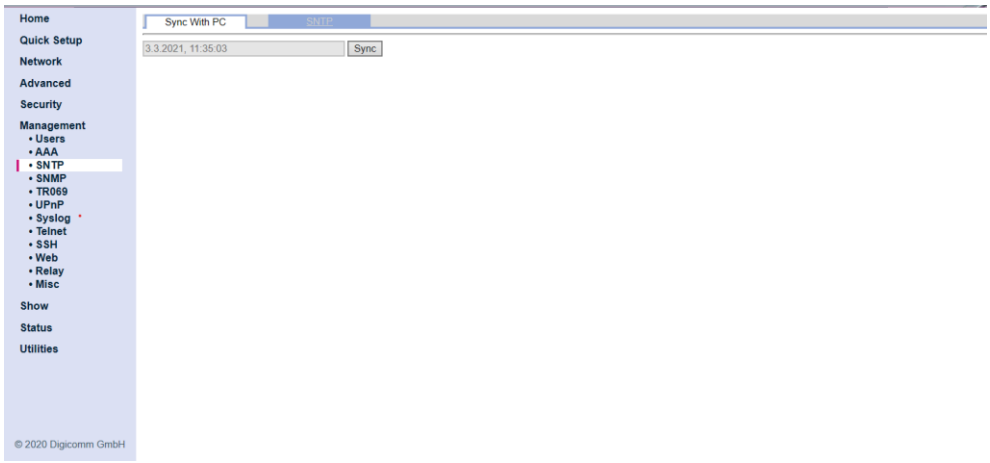
Die Zeitsynchronisierung ist ein wichtiger Faktor für alle Unternehmen, die von ihren IT-Systemen abhängig sind. Grund hierfür ist die in allen Systemen vorhandene Uhr, die als Zeitgeber für diverse Systemfunktionen fungiert. Ohne die Zeitsynchronisierung weichen die Systemuhren voneinander ab und führen zum Ausfall von Zeitplänen für das Filtern von Firewall-Paketen, Sicherheitsrisiken oder die unplanmäßige Ausführung von virtuellen Servern.

Die Abkürzung SNTP steht für das Simple Network Time Protocol, eine Variation des Network Time Protocol (NTP), das die Synchronisierung von Computeruhren im Internet ermöglicht. SNTP kann für eine optimale Leistung der gesamten NTP-Implementierung genutzt werden. Diese Funktion wird nur im Modus „Router“ unterstützt.

Es gibt zwei Methoden zur Synchronisierung der Zeit, die Synchronisierung über den PC oder per SNTP. Falls Sie sich für die Synchronisierung über den PC entscheiden, übernimmt das SHDTU die Zeiteinstellung der internen Uhr des PCs. Falls Sie eine Synchronisierung per SNTP festlegen, verwendet das SHDTU das Protokoll für die Synchronisierung mit dem Zeitserver. Bei einer Synchronisierung über den Zeitserver per SNTP ist die Konfiguration der Optionen „Service“, „Time Server“ und „Time Zone“ erforderlich. Für die Synchronisierung mit dem PC müssen die oben genannten Parameter nicht konfiguriert werden.

6.3.1 SNTP/ Sync With PC – Synchronisation mit dem PC

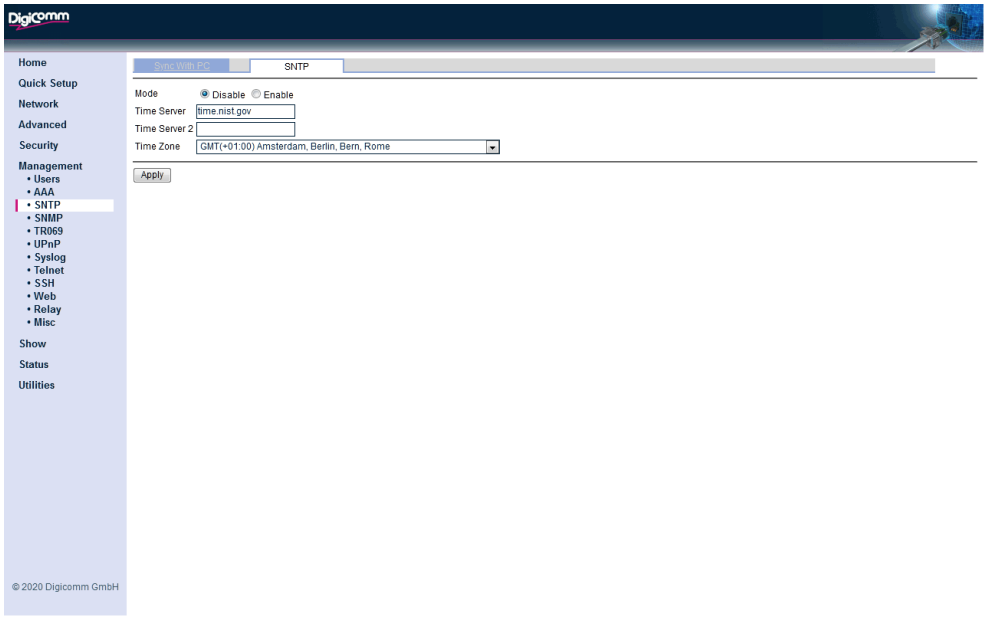
Klicken Sie auf den Button „Sync With PC“, um auf die Konfigurationsseite zu gelangen.



Falls Sie sich für die Synchronisierung über den PC entscheiden, übernimmt das SHDTU die Zeiteinstellung der internen Uhr des PCs wenn Sie auf die Schaltfläche „Synchronisieren klicken“

6.3.2 SNTP/ SNTP

Klicken Sie auf den Button „SNTP“, um auf die Konfigurationsseite zu gelangen.



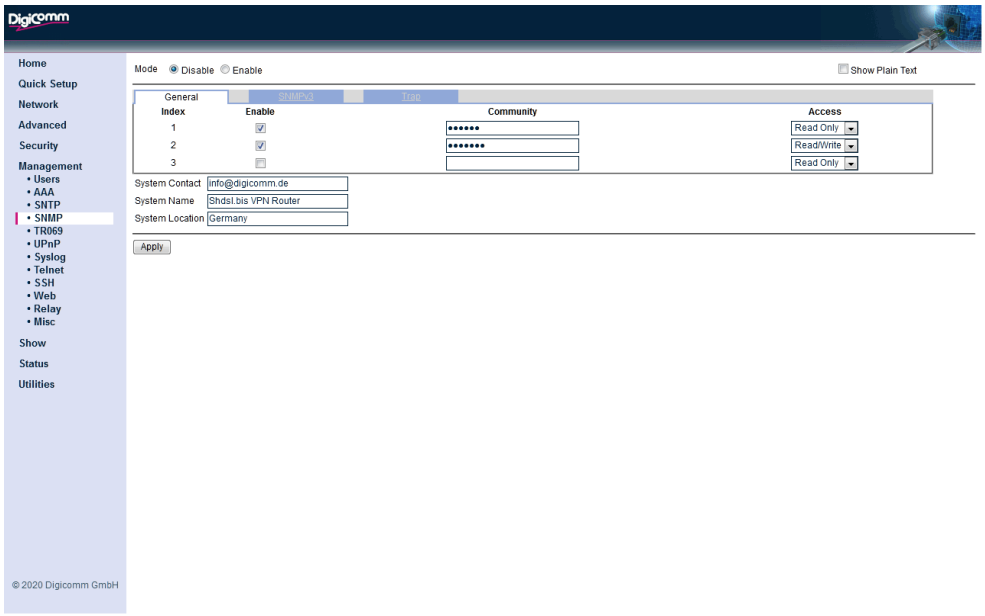
SNTP Filter Parameter

Mode	Aktivieren/ Deaktivieren SNTP Deamon
Time Server	Zeit Server
Time Server 2	Zeit Backup Server
Time Zone	Zeitzone

6.4 SNMP (Simple Network Managemend Protocol)

6.4.1 SNMP/ General

Klicken Sie auf den Button „General“, um auf die Konfigurationsseite zu gelangen.



SNMP Parameter

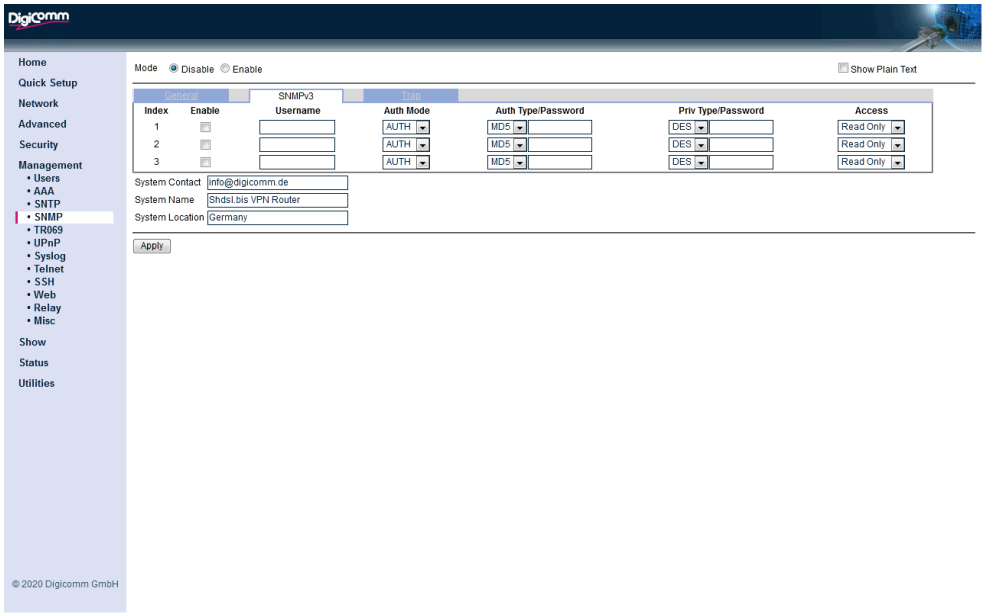
Mode	Aktivieren/ Deaktivieren Sie SNMP global
System Contact	System MIB Contact Name
System Name	System MIB Name
System Location	System MIB Location

SNMP Generelle Parameter

Enable	Aktivieren/ Deaktivieren Sie den SNMP Eintrag.
Community	SNMP Community Name.
Access	Read Only – Erlaubt das Lesen der OIDs. Read/Write- Erlaubt das Lesen und Schreiben der OIDs.

6.4.2 SNMP/ SNMPV3

Klicken Sie auf den SNMPV3 Button um auf die SNMP/ SNMPV3 Einstellungs-Seite zu gelangen.



SNMP Parameter

Mode	Aktivieren oder Deaktivieren SNMP
System Contact	System MIB Contact Name
System name	System MIB Name
System Location	System MIB Location

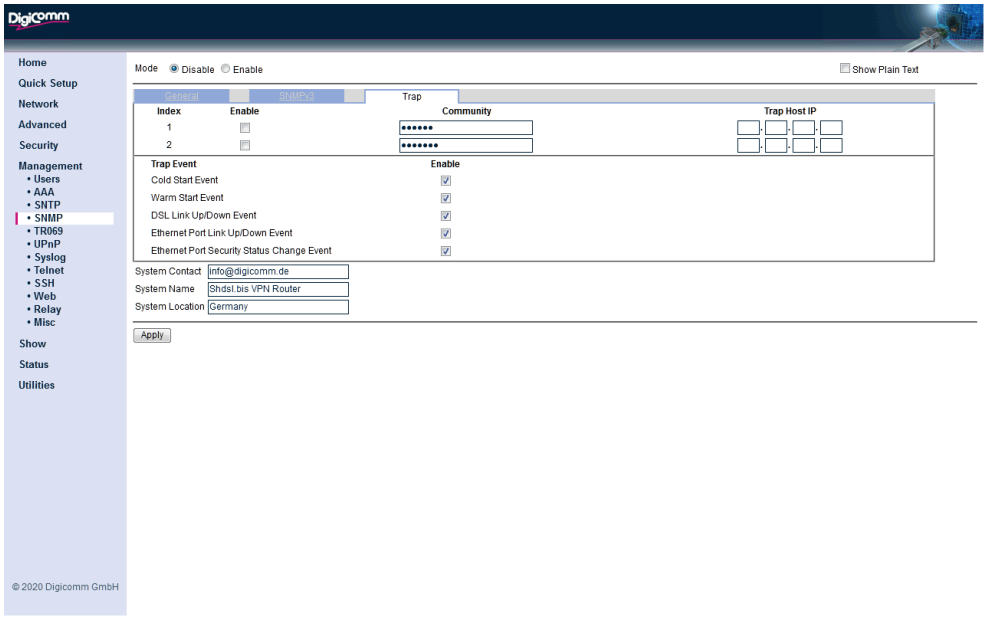
SNMP Generelle Parameter

Enable	Aktivieren/ deaktivieren Sie den SNMP V3 Benutzer Eintrag
UserName	SNMP V3 User Name
Auth Mode	NONE – Keine Authentifikation, Keine Privatsphäre AUTH – Authentifikation, Keine Privatsphäre PRIV - Authentifikation und Privatsphäre
Auth Type	Wählen Sie aus MD5 oder SHA
Auth Password	Vergeben Sie ein Authentifikations- Passwort
Priv Type	Wählen Sie aus DES oder AES
Priv Password	Vergeben Sie ein Passwort für die Privatsphäre
Access	Read Only - der SNMP V3 Nutzer ist berechtigt die OIDs nur zu lesen

Read/ Write – der SNMP V3 Nutzer ist berechtigt zu lesen und die Konfiguration der OIDs zu bearbeiten.

6.4.3 SNMP/ TRAP

Klicken Sie auf den TRAP Button um auf die SNMP/ TRAP Einstellungs-Seite zu gelangen.



SNMP Parameter

Mode	Aktivieren/ Deaktivieren von SNMP
System Contact	Geben Sie eine Kontaktperson bzw. eine E-Mail-Adresse an
System Name	Vergeben Sie einen System MIB Namen
System Location	Geben Sie an, wo sich das System befindet Deutschland/ Germany

SNMP Trap Parameter

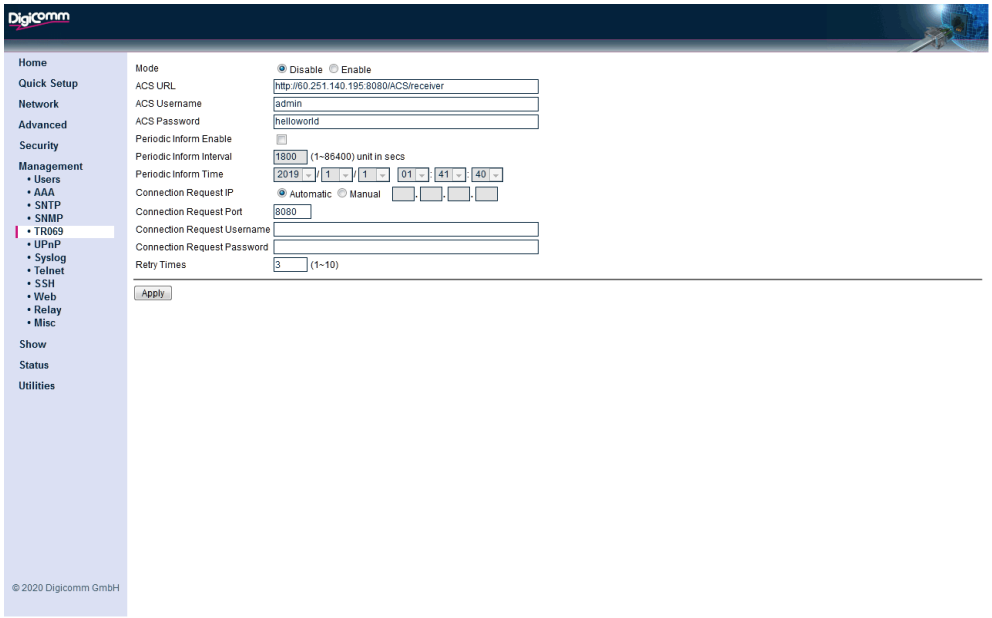
Enable	Aktivieren/ Deaktivieren sich durch Setzen der Haken die Trap Option
Community	Der Community Name der zum Senden des Traps verwendet wird
Trap Host IP	The SNMP Trap Server

SNMP Trap Events

Cold Start Event	Aktivieren/ Deaktivieren Sie das Trap Ereignis
Warm Start Event	Aktivieren/ Deaktivieren Sie das Trap Ereignis
DSL Link Up/ Down Event	Aktivieren/ Deaktivieren Sie das Trap Ereignis
Ethernet Port Link Up/ Down Event	Aktivieren/ Deaktivieren Sie das Trap Ereignis
Ethernet Port Security Status Change Event	Aktivieren/ Deaktivieren Sie das Trap Ereignis

6.5 TR069

TR-069 (Abkürzung für „Technical Report 069“) ist eine technische Spezifikation des DSL Forums mit der Bezeichnung „CPE WAN Management Protocol (CWMP)“. Es definiert ein Anwendungsschichtprotokoll für das Remote-Management von Endbenutzergeräten. Als bidirektionales HTTP-basiertes Protokoll ermöglicht es die Kommunikation zwischen CPE (Customer Premises Equipment) und ACS (Auto Control Servers). Es umfasst eine sichere automatische Konfiguration und die Steuerung anderer CPE Verwaltungsfunktionen innerhalb eines integrierten Frameworks. Mithilfe von TR-069 können die Terminals eine Verbindung zu den ACS (Auto Configuration Servers) herstellen und eine automatische Konfiguration durchführen.



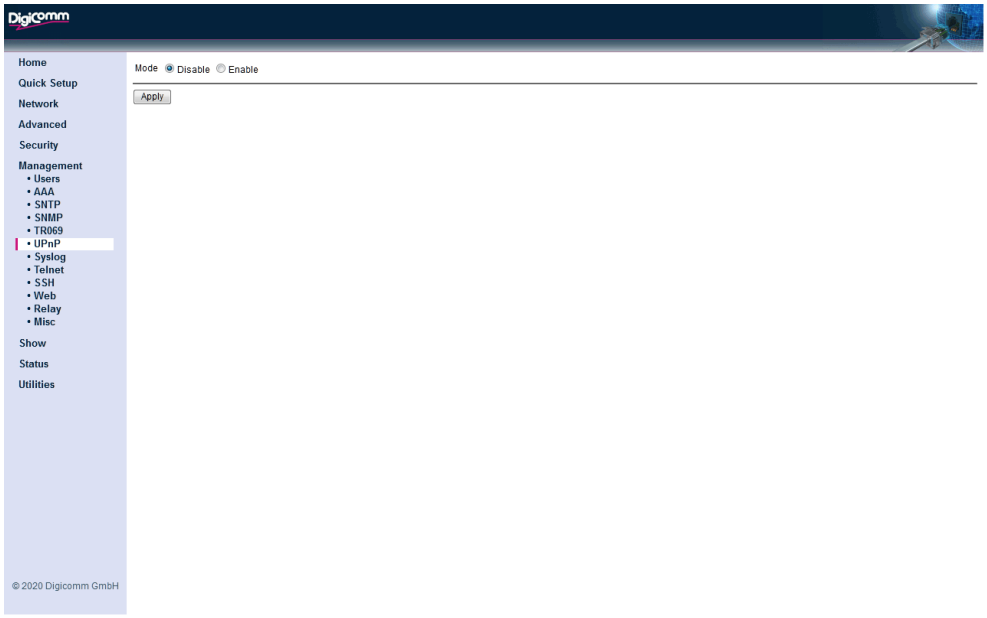
TR069 Parameter

Mode	Aktivieren /Deaktivieren von SNMP
ACS URL	Die ACS-URL in Form eines gültigen http oder HTTPS Formates
ACS User Name	Der Benutzername zur Verbindung mit dem Access Control Server
ACS Password	Das Passwort zur Verbindung mit dem ACS Server
Periodic Inform Enable	Aktivieren /Deaktivieren Sie den CPE (Slave) um regelmäßig Informationen an den ACS zu senden
Periodic Inform Interval	Die Dauer des Intervalls in Sekunden
Periodic Infrom Time	Die absolute Informationszeit
Connection Request IP	Geben Sie hier die IP-Adresse des Slaves (CPE) ein, der mit dem ACS verbunden werden soll.
Connection Request Port	Geben Sie hier den Port des Slaves (CPE) ein, der mit dem ACS verbunden werden soll.
Connection Request User Name	Geben Sie den Benutzernamen ein, den der ACS verwendet um eine Verbindung zum CPE (Slave) herzustellen.
Connection Request Password	Geben Sie das Passwort ein, den der ACS verwendet um eine Verbindung zum CPE (Slave) herzustellen.
Retry Times	Hier geben Sie an, wie oft der Verbindungsaufbau wiederholt wird.

6.6 UPnP (Universal Plug and Play)

UPnP ™ (Universal Plug and Play) ist eine Reihe von Protokollen, mit denen ein PC automatisch andere UPnP-Geräte (von einem Internet-Gateway-Gerät bis zu einem Lichtschalter) erkennen, eine XML-Beschreibung des Geräts und seiner Dienste abrufen und das Gerät steuern kann und abonnieren eine Echtzeit-Ereignisbenachrichtigung.

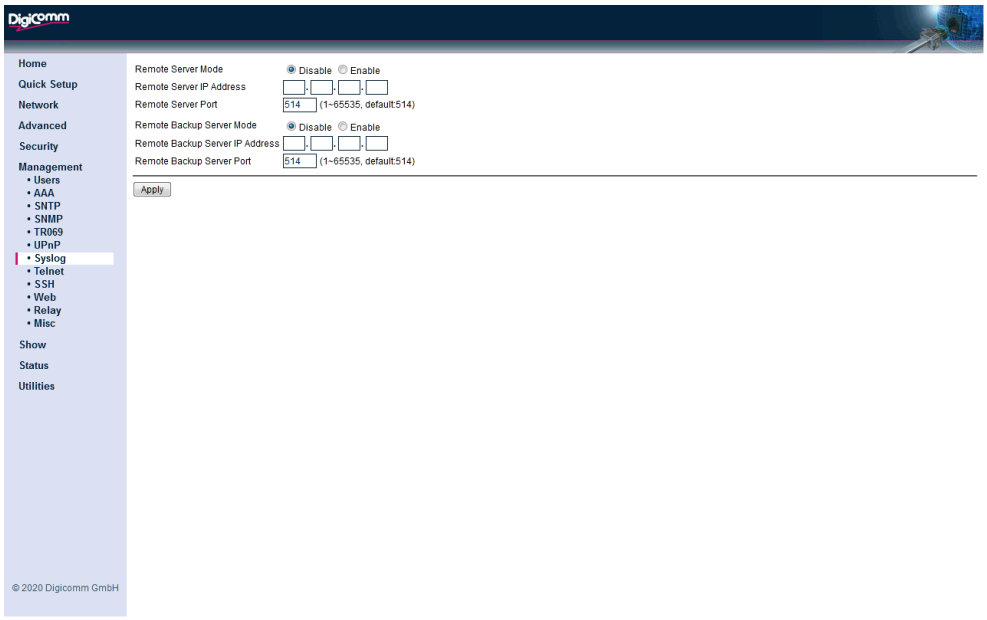
PC's die UPnP verwenden, können die LAN/ WAN-IP-Adresse des VPN Routers abrufen und dann die IP-Adresse zum Verwalten des Gerätes verwenden.



6.7 Syslog

Syslog ist ein Standardverfahren für die Zusammenfassung verschiedener Protokolle. Sie können einen Syslog-Server für die Speicherung Ihrer Serverprotokolle an einem Remote Standort verwenden, um sie später durchzusehen oder langfristig dort abzulegen.

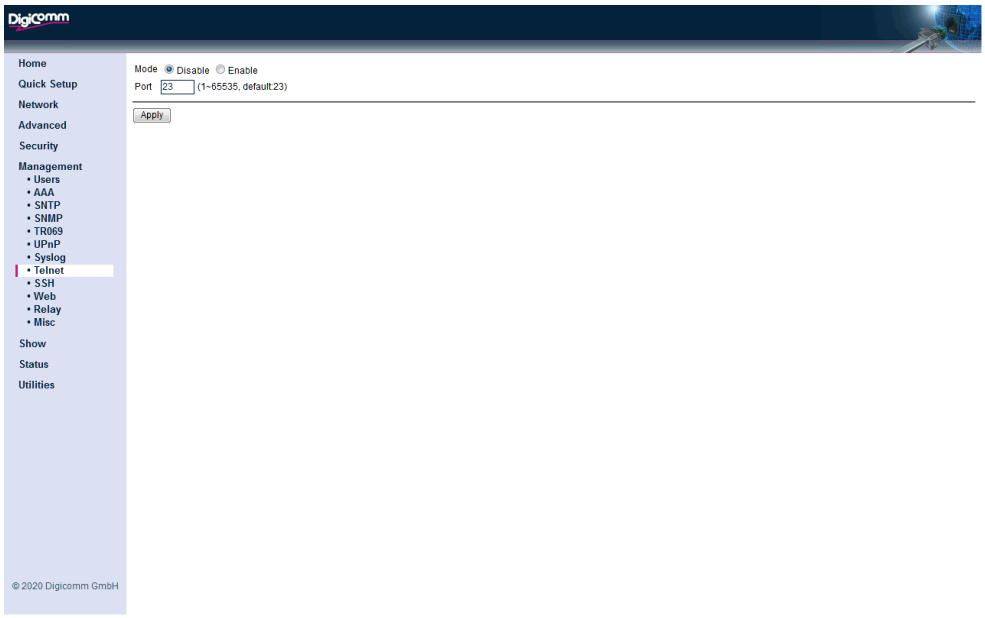
Um die Protokolle an den LOG-Server zu senden, müssen Sie die anderen Server in Ihrem Netzwerk für den Versand von Protokollen an diesen Server konfigurieren.



Syslog Parameter

Remote Server Mode	Aktivieren/ Deaktivieren Sie die Remote Server Option
Remote Server IP Address	Geben Sie die IP-Adresse des Syslog-Remote-Servers ein
Remote Server Port	Geben Sie den Server Port des Syslog Remote Servers ein
Remote Backup Server Mode	Aktivieren/ Deaktivieren Sie die Remote Backup Server Option.
Remote Backup Server IP Address	Geben Sie die IP-Adresse des Syslog-Backup Remote-Servers ein
Remote Backup Server Port	Geben Sie den Server Port des Syslog Backup Remote Servers ein

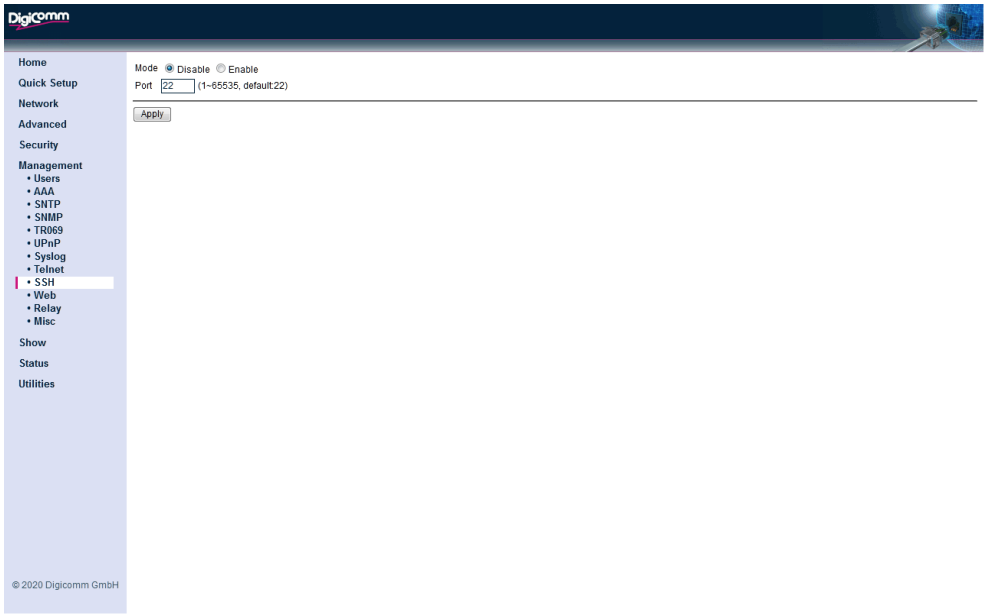
6.8 Telnet



Telnet Server Parameter

Mode	Aktivieren/ Deaktivieren die Telnet Server Option
Port	Geben Sie den Telnet Service Port

6.9 SSH

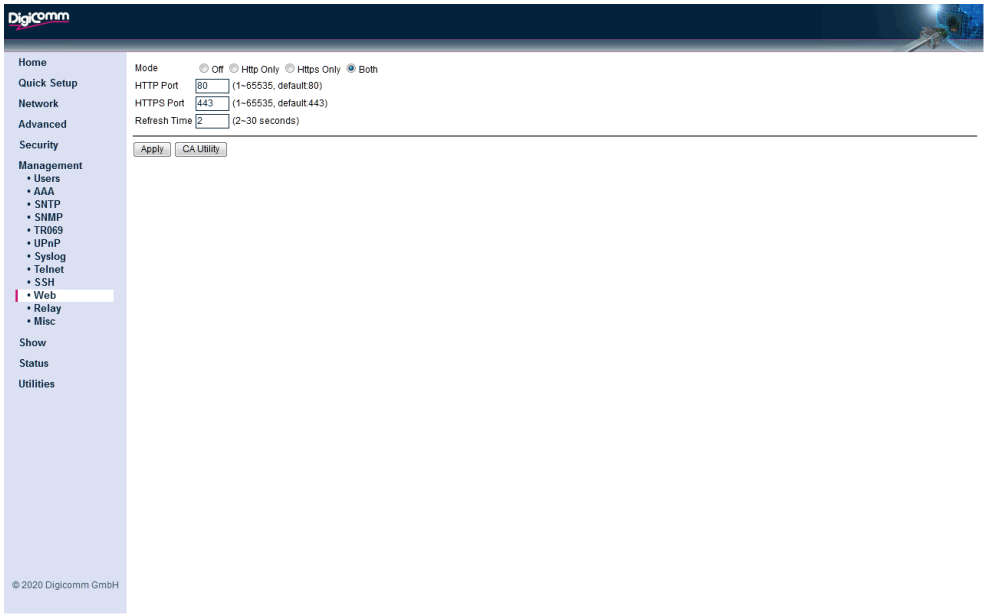


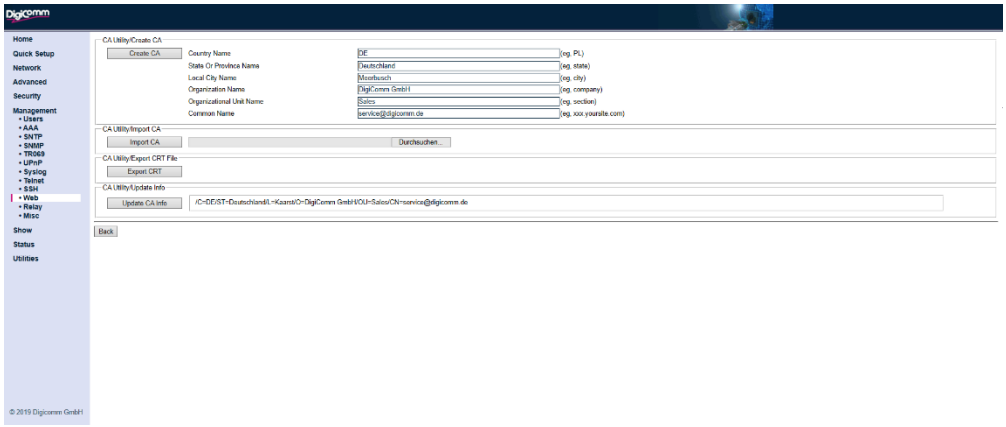
SSH Server Parameter

Mode	Aktivieren/ Deaktivieren die SSH Server
Port	SSH Service Port

6.10 Web

Mit der Web-Option wird eine Aktualisierung von Webseiten, wenn Sie die Seiten mit dynamischen Statusdaten anzeigen ermöglicht. Für die Aktualisierung können Sie einen Zeitraum von 2 bis 30 Sekunden einstellen. Als Werkseinstellung sind hier 2 Sekunden festgelegt. Für Web Browser können Sie den standardmäßig eingestellten Port durch Eingabe der neuen Port-Nummer ändern. Falls Sie diese Standardeinstellung ändern, müssen Sie die neue Port Nummer den entsprechenden Benutzern mitteilen. Als Werkseinstellung ist hier Port 80 festgelegt. Klicken Sie auf „Apply“ um die Änderungen zu übernehmen, um die Einrichtung abzuschließen.

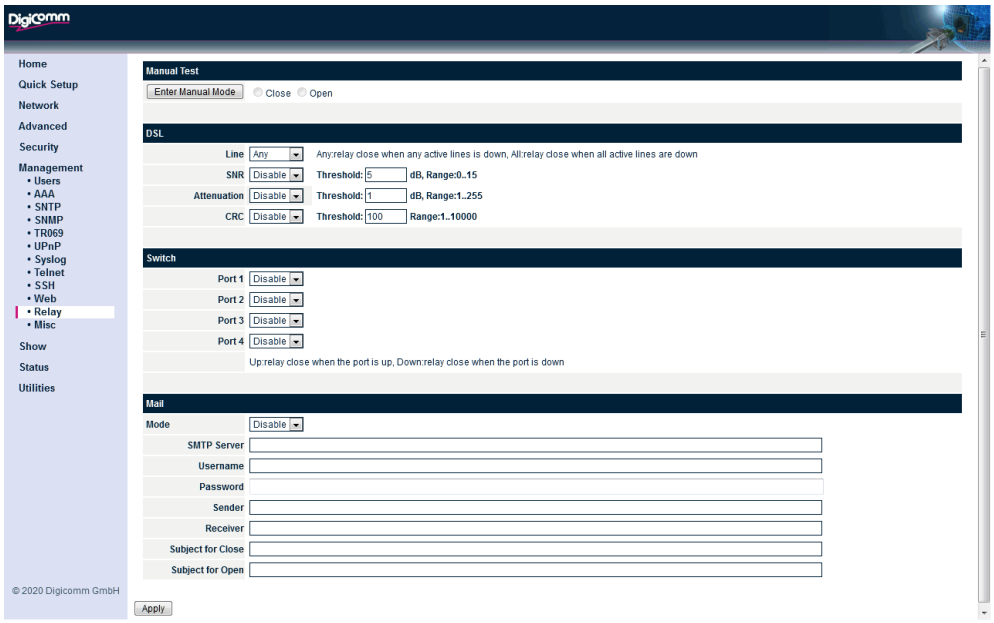




Web Parameter

Mode	Aus (Off), Http Only (nur http), Https Only (nur Https) und Both (Beides)
Http Port	Geben Sie die Port Nummer des Http Services ein
Https Port	Geben Sie die Port Nummer des Https Services ein
Refresh Time	Hier geben Sie an, wie oft die Seite wieder neu aufgebaut werden soll.

6.11 Relay (Relais)



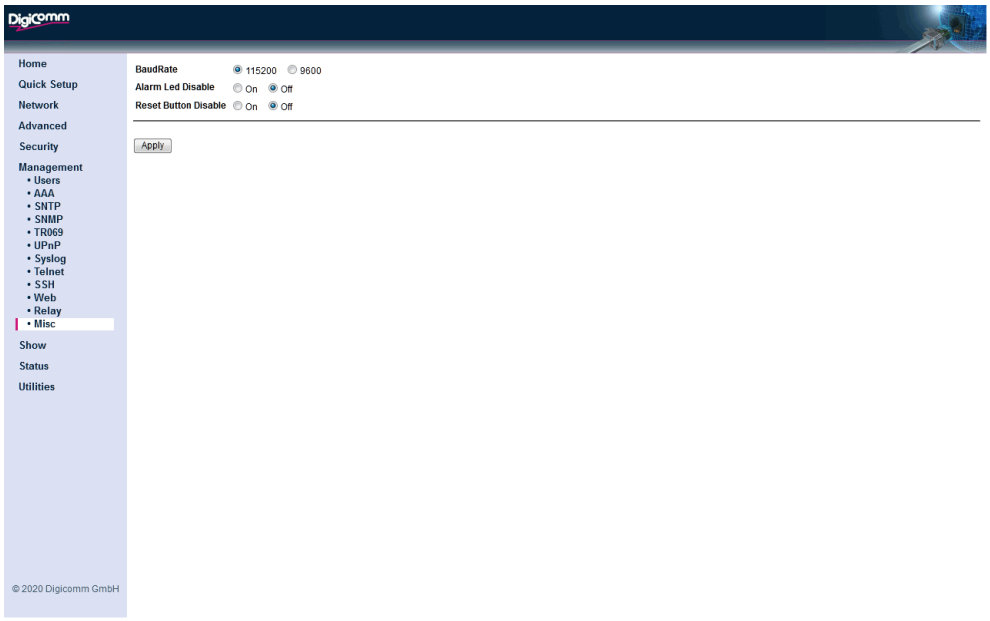
Enter Manual Mode	Sie können einen manuellen Testmodus aufrufen, indem Sie auf Schaltfläche „ Enter Manual Mode“ klicken. In diesem Modus wird das Relais manuell gesteuert. Sie können über die Optionsfelder Schließen (Close) oder Öffnen (Open) den Relais-Status ändern-
DSL Line	Disable (Deaktivieren) Any Das Relais schließt, sobald eine aktive Leitung ausfällt. All Das Relais schließt, sobald alle aktiven Leitungen ausfallen.
SNR/ Threshold	Das Signal-Rausch-Verhältnis ist ein in der Wissenschaft und Technik verwendeter Messwert, der die Stärke eines erwünschten Signals mit der Stärke der Hintergrundgeräusche vergleicht. Der Grenzwert kann in einem Bereich von 0 bis 15 dB festgelegt werden. Das Relais wird geschlossen, sobald der Modus aktiviert ist und der angegebene Threshold- Wert überschritten wird.
Attenuation/ Threshold	Der Grenzwert für die Dämpfung kann in einem Bereich von 1 bis 255 dB festgelegt werden. Das Relais wird geschlossen, sobald der Modus aktiviert ist und der angegebene Threshold- Wert überschritten wird.
CRC/ Threshold	Bei der CRC (zyklischen Redundanzprüfung) handelt es sich um einen Code zur Fehlererkennung, der häufig in digitalen Netzwerken und Speichergeräten verwendet wird, um zufällige Änderungen an Rohdaten erkennen zu können. Der Grenzwert für die zyklische Redundanzprüfung kann in einem Bereich von 1 bis 10000 festgelegt werden. Das Relais wird geschlossen, sobald der Modus aktiviert ist und der angegebene Threshold-Wert überschritten wird
Switch Port 1 bis 4 Mode	Disable (Deaktiviert) UP Das Relais schließt wenn der Port offen ist. Down Das Relais schließt wenn der Port nicht aktiv ist.

Mail

Bei einem offenen Mail-Relais handelt es sich um einen SMTP-Server, dessen Konfiguration einem beliebigen Benutzer im Internet den Versand von E-Mails über diesen Server erlaubt, und nicht nur den Empfang oder Versand von E-Mails durch bekannte Benutzer

Mode	Aktivieren/ Deaktivieren Sie das Senden von E-Mails wenn das Relais geschaltet wird.
SMTP Server	Geben Sie die IP-Adresse des E-Mail Servers ein.
User Name	Geben Sie das E-Mail Konto des Benutzers ein
Password	Geben Sie das Passwort des E-Mail Kontos an.
Sender	Geben Sie den Namen des E-Mail Absenders an.
Receiver	Geben Sie den Empfänger der E-Mail an.
Subject for Close	Geben Sie den „Betreff“ der E-Mail ein, wenn das Relais geschlossen wird.
Subject for Open	Geben Sie den „Betreff“ der E-Mail ein, wenn das Relais geöffnet wird.

6.12 Misc



Misc Parameter

Baud Rate	Wählen Sie zwischen 115200 oder 9600 aus
Alarm LED Disable	ON- Deaktivieren Sie die Alarm-LED-Funktion. Die Alarm-LED ist ausgeschaltet
Reset Button Disable	ON Deaktivieren Sie die Reset Funktion

7 Show

Über den Menüpunkt „Show“ kommen Sie auf die folgenden Menüpunkte:

1. Information
2. Syslog
3. Dhcpd Lease
4. Cpu Info
5. Scipt

7.1 Information

MCSV

MCSV: „MCSV“ steht für die Manufacture's Concurrent Software Version. Bei dieser Version handelt es sich um die ursprüngliche Werkseinstellung, die selbst nach einem Upgrade des Routers erhalten bleibt. Diese dient der internen Identifizierung.

Software Version: Firmware die aktuell auf dem Gerät ist

Chipset Name: Der Name und die Version des G.SHDSL-Chipsatzes.

DSL Chip Name:Der Name des G.SHDSL Chipsatzes

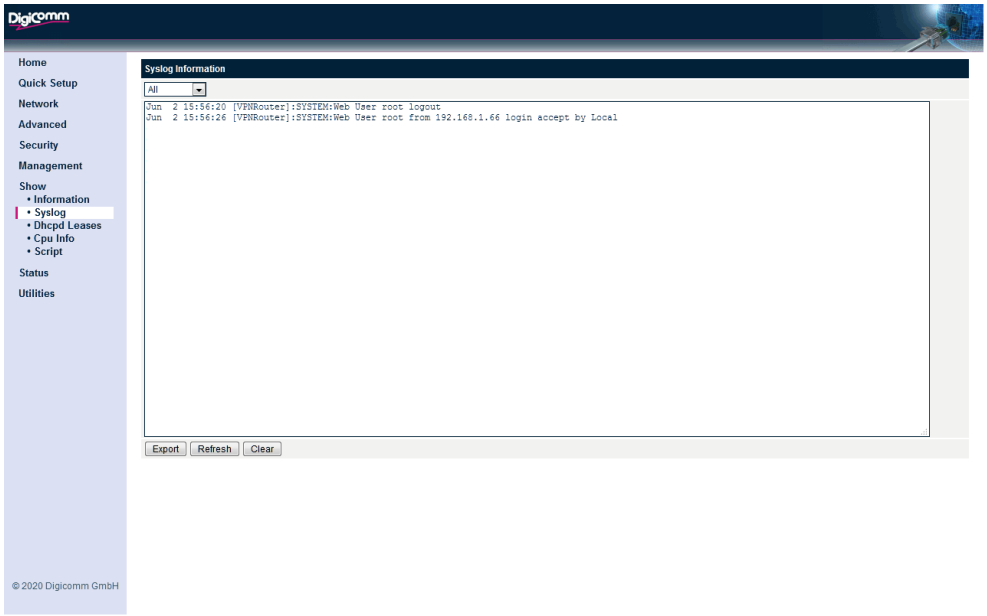
DSL phy/IDC Firmware Version: G.Shdsl Firmware Version

Current Time: Dieses Feld gibt das aktuelle Datum und die Uhrzeit des SHDTU‘s an.

System Up Time: Die Gesamtbetriebsdauer des SHDTU‘s.

7.2 Syslog

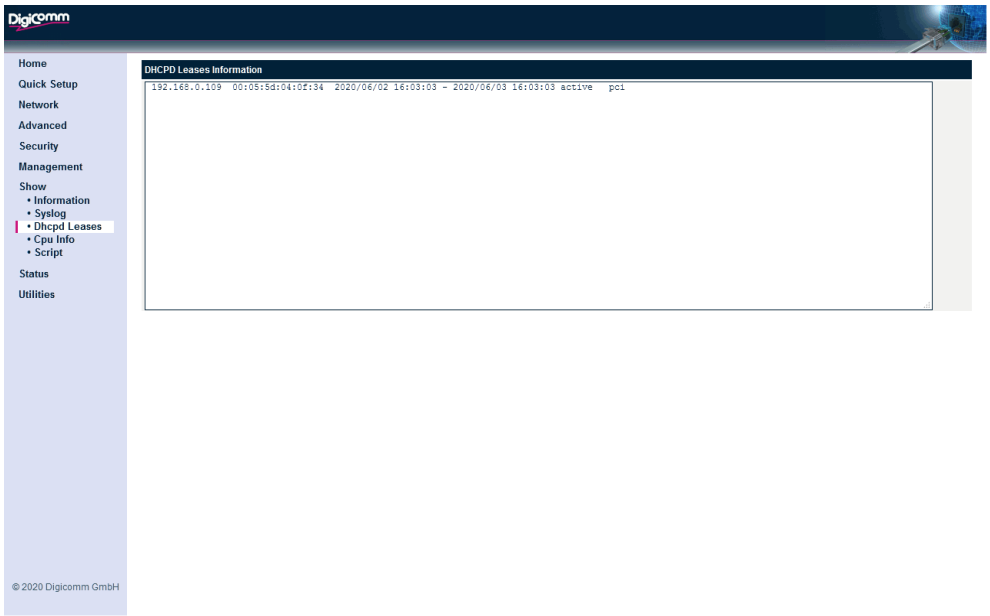
Die Funktion „SysLog“ zeigt alle Systemprotokolle an.



Klicken Sie auf „Export, um den Download des Log-Files zu starten
Klicken Sie auf „Refresh“, um die Ansicht zu aktualisieren
Klicken Sie auf „Clear“, um die Ansicht zu löschen.

7.3 Dhcpd Lease

Wenn der DHCP- Server aktiviert ist, werden auf dieser Seite die DHCP-Clients/Hosts angezeigt



7.4 CPU Info

Load Average (Durchschnittliche Ladezeit)
Durchschnittliche Ladezeit 1 Minute, 5 Minuten und 15 Minuten

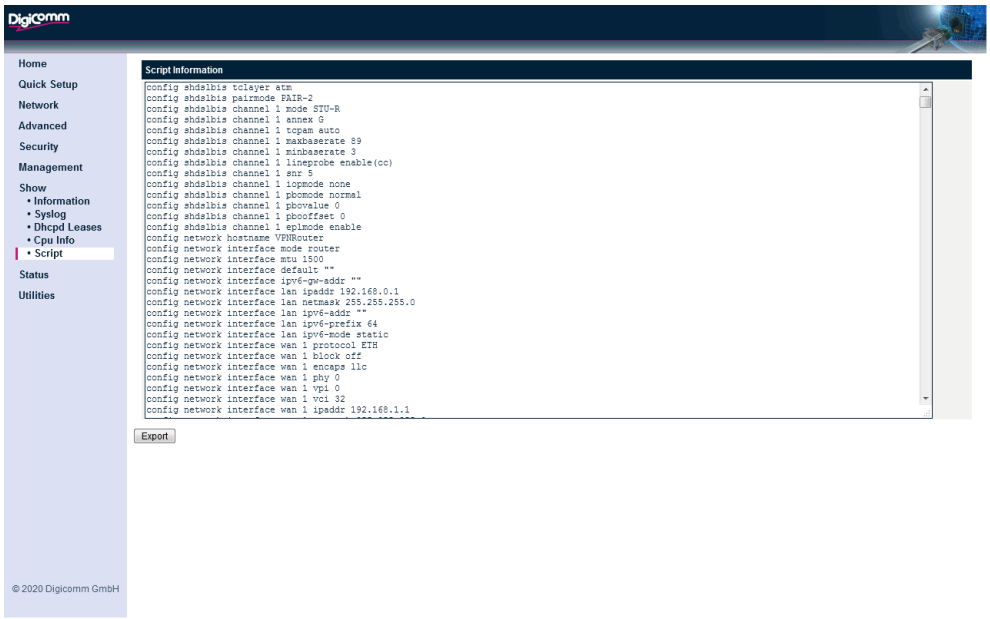
Memory (Speicher)
Speichernutzung: Total (insgesamt), Used (belegter Speicher), Free (freier Speicherplatz), Buffers (Puffer) und Cached (zwischengespeichert)

CPU

CPU Informationen

7.5 Script

Hier finden Sie die aktuelle Konfiguration des Gerätes in „Skript-Form“ und kann per Export-Button exportiert werden.



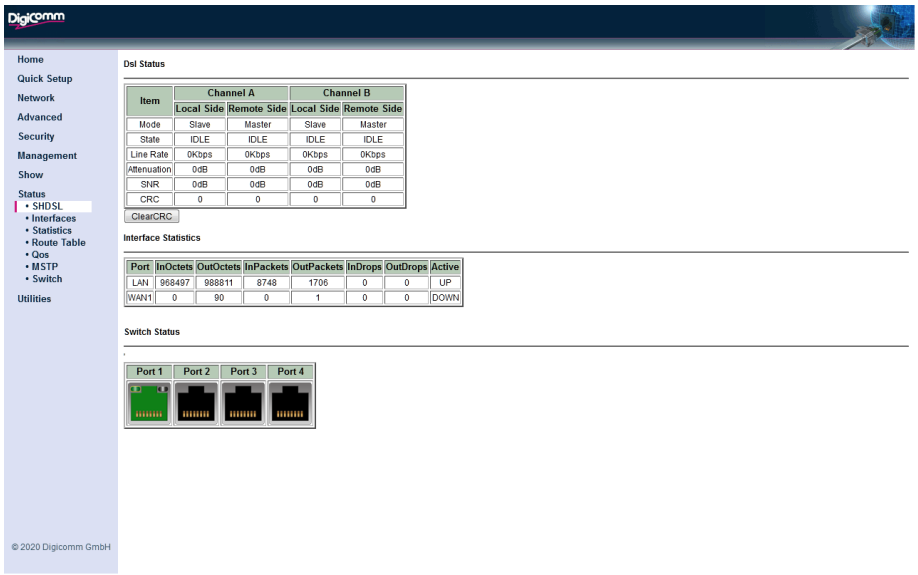
8 Status

Über den Menüpunkt „Status“ kommen Sie auf die folgenden Menüpunkte:

1.SHDSL
2.Interfaces
3.Statistics
4. Route Table
5. Qos
6. MSTP
7. Switch

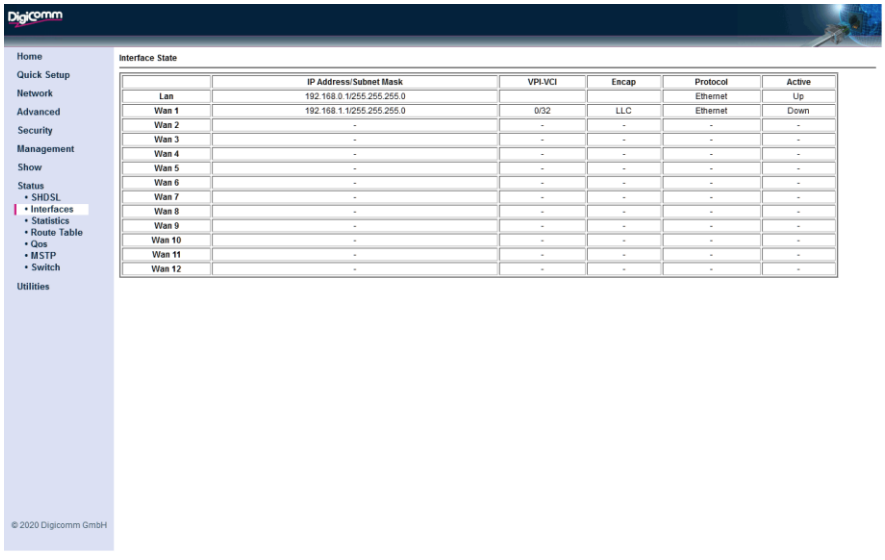
8.1 SHDSL

Unter SHDSL wird der DSL-Status, die Schnittstellenstatistik und die Zusammenfassung des Switch-Status angezeigt. Wenn Sie auf Clear CRC (CRC löschen) klicken, wird die Anzahl der CRC-Fehler gelöscht.



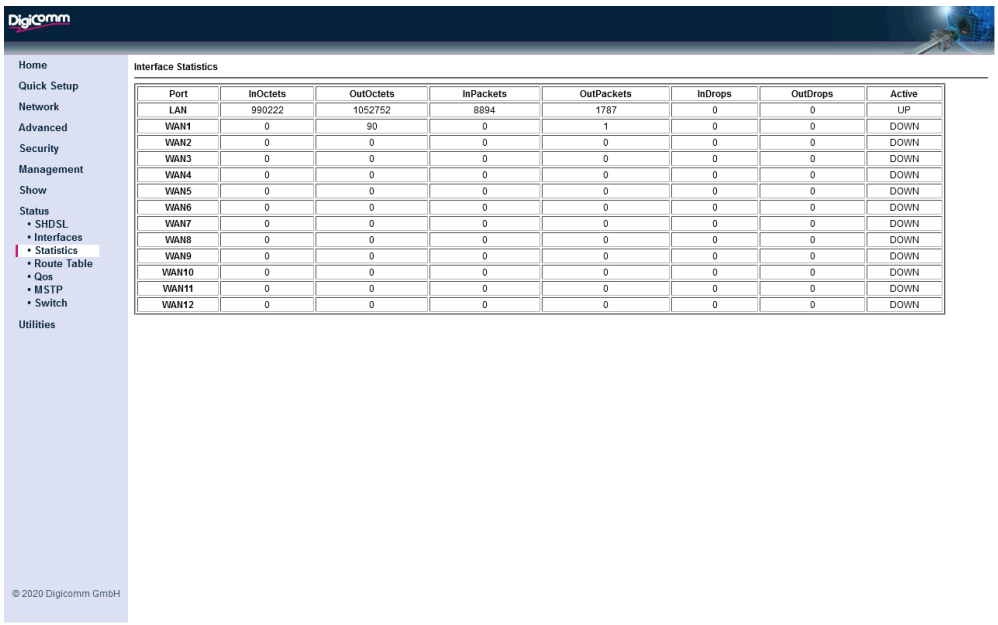
8.2 Interfaces (Schnittstellen)

Unter dem Menüpunkt „Interfaces“ wird der gesamte Schnittstellenstatus angezeigt.



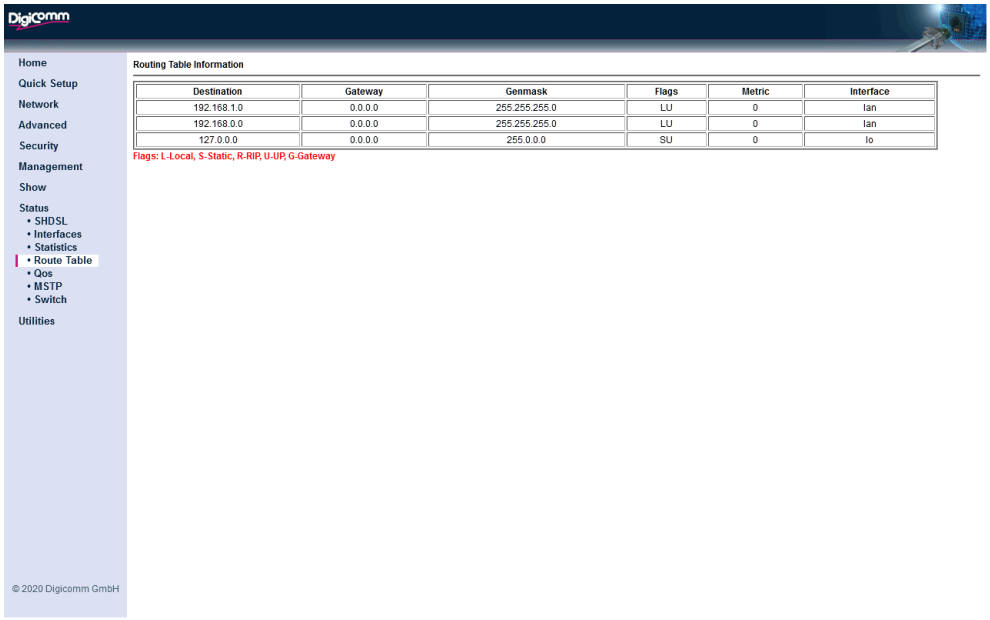
8.3 Statistics (Statistik)

Unter dem Menüpunkt „Statistics“ wird der gesamte Schnittstellenstatus angezeigt.



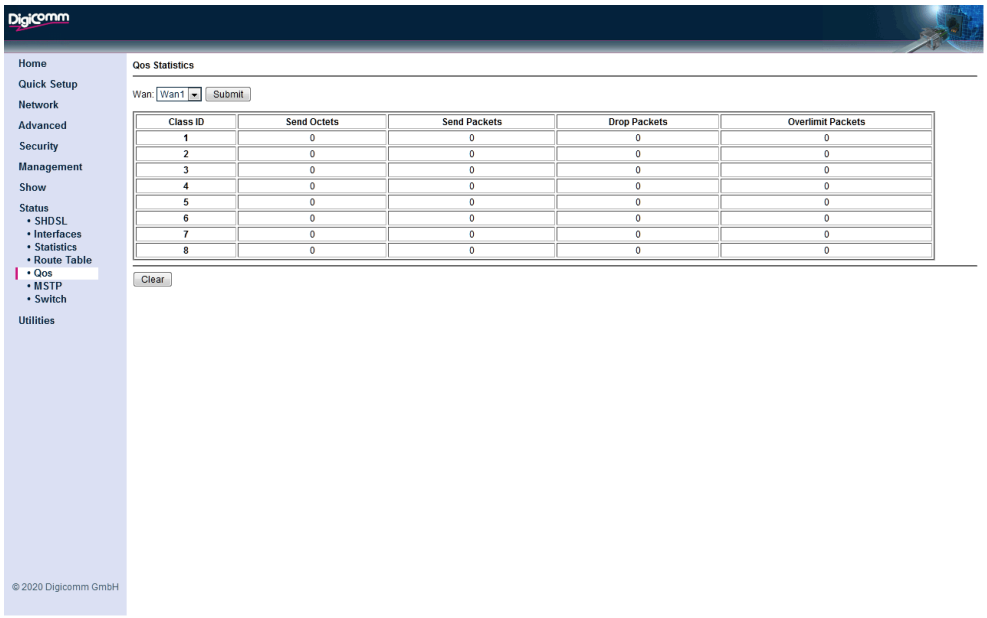
8.4 Route Table (Routing Tabelle)

Unter dem Menüpunkt „Route Table“ werden alle statischen/ dynamischen Routing-Informationen angezeigt.



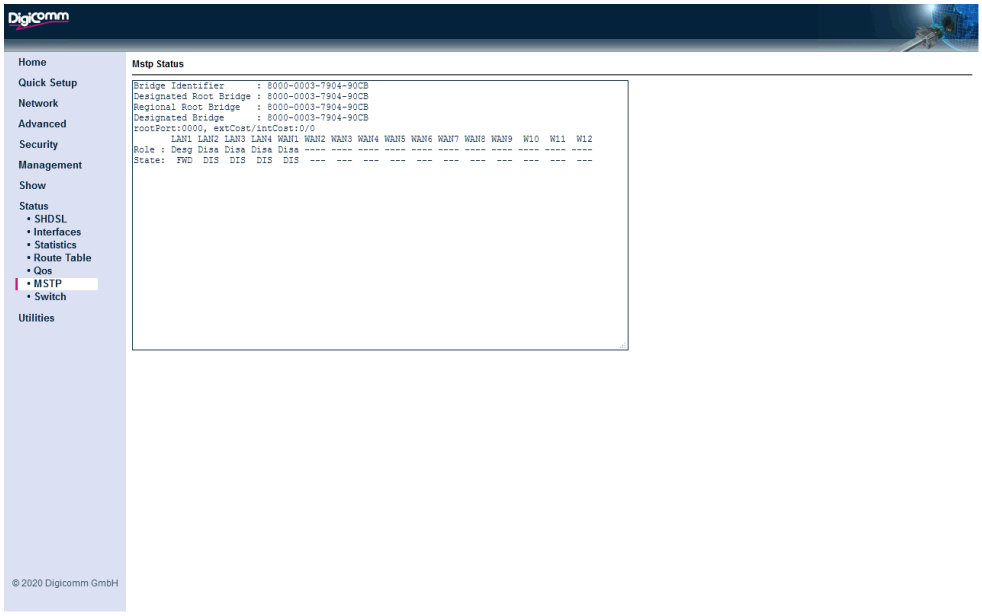
8.5 Qos (Quality of Service)

Wenn Qos aktiviert ist, werden auf dieser Seite die QOS-Klassen- / Warteschlangenstatistiken angezeigt.



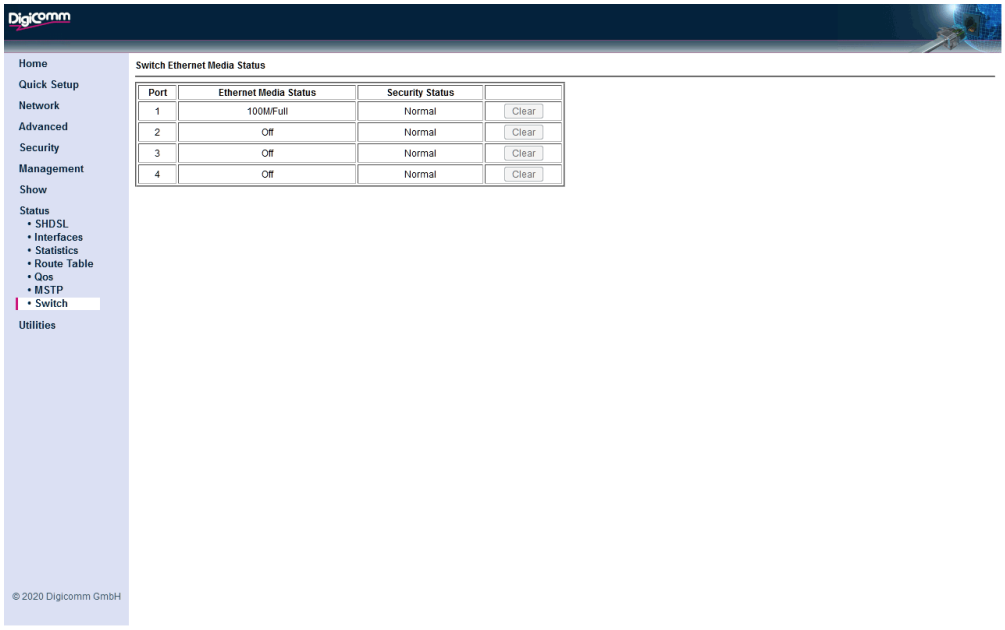
8.6 MSTP

Wenn STP aktiviert ist, zeigt die Seite den aktuellen STP/ Port-Status an.



8.7 Switch

VPN Router zeigt den Switch-Port-Status auf der Seite an. Wenn sich der Port im Sperrzustand befindet, klicken Sie auf die Schaltfläche „Löschen“, um ihn zu löschen.


Digicomm
Home
Quick Setup
Network
Advanced
Security
Management
Show
Status
• SHDSL
• Interfaces
• Statistics
• Route Table
• Qos
• MSTP
• Switch
Utilities
© 2020 Digicomm GmbH
Switch Ethernet Media Status
Port
Ethernet Media Status
Security Status
1
100M/Full
Normal
Clear
2
Off
Normal
Clear
3
Off
Normal
Clear
4
Off
Normal
Clear

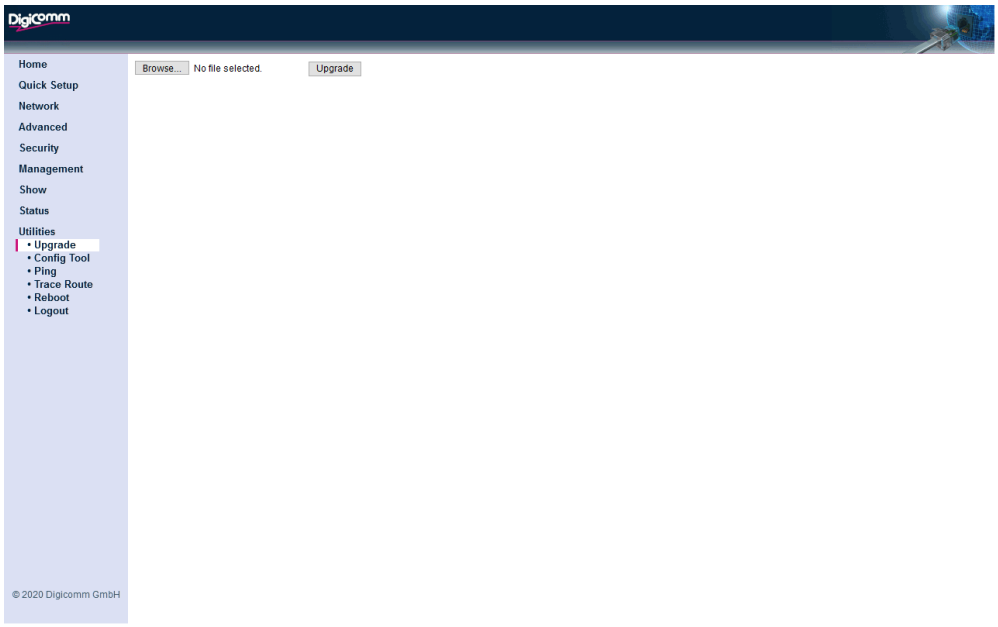
9 Utilities

Über den Menüpunkt „Utilities“ kommen Sie auf die folgenden Menüpunkte:

1. Upgrade
2. Config Tool
3. Ping
4. Trace Route
5. Reboot
6. Logout

9.1 Upgrade

Klicken Sie auf den Button „Browse“ und wählen die Datei aus, die Sie auf das Gerät einspielen möchten. Klicken Sie anschließend auf den Button „Upgrade“ um das Firmware-Upgrade zu starten.



9.2 Config Tool (Konfigurations Tool)

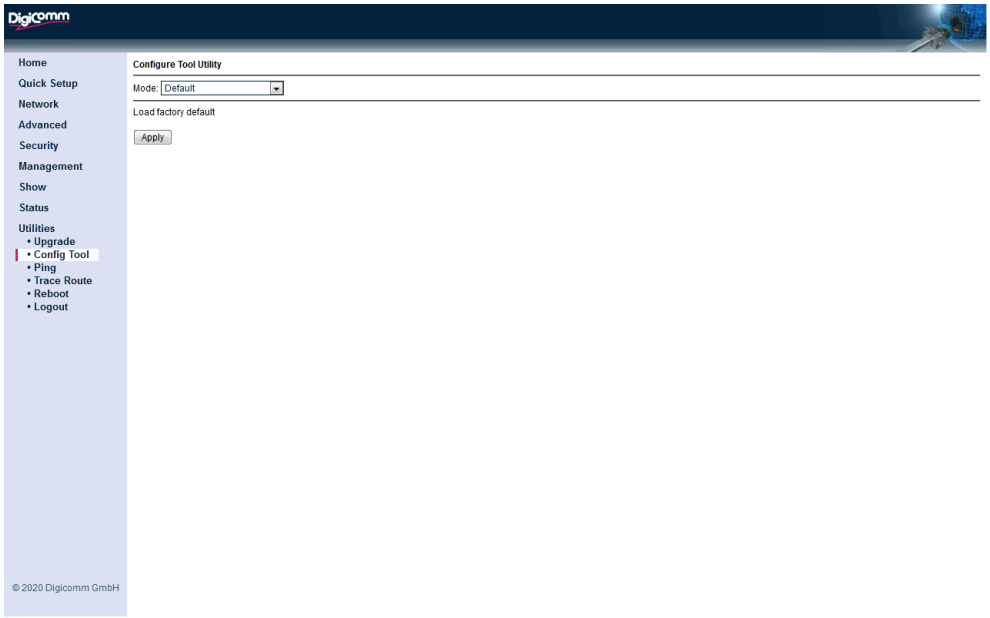
Über den Menüpunkt „Config Tool“ können Sie die Standardkonfigurations-, Sicherungs- und Wiederherstellungskonfigurationsdatei laden.

9.2.1 Config/ Load Default

Wählen Sie „Default“ um auf die Einstellungsseite aufzurufen.

Klicken Sie auf „Apply/ Bestätigen“, um den Standardladevorgang zu starten.

Hinweis: Das Gerät wird nach dem Laden der Standardkonfiguration automatisch neu gestartet.

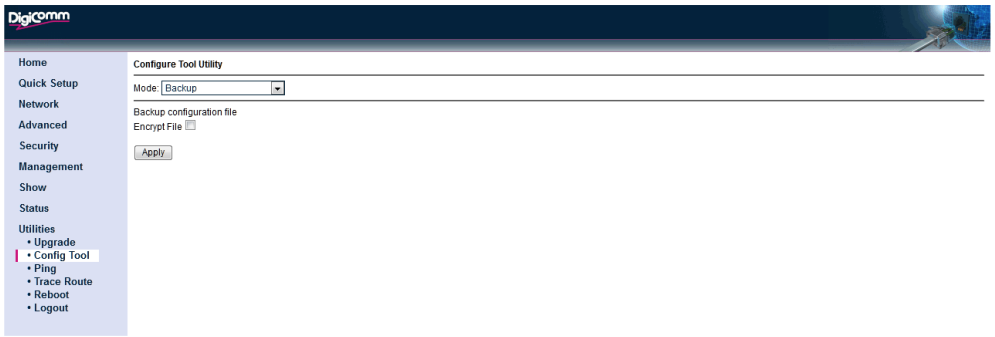


9.2.2 Config/ Backup (Sicherung)

Wählen Sie „Backup“ um die Einstellungsseite aufzurufen.

Klicken Sie auf „Apply/ Bestätigen“, und die aktuelle Konfiguration des Gerätes wird auf den PC heruntergeladen.

Die „Sicherungsdatei“ wird verschlüsselt, wenn das Kontrollkästchen " Encrypt File Verschlüsselungsdatei" aktiviert ist.

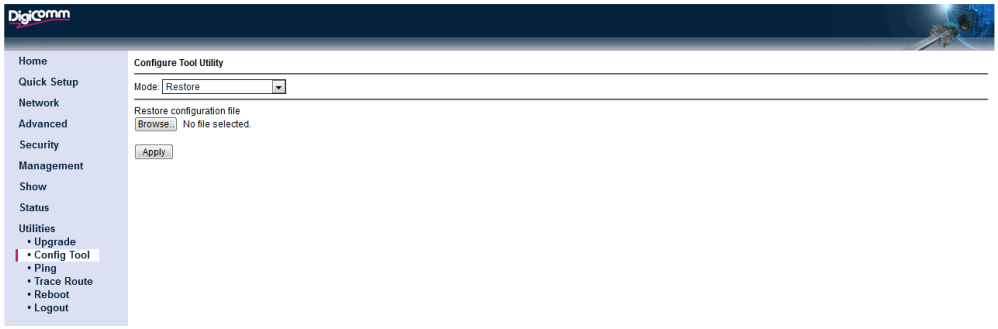


9.2 3 Config/ Restore (Wiederhestellen)

Wählen Sie „Restore“ um die Einstellungsseite aufzurufen.

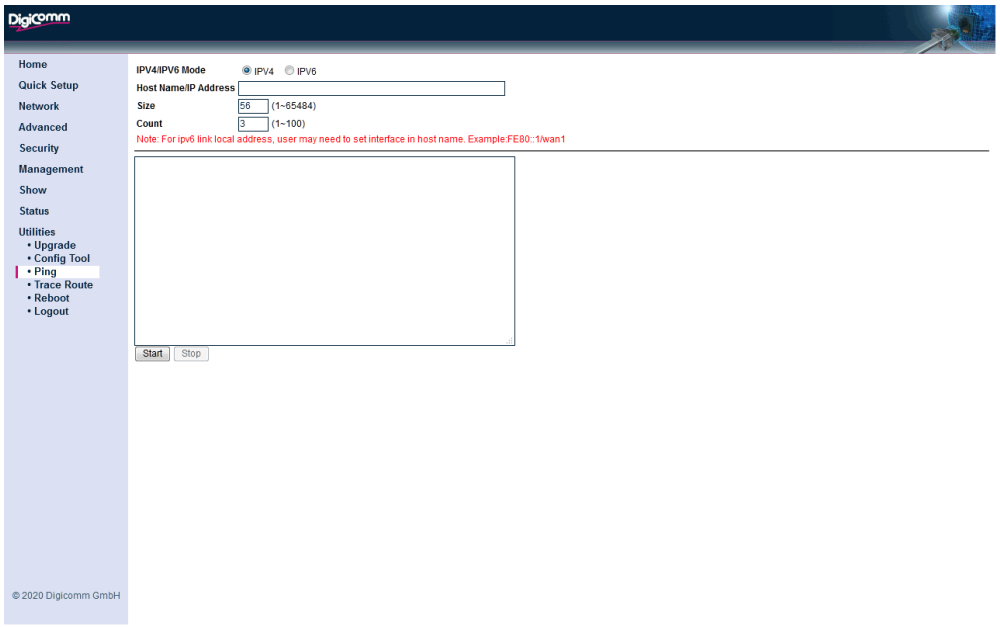
Klicken Sie auf die Schaltfläche „Browse“ (Durchsuchen), um die wiederherzustellende Konfigurationsdatei auszuwählen, klicken Sie dann auf die Schaltfläche „Apply“ (Übernehmen) und bestätigen Sie den Vorgang, um den Wiederherstellungsvorgang zu starten.

Hinweis: Das Gerät wird nach der Wiederherstellung der Konfigurationsdatei automatisch neu gestartet. Beim Wiederherstellen werden sowohl verschlüsselte Dateien als auch nicht verschlüsselte Dateien akzeptiert.



9.3 Ping

Das SHDTU unterstützt das Ping-Tool zur Diagnose.



Ping Parameter

IPv4/ IPv6 Wählen Sie zwischen IPv4 und IPv6 aus
Host Name/ IP Address Ping-Ziel in Hostname oder IP-Adresse

Size Ping Paketgröße
Count Ping Zähler

9.4 Trace Route

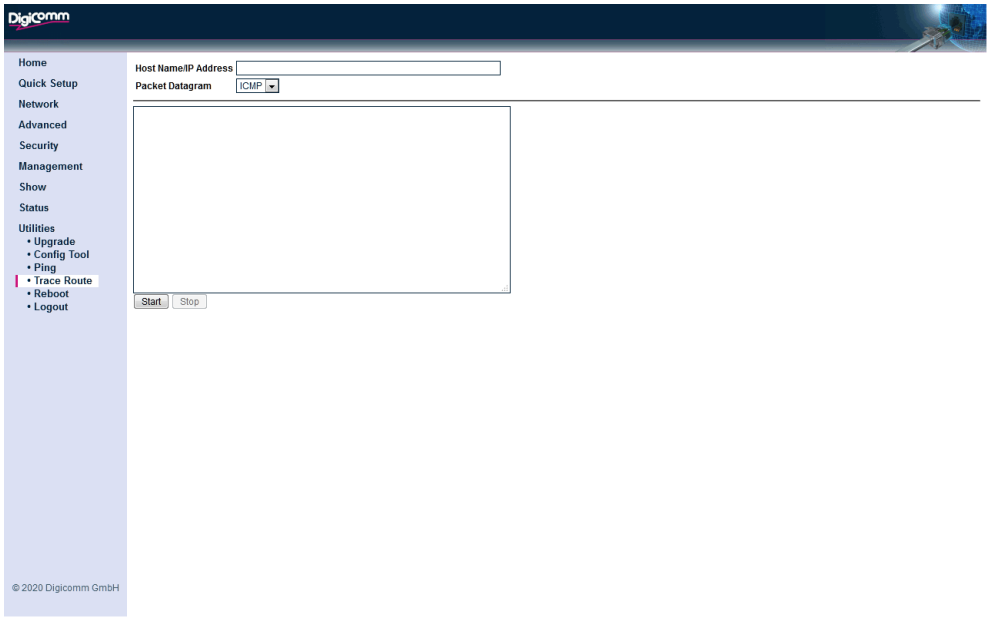
Das SHDTU unterstützt das Trace-Route Tool zur Diagnose.

Mithilfe des Befehls „Trace Route“ lässt sich nachverfolgen, welchen Weg die Datenpakete über das Netzwerk von Internet-Routern nehmen, während sie vom SHDTU an die Zieladresse weitergeleitet werden. Die „Länge“ der Netzwerkverbindung wird durch die Zahl der Internet-Router im Trace-Route-Pfad angegeben.

Dieser Befehl eignet sich für die Diagnose langsamer Netzwerkverbindungen. Falls Sie beispielsweise eine Seite im Internet in der Regel problemlos aufrufen können, sie heute jedoch sehr langsam reagiert, kann Ihnen der an diese Seite gerichtete Befehl „Trace Route“ einen oder mehrere Hops mit entsprechend langen Zeiten anzeigen. Oder Sie erhalten die Markierung „*“ – diese weist darauf hin, dass die Verbindung extrem

langsam ist. In diesem Fall liegt das für die Verzögerung verantwortliche Problem bei Ihrem Internetanbieter oder einem Backbone Provider und Sie haben wohl keine andere Wahl, als sich in Geduld zu üben.

Host name oder IP: Geben Sie den Hostnamen und die IP-Adresse an, an die der Ping gerichtet werden soll.
Update Interval: Legen Sie die Anzahl an Sekunden fest, die auf eine Antwort vom jeweiligen Host gewartet werden soll.



Trace Route Parameter

Host Name/ IP Address	Ziel Hostname oder IP-Adresse
Packet Datagram	ICMP oder UDP

9.5 Reboot

Klicken Sie auf das „Reboot“ Menü und bestätigen Sie den Vorgang wenn das Gerät neu gestartet werden soll.

9.6 Logout

Klicken Sie auf das „Logout“ Menü und bestätigen Sie den Vorgang wenn Sie sich ausloggen möchten.

10 Abkürzungsverzeichnis

EoA (Ethernet über ATM)

Das EoA (Ethernet-over-ATM)-Protokoll dient zur Übertragung von Daten zwischen zwei Local Area Networks, die das Ethernet-Protokoll verwenden und Wide Area Networks, in denen das ATM-Protokoll zum Einsatz kommt. In vielen Netzwerken der Telekommunikationsbranche wird das ATM-Protokoll verwendet. Bietet ein Internetanbieter DSL-Dienste an, nutzt er hierfür häufig das EoA-Protokoll für die Datenübertragung an die DSL-Modems seiner Kunden.

EoA kann für die Herstellung einer Bridge-Verbindung zwischen einem DSL-Modem und dem Internetanbieter verwendet werden. Mithilfe einer Bridge-Verbindung lassen sich Daten zwischen dem Netzwerk eines Internetanbieters und dem seiner Kunden austauschen, als würden sich die Netzwerke im gleichen physischen LAN befinden. Bridge-Verbindungen verwenden kein IP-Protokoll. Mithilfe von EoA ist auch die Konfiguration einer gerouteten Verbindung zum Internetanbieter möglich, die für den Datenaustausch das IP-Protokoll verwendet

IPoA (Dynamic IP over ATM)

IPoA (Dynamic IP over ATM)-Schnittstellen übertragen IP-Pakete über AAL5. AAL5 bietet den IP-Hosts im gleichen Netzwerk die Datenverbindungsschicht für die Kommunikation. Zudem müssen die IP-Pakete etwas überarbeitet werden, um diesen Hosts die Kommunikation in den gleichen ATM-Netzwerken zu ermöglichen. Als Träger-Netzwerk von IP-Diensten bietet ATM extrem schnelle Punkt-zu-Punkt-Verbindungen, was die Bandbreitenleistung eines IPNetzwerks deutlich verbessert. Auf der anderen Seite gewährleistet ATM eine hervorragende Netzwerkleistung und optimales QoS.

PPPoA/ PPPoE

Bei PPPoA (Point-to-Point Protocol over ATM) und PPPoE (Point-to-Point Protocol over Ethernet) handelt es sich um Authentifizierungs- und Verbindungsprotokolle, die von vielen Anbietern für einen Breitband-Internetzugang verwendet werden. Diese Spezifikationen dienen der Verbindung mehrerer Computerbenutzer in einem Ethernet Local Area Network mit einer Remote-Site über herkömmliche Teilnehmeranschlussgeräte, womit Telefongesellschaften ein Modem und ähnliche Geräte bezeichnen. PPPoE und PPPoA können in Büros oder Privatgebäuden eingesetzt werden. Benutzer greifen gemeinsam über eine herkömmliche Telefonleitung (Digital Subscriber Line, DSL), ein Kabelmodem oder eine Wireless-Verbindung auf das Internet zu. PPPoE und PPPoA kombinieren das häufig für Einwahlverbindungen verwendete Point-to-Point Protocol (PPP) mit dem Ethernet- oder ATMProtokoll, das Unterstützung für mehrere Benutzer in einem Local Area Network bietet. Die PPP-Protokolldaten werden in einem Ethernet-Frame oder ATM-Frame eingekapselt.

VPI

VPI (Virtual Path Identifier) wird zum Einrichten von permanenten virtuellen ATM-Kanälen (PVC) verwendet.

VCI

Die Virtual Channel Identifier wird zum Einrichten von permanenten virtuellen ATM-Kanälen (PVC) verwendet.

Sie brauchen technische Unterstützung?

Unser Support-Team hilft Ihnen gerne weiter:

Telefon +49 (0)2159/ 693 75-50
E-Mail: support@digicomm.de

AddSecure GmbH
Breite Str. 10
40670 Meerbusch