



NetModule AG Router NB3800

Yazılım Sürümü 4.8.0.104 için Kullanıcı Kılavuzu



Sürüm 2.2087

NetModule AG, Switzerland

28 Ocak 2025



NetModule AG Yönlendirici NB3800

Bu kılavuz, NB3800 ürün tipinin tüm varyantlarını kapsar.

Bu kılavuzda telif hakkıyla korunan ticari markaların adlandırılması, özel olarak belirtilmemiş olsa bile, bu adların ticari marka ve ticari ad koruma yasası anlamında özgür olarak kabul edilebileceği ve dolayısıyla herkes tarafından serbestçe kullanılabilmesi anlamına gelmemelidir.

Telif Hakkı ©2025 NetModule AG, İsviçre

Tüm hakları saklıdır

Kılavuzlar ve yazılımlar telif hakkıyla korunmaktadır. Tüm hakları saklıdır. Kopyalama, çoğaltma, çevirme, herhangi bir elektronik ortama veya makinede taranabilir forma dönüştürme, bütünüyle veya kısmen izin verilmez. Bir istisna, kendi kullanımınız için yazılımın bir yedek kopyasının hazırlanmasıdır.

Burada açıklanan performans özellikleri, yalnızca sözleşme yapılırken açıkça kararlaştırılmışsa bağlayıcıdır. Bu belge, NetModule AG tarafından şirketin bilgisi dahilinde üretilmiştir. NetModule AG, bu belgenin içeriğini önceden haber vermeden değiştirme hakkını saklı tutar. NetModule AG, bu belgedeki bilgilerin doğruluğu veya kesinliği konusunda hiçbir garanti veremez.

NetModule AG, ağ bileşenlerinin veya ilişkili işletim yazılımının kullanımından kaynaklanan hasarlardan sorumlu tutulamaz. Ayrıca, lisans sözleşmesinde belirtilen kullanım koşullarına atıfta bulunuyoruz.

Ürün, diğer şeylerin yanı sıra, üçüncü taraflarca geliştirilen ve Açık Kaynak Yazılım lisansı altında lisanslanan Açık Kaynak Yazılım dosyalarını içerir, 3. bölüme bakın.

Bize ulaşın

<https://support.netmodule.com>

NetModule AG
Maulbeerstrasse 10
CH-3011 Bern
İsviçre

Tel +41 31 985 25 10
Faks +41 31 985 25 11
info@netmodule.com
<https://www.netmodule.com>



İçerikler

1. NetModule'e Hoş Geldiniz.....	6
2. Uygunluk.....	7
2.1. Güvenlik Talimatları.....	7
2.2. Uygunluk Bildirimi.....	9
2.3. Atık Bertarafı.....	12
2.4. Ulusal Kısıtlamalar.....	12
3. FOSS.....	13
3.1. Üründe kullanılan Açık Kaynak Yazılım.....	13
3.2. Açık Kaynak Yazılımın daha fazla kullanımına ilişkin garanti.....	13
3.3. Tersine Mühendislik İzni (sadece LGPL lisanslı bileşenler için).....	14
Teşekkürler.....	14
4. Spesifikasyonlar.....	15
4.1. Görünüm.....	15
4.2. Özellikler.....	16
4.3. Çevresel Özellikler.....	17
4.4. Arayüzler.....	18
4.4.1. Genel Bakış.....	18
4.4.2. LED Göstergeler.....	20
4.4.2. Ethernet LED Göstergeleri.....	21
4.4.3. Yeniden Başlatma.....	21
4.4.4. Mobil.....	21
4.4.5. WLAN.....	22
4.4.6. GNSS.....	23
4.4.7. USB 2.0 Host Port.....	24
4.4.8. M12 Ethernet Konektör.....	24
4.4.9. Güç Kaynağı.....	25
4.4.10. Genişletme Yuvaları.....	27
4.5. Veri Depolama (Seçenek “Dx”).....	33
5. Kurulum.....	35
5.1. Micro-SIM (3FF) Kart Kurulumu.....	35
5.2. WWAN Antenlerinin Kurulumu.....	35
5.3. WLAN Antenlerinin Kurulumu.....	38
5.5. GNSS Anteni Kurulumu.....	38
5.6. Yerel Alan Ağı (LAN) Kurulumu.....	38
5.6. Güç Kaynağının Kurulumu.....	39
5.7. Ses Arayüzünün Kurulumu.....	39
6. Yapılandırma.....	40
6.1. İlk Adımlar.....	40
6.1.1. İlk Erişim.....	40
6.1.2. Otomatik Mobil Veri Bağlantısı.....	41
6.1.3. Kurtarma (Recovery).....	41
6.2. ANASAYFA (Home).....	43
6.3. ARAYÜZLER.....	45
6.3.1. WAN.....	45
6.3.2. Ethernet.....	50
6.3.3. Mobil.....	59
6.3.4. WLAN.....	65
6.3.5. Yazılım Köprüleri (Software Bridges).....	73
6.3.6. USB.....	74
6.3.7. Seri Haberleşme.....	76



6.3.8. Ses (Audio).....	78
6.3.9. GNSS.....	79
6.4. YÖNLENDİRME (ROUTING).....	82
6.4.1. Statik Rotalar.....	82
6.4.2. Genişletilmiş Yönlendirme.....	84
6.4.3. Çoklu Yol Rotaları (Multipath Routes).....	85
6.4.4. Multicast.....	86
6.4.5. BGP.....	87
6.4.6. OSPF.....	88
6.4.7. Mobile IP.....	89
6.4.8. Quality Of Service (Servis Kalitesi).....	91
6.5. GÜVENLİK DUVARI (FIREWALL).....	93
6.5.1. Yönetim.....	93
6.5.2. Adres/Port Grupları.....	93
6.5.3. Kurallar.....	94
6.5.4. NAPT.....	95
6.6. VPN.....	98
6.6.1. OpenVPN.....	98
6.6.2. IPSec.....	104
6.6.3. PPTP.....	110
6.6.4. GRE.....	113
6.6.5. L2TP.....	114
6.6.6. Dial-In.....	115
6.7. Servisler (Services).....	116
6.7.1. SDK.....	116
6.7.2. DHCP Sunucu.....	123
6.7.3. DNS Sunucu.....	125
6.7.4. NTP Sunucu.....	126
6.7.5. Dinamik DNS (Dynamic DNS).....	127
6.7.6. E-Posta (E-Mail).....	129
6.7.7. Etkinlikler (Events).....	130
6.7.8. SMS.....	131
6.7.9. SSH/Telnet Sunucu.....	133
6.7.10. SNMP Ajanı (SMNP Agent).....	135
6.7.11. Let's Encrypt.....	140
6.7.12. Web Sunucu (Web Server).....	141
6.7.13. MQTT Broker.....	142
6.7.14. Softflow.....	143
6.7.15. Keşif (Discovery).....	144
6.7.16. Yedeklilik (Redundancy).....	145
6.7.17. ITxPT.....	147
6.7.18. Ses Ağ Geçidi (Voice Gateway).....	155
6.7.19. Erişim Denetimcisi WLAN-AP (Access Controller WLAN-AP).....	159
6.7.20. Hotspot.....	167
6.8. SİSTEM.....	174
6.8.1. Sistem.....	174
6.8.2. Kimlik Doğrulama (Authentication).....	180
6.8.3. Yazılım Güncelleme (Software Update).....	183
6.8.4. Modül Donanım Yazılımı Güncelleme (Module Firmware Update).....	184
6.8.5. Yazılım Profilleri (Software Profiles).....	184
6.8.6. Yapılandırma.....	185
6.8.7. Sorun giderme (Troubleshooting).....	188
6.8.8. Anahtarlar ve Sertifikalar (Keys and Certificates).....	191



6.8.9. Lisanslama (Licensing).....	196
6.8.10. Yasal Uyarı.....	197
6.9. ÇIKIŞ (LOGOUT).....	198
7. Komut Satırı Arayüzü (Command Line Interface).....	199
7.1. Genel Kullanım.....	200
7.2. Yardım.....	201
7.3. Yapılandırma Parametrelerinin Alınması.....	201
7.4. Yapılandırma Parametrelerinin Yazılması.....	201
7.5. Yapılandırmanın Tamamlandığını Kontrol Etme.....	202
7.6. Durum Bilgilerinin Alınması.....	202
7.7. Ağları Tarama.....	203
7.8. E-posta veya SMS Gönderme.....	203
7.9. Sistem Güncelleme.....	203
7.10. Anahtarları ve Sertifikaları Yönet.....	204
7.11. Servisleri Yeniden Başlatmak.....	204
7.12. Hata Ayıklama.....	205
7.13. Sistemi Sıfırlama.....	205
7.14. Sistemi Yeniden Başlatma.....	205
7.15. Kabuk Komutlarını Çalıştırma.....	205
7.16. Komut Geçmişi.....	206
7.17. CLI-PHP.....	206
A. Ek.....	211
A.1. Kısaltmalar.....	211
A.2. Sistem Olayları (System Events).....	213
A.3. Fabrika Yapılandırması.....	215
A.4. SNMP VENDOR MIB.....	216
A.5. SDK Örnekleri.....	217


1. NetModule'e Hoş Geldiniz

Bir NetModule AG ürünü satın aldığınız için teşekkür ederiz. Bu belge size cihaz ve özellikleri hakkında bir giriş sağlamalıdır. Aşağıdaki bölümler, cihazın devreye alınması, kurulum prosedürü ile ilgili tüm yönleri açıklar ve yapılandırma ve bakıma yönelik yararlı bilgiler sağlar. Örnek SDK betikleri veya yapılandırma örnekleri gibi daha fazla bilgiyi şu adresteki wiki'mizde bulabilirsiniz: <https://wiki.netmodule.com>

2. Uygunluk

Bu bölümde yönlendiricinin çalıştırılmasına ilişkin genel bilgiler verilmektedir.

2.1. Güvenlik Talimatları

Lütfen kılavuzda  sembolüyle işaretlenmiş tüm güvenlik talimatlarına dikkatlice uyun.



Uyumluluk Bilgileri:

- NetModule yönlendiricileri, iletişim modülünün öngörülen uygulama ve ortamlarda kullanımını düzenleyen tüm geçerli ulusal ve uluslararası yasalara ve özel kısıtlamalara uygun şekilde kullanılmalıdır.



Cihazdaki aksesuarlar/değişiklikler hakkında bilgi:

- Yaralanmaları ve sağlık risklerini önlemek için lütfen yalnızca orijinal aksesuarları kullanın.
- Cihazda yapılan değişiklikler veya yetkisiz aksesuarların kullanımı garantiyi geçersiz kılacak ve potansiyel olarak çalışma lisansını geçersiz kılacaktır.
- NetModule cihazları açılmamalıdır (SIM kartlar talimatlara göre kullanılabilir).

**Cihazdaki arayüzler hakkında bilgi:**

- NetModule yönlendirici arayüzlerine bağlı tüm sistemler SELV (Safety Extra Low Voltage, Güvenlik Ekstra Düşük Voltaj) sistemleri için gereklilikleri karşılamalıdır.
- Bağlantılar binadan çıkmamalı veya bir aracın gövde kabuğuna nüfuz etmemelidir.
- Anten bağlantıları yalnızca geçici aşırı gerilimler (IEC 62368-1'e göre) harici koruma devreleri tarafından 1500 V_{Peak}'e kadar sınırlandırılırsa binadan veya araç gövdesinden çıkabilir. Diğer tüm bağlantılar bina veya araç gövdesi içinde kalmalıdır.
- Takılan antenler her zaman insanlardan en az 40 cm uzakta olmalıdır.
- Tüm antenler birbirinden en az 20 cm uzakta olmalıdır; kombine antenler (mobil radyo / WLAN / GNSS) durumunda, radyo teknolojileri arasında yeterli izolasyon olmalıdır.
- WLAN arayüzüne sahip cihazlar yalnızca geçerli Düzenleyici Alan (Regulatory Domain) yapılandırıldığında çalıştırılabilir. Ülkeye, anten sayısına ve anten kazancına özel dikkat gösterilmelidir (ayrıca bkz. bölüm 6.3.4). Daha yüksek amplifikasyona sahip WLAN antenleri, sertifikalı uzman personel tarafından doğru şekilde yapılandırılmış NetModule yönlendirici "Gelişmiş-RF-Yapılandırma (Enhanced-RF-Configuration)" yazılım lisansı ve anten kazancı ve kablo zayıflaması ile kullanılabilir. Yanlış yapılandırma, onayın kaybedilmesine yol açacaktır.
- Bir antenin maksimum kazancı (bağlantı kablolarının zayıflaması dahil) ilgili frekans aralığında aşağıdaki değerleri aşmamalıdır:
 - Mobil radyo (600MHz .. 1GHz) < 3,2dBi,
 - Mobil radyo (1,7GHz .. 2GHz) < 6,0dBi
 - Mobil radyo (2,5GHz .. 4,2GHz) < 6,0dBi
 - WiFi (2,4GHz .. 2,5GHz) < 3,2dBi, WiFi (5,1GHz .. 5,9GHz) < 4,5dBi
- GNSS sinyallerinin kötü niyetli üçüncü taraf cihazlar tarafından gizlenebileceğini veya engellenebileceğini unutmayın.
- NetModule yönlendiricileriyle yalnızca akım sınırlı SELV çıkış voltaj aralığına sahip CE uyumlu güç kaynakları kullanılabilir¹.
- Güç Kaynağı Sınıfı 3 (PS3) güç kaynağı (100 W veya daha fazla) yalnızca yönlendiriciye giden güç kablosunda bir kablo gerginlik giderici uygulanması koşuluyla kullanılabilir. Bu tür bir kablo gerginlik giderici, yönlendirici vida terminali konektöründeki tellerin bağlantısının kesilmemesini sağlar (örneğin, bir hata koşulu altında yönlendirici kabloya dolanacaktır). Kablo gerginlik giderici, yönlendiricinin kablosuna uygulanan 30 N'luk (1 kg'a kadar yönlendirici ağırlığı için) bir çekme kuvvetine dayanmalıdır.

¹Not: Pb seçeneği (72-110 VDC) olan yönlendiriciler için güç kaynakları, voltaj 60 VDC'den büyük olduğundan SELV devresi olamaz.

**FCC Uyarısı:**

- Uyumluluktan sorumlu tarafça açıkça onaylanmayan herhangi bir Değişiklik veya modifikasyon, kullanıcının ekipmanı çalıştırma yetkisini geçersiz kılabilir.
- Bu cihaz, FCC Kuralları'nın 15. bölümüne uygundur. Çalıştırma aşağıdaki iki koşula tabidir:
 - (1) Bu cihaz zararlı girişime neden olamaz ve
 - (2) bu cihaz, istenmeyen çalışmaya neden olabilecek girişim dahil olmak üzere alınan herhangi bir girişimi kabul etmelidir.
- Not: Bu ekipman, FCC Kuralları'nın 15. bölümüne uygun olarak B Sınıfı dijital cihaz için sınırlara uygun olduğu test edilmiş ve bulunmuştur. Bu sınırlar, konut kurulumunda zararlı girişime karşı makul koruma sağlamak üzere tasarlanmıştır. Bu ekipman, radyo frekansı enerjisi üretir ve yayabilir ve talimatlara uygun şekilde kurulmaz ve kullanılmazsa radyo iletişimlerinde zararlı girişime neden olabilir. Ancak, belirli bir kurulumda girişimin oluşmayacağına dair bir garanti yoktur. Bu ekipman radyo veya televizyon alımında zararlı parazite neden oluyorsa, bu durum ekipmanı kapatıp açarak belirlenebilir, kullanıcının paraziti aşağıdaki önlemlerden bir veya daha fazlasıyla düzeltmeye çalışması önerilir:
 - Alıcı anteni yeniden yönlendirin veya yerini değiştirin.
 - Ekipman ile alıcı arasındaki mesafeyi artırın.
 - Ekipmanı, alıcının bağlı olduğu devreden farklı bir devredeki prize bağlayın.
 - Yardım için bayiye veya deneyimli bir radyo/TV teknisyenine danışın.
 - Maruz Kalma Gereksinimleri: FCC RF maruz kalma uyumluluk gereksinimlerine uymak için, cihaz tüm kişilerden en az 40 cm'lik bir ayırma mesafesi sağlayacak şekilde kurulmalıdır.

**Genel güvenlik talimatları:**

- Akaryakıt istasyonlarında, kimyasal tesislerde, patlayıcı veya potansiyel olarak patlayıcı yerlerdeki sistemlerde radyo ünitelerinin kullanım sınırlamalarına uyun.
- Cihazlar uçaklarda kullanılamaz.
- Kalp pilleri ve işitme cihazları gibi kişisel tıbbi cihazların yakınında özellikle dikkatli olun.
- NetModule yönlendiricileri ayrıca televizyon setlerinin, radyo alıcılarının ve kişisel bilgisayarların yakın mesafesinde parazite neden olabilir.
- Bir fırtına sırasında asla anten sistemi üzerinde çalışma yapmayın.
- Cihazlar genellikle normal iç mekan kullanımı için tasarlanmıştır. Cihazları IP40'tan daha kötü olağanüstü çevre koşullarına maruz bırakmayın.
- Bunları agresif kimyasal atmosferlere ve belirtilenlerin dışındaki nem veya sıcaklıklara karşı koruyun.
- Çalışan bir sistem yapılandırmasının bir kopyasını oluşturmanızı şiddetle öneririz. Daha sonra daha yeni bir yazılım sürümüne kolayca uygulanabilir.

2.2. Uygunluk Bildirimi

NetModule cihazları, tedarik edildikleri formda ve amaçlanan kullanım sırasında, AB Radyo Ekipmanı Direktifi 2014/53/EU'nun temel gerekliliklerine uygundur. İmzalı Uygunluk Beyanı <https://www.netmodule.com/downloads> adresinden edinilebilir.

Aşağıda, RED Direktifi 2014/53/EU, Madde 10 (8a, 8b)'ye göre, çalışma frekans bantları ve iletilen ilgili maksimum radyo frekans gücü gösterilmektedir.

WLAN maksimum çıkış gücü

IEE 802.11b/g/n

Çalışma frekans aralığı: 2412-2472 MHz (13 kanal)

Maksimum çıkış gücü: 14,93 dBm EIRP ortalaması (anten portunda)

IEE 802.11a/n/ac

Çalışma frekans aralığı: 5180-5350 MHz / 5470-5700 MHz (19 kanal)

Maksimum çıkış gücü: 22,91 dBm EIRP ortalaması (anten portunda)

Hücresel maksimum çıkış gücü

GSM Band 900

Çalışma frekans aralığı: 880-915, 925-960 MHz

Maksimum çıkış gücü: 33,5 dBm nominal

GSM Band 1800

Çalışma frekans aralığı: 1710-1785, 1805-1880 MHz

Maksimum çıkış gücü: 30,5 dBm nominal

WCDMA Band I

Çalışma frekans aralığı: 1920-1980, 2110-2170 MHz

Maksimum çıkış gücü: 25,7 dBm nominal

WCDMA Band III

Çalışma frekans aralığı: 1710-1785, 1805-1880 MHz

Maksimum çıkış gücü: 25,7 dBm nominal

WCDMA Band VIII

Çalışma frekans aralığı: 880-915, 925-960 MHz

Maksimum çıkış gücü: 25,7 dBm nominal

LTE FDD Band 1

Çalışma frekans aralığı: 1920-1980, 2110-2170 MHz

Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 3

Çalışma frekans aralığı: 1710-1785, 1805-1880 MHz

Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 7

Çalışma frekans aralığı: 2500-2570, 2620-2690 MHz

Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 8

Çalışma frekans aralığı: 880-915, 925-960 MHz

Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 20

Çalışma frekans aralığı: 832-862, 791-821 MHz

Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 28

Çalışma frekans aralığı: 703-748, 758-803
Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 38
Çalışma frekans aralığı: 2570-2620 MHz
Maksimum çıkış gücü: 25 dBm nominal

LTE FDD Band 40
Çalışma frekans aralığı: 2300-2400 MHz
Maksimum çıkış gücü: 25 dBm nominal

5G NR Band 1
Çalışma frekans aralığı: 1920-1980, 2110-2170 MHz
Maksimum çıkış gücü: 25 dBm nominal

5G NR Band 3
Çalışma frekans aralığı: 1710-1785, 1805-1880 MHz
Maksimum çıkış gücü: 25 dBm nominal

5G NR Band 7
Çalışma frekans aralığı: 2500-2570, 2620-2690 MHz
Maksimum çıkış gücü: 25 dBm nominal

5G NR Band 8
Çalışma frekans aralığı: 880-915, 925-960 MHz
Maksimum çıkış gücü: 25 dBm nominal

5G NR Band 20
Çalışma frekans aralığı: 832-862, 791-821 MHz
Maksimum çıkış gücü: 25 dBm nominal

5G NR Band 28
Çalışma frekans aralığı: 703-748, 758-803 MHz
Maksimum çıkış gücü: 25 dBm derecelendirilmiş

5G NR Band 38
Çalışma frekans aralığı: 2570-2620 MHz
Maksimum çıkış gücü: 25 dBm derecelendirilmiş

5G NR Band 40
Çalışma frekans aralığı: 2300-2400 MHz
Maksimum çıkış gücü: 25 dBm dereceli

5G NR Band 77
Çalışma frekans aralığı: 3300-4200 MHz
Maksimum çıkış gücü: 25 dBm dereceli

5G NR Band 78
Çalışma frekans aralığı: 3300-3800 MHz
Maksimum çıkış gücü: 25 dBm dereceli



2.3. Atık Bertarafı



Lütfen cihazınızın kullanım ömrü dolduktan sonra, normal atıklardan ayrı olarak, Avrupa Parlamentosu ve Konseyinin 2012/19/AB sayılı Atık Elektrikli ve Elektronik Ekipman (AEEE) [Waste Electrical and Electronic Equipment (WEEE)] Direktifi uyarınca uygun bir toplama noktası aracılığıyla bertaraf edilmesini sağlayın.

2.4. Ulusal Kısıtlamalar

Bu ürün genel olarak tüm AB ülkelerinde (ve RED Direktifi 2014/53/EU'yu takip eden diğer ülkelerde) herhangi bir sınırlama olmaksızın kullanılabilir. Belirli bir ülke için daha fazla ulusal radyo arayüzü düzenlemesi ve gereksinimi almak için lütfen WLAN Düzenleme Veritabanımıza bakın.

3. FOSS

Bu bölümde FOSS (Free Open Source Software, Özgür Açık Kaynak Yazılım) hakkında bilgi verilmektedir.

3.1. Üründe kullanılan Açık Kaynak Yazılım

Bu ürün, üçüncü taraflarca geliştirilen ve açık kaynak lisanslarıyla sunulan bazı yazılımlar içermektedir. Bu yazılımlar telif hakkıyla korunur ve kullanım haklarınız, ilgili açık kaynak lisanslarına tabidir. Bu lisanslara uymanız, yazılımı yasal olarak kullanmanızı sağlar.

Ürüne ait diğer NetModule AG lisans koşulları ile açık kaynak lisans koşulları arasında bir çelişki olursa, açık kaynak lisans şartları geçerli olur.

Açık kaynak yazılımlar için herhangi bir ücret talep edilmez. Üründe yer alan açık kaynak bileşenler ve bunların lisans bilgileri şu yollarla görüntülenebilir:

- Web Arayüzü: SYSTEM > Legal Notices > Licenses
- Komut Satırı: /usr/local/share/license

Eğer ürünle birlikte verilen açık kaynak yazılımlardan herhangi biri GNU Genel Kamu Lisansı (General Public License, GPL), GNU Daha Az Genel Kamu Lisansı (Lesser General Public License, LGPL) veya benzeri bir lisans altındaysa ve kaynak kodları ürünle birlikte sağlanmadıysa:

Ürünü satın aldıktan sonraki 3 yıl boyunca, sadece kargo ve işlem ücreti karşılığında bu yazılımların kaynak kodunu NetModule AG'den talep edebilirsiniz.

Bunun için: Ürünün etiketinde bulunan isim ve kimlik numarası ile birlikte, satın alma tarihinden itibaren 3 yıl içinde, aşağıdaki adrese başvurabilirsiniz:

“NetModule AG, Head of R and D, Maulbeerstrasse 10, 3011 Bern, Switzerland” alternatif olarak, teknik destek birimimize şu adresten ulaşabilirsiniz: “support@netmodule.com”

3.2. Açık Kaynak Yazılımın daha fazla kullanımına ilişkin garanti

NetModule AG, bu üründe yer alan Açık Kaynak Yazılımın, amaçlanan kullanım dışında kullanılmasından doğabilecek sorunlar için garanti vermez. Yazılımın lisansları, varsa, ilgili yazar veya lisans sahiplerinin sağladığı garantileri belirtir. NetModule AG, yazılım veya ürün yapılandırmasında yapılan değişikliklerden kaynaklanan hatalar için sorumluluk kabul etmez. Ayrıca, Açık Kaynak Yazılımın üçüncü tarafların fikri mülkiyet haklarını ihlal etmesi durumunda NetModule AG'ye karşı herhangi bir garanti talebi ileri sürülemez. GPL ve LGPL bileşenleri için geçerli olan feragatname şöyledir: “Bu program, faydalı olacağı umuduyla dağıtılmaktadır, ancak HERHANGİ BİR GARANTİ VERİLMEMEKTEDİR; özellikle SATILABİLİRLİK veya BELİRLİ BİR AMACA UYGUNLUK garantisi ima edilmemektedir. Daha fazla bilgi için GNU Genel Kamu Lisansı ve GNU Daha Az Genel Kamu Lisansı'na bakınız.”

Geriye kalan açık kaynaklı bileşenler için, ilgili lisans metinlerindeki hak sahiplerinin sorumluluk istisnaları geçerlidir. Varsa, teknik destek yalnızca değiştirilmemiş yazılımlar için sağlanacaktır.



3.3. Tersine Mühendislik İzni (sadece LGPL lisanslı bileşenler için)

Müşteriye bu izni vermek için, ürünün tüm üçüncü taraf yazılım tedarikçileri NetModule AG'ye de bu izni vermelidir.

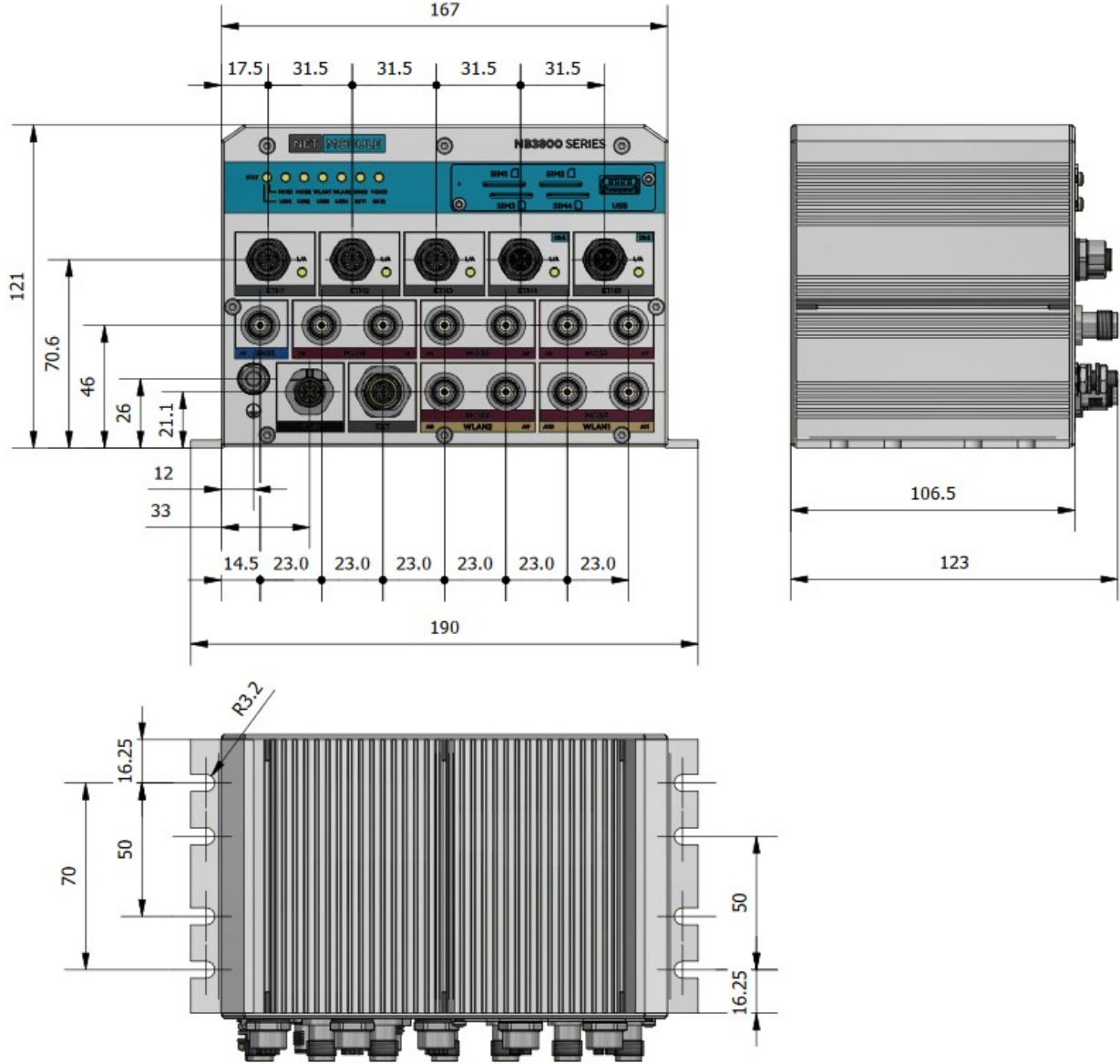
Yalnızca açık kaynaklı bir lisansa uymak için gerekli ölçüde, Lisans Sahibi, Son Kullanıcıların NB180 yazılımını kendi kullanımı için değiştirmesine ve bu tür değişiklikleri hata ayıklamak için tersine mühendislik yapmasına izin verebilir. Ancak, Lisans Sahibi Son Kullanıcıyı kısıtlamalıdır ve Son Kullanıcının tersine mühendislik veya hata ayıklama sırasında edinilen bilgiyi üçüncü taraflara iletmesi yasaktır. Ayrıca, Lisans Sahibi Son Kullanıcıyı kısıtlamalıdır ve Son Kullanıcının NB180 yazılımının değiştirilmiş sürümlerini dağıtması yasaktır. Her durumda, Son Kullanıcılar bu değişiklikler olmadan da kusurun oluşacağını kanıtlayamadığı sürece NB180 yazılımı üzerindeki garanti talepleri sona erecektir.

Teşekkürler

- PHP, <http://www.php.net> adresinden ücretsiz olarak edinilebilir
- OpenSSL Toolkit'te kullanılmak üzere OpenSSL Projesi tarafından geliştirilen yazılım (<http://www.openssl.org>)
- Eric Young (eay@cryptsoft.com) tarafından yazılan kriptografik yazılım
- Tim Hudson (tjh@cryptsoft.com) tarafından yazılan yazılım
- Jean-loup Gailly ve Mark Adler tarafından yazılan yazılım
- RSA Data Security, Inc. tarafından MD5 Mesaj Özeti Algoritması
- Dr. Brian Gladman tarafından yayımlanan koda dayalı AES şifreleme algoritmasının bir uygulaması
- David Ireland tarafından orijinal olarak yazılan çoklu hassasiyetli aritmetik kod
- The FreeBSD Project'ten (<http://www.freebsd.org>) yazılım

4. Spesifikasyonlar

4.1. Görünüm



4.2. Özellikler

NB3800'ün tüm modelleri aşağıdaki standart işlevlere sahiptir:

- Galvanik olarak izole edilmiş güç kaynağı
- 2x Gbit Ethernet portu (M12, x kodlu)
- 3x Hızlı Ethernet portu (M12, d kodlu)
- 1x USB 2.0 ana bilgisayar portu
- 4x mini SIM kart yuvası (2FF)
- 1x Genişletme portu

NB3800 aşağıdaki seçeneklerle donatılabilir:

- 5G, LTE, UMTS, GSM
- WLAN IEEE 802.11
- GPS/GNSS
- GSM-R
- RS-232
- RS-485
- IBIS
- CAN
- Ses
- 1 TB dahili depolama
- Yazılım Anahtarları

Modüler yaklaşımı sayesinde NB3800 yönlendirici ve donanım bileşenleri, girintili kullanım veya uygulamaya göre keyfi olarak monte edilebilir. Özel proje gereksinimleriniz olması durumunda lütfen bizimle iletişime geçin.

4.3. Çevresel Özellikler

Parametre	Değerler
Giriş Voltajı (Varyant Pa)	24 V _{DC} ila 48 V _{DC} (±30%)
Giriş Voltajı (Varyant Pb)	72 V _{DC} ila 110 V _{DC} (±30%)
Çalışma Sıcaklığı Aralığı	Standart : -25°C ile +70°C arası 24-48 VDC: EN50155 TX (-40 ° C ila +70 ° C) maks. 4 radyo modülüyle 24-48 VDC: EN50155 T1 (-25 ° C ila +55 ° C) maks. 6 radyo modülüyle 72-110 VDC: EN50155 TX (-40 ° C ila +70 ° C) maks. 4 radyo modülüyle 72-110 VDC: EN50155 T2 (-40 ° C ila +55 ° C) maks. 5 radyo modülüyle
Depolama Sıcaklığı Aralığı	-40°C ila +85°C
Nem	0 ila %95 (yoğuşmasız)
Rakım (Varyant Pa)	4000m'ye kadar
Rakım (Varyant Pb)	2000m'ye kadar
Aşırı Gerilim Sınıfı	I
Kirlilik Derecesi	2
Giriş Koruma Sınıfı	IP40 (SIM ve USB kapakları takılıyken)

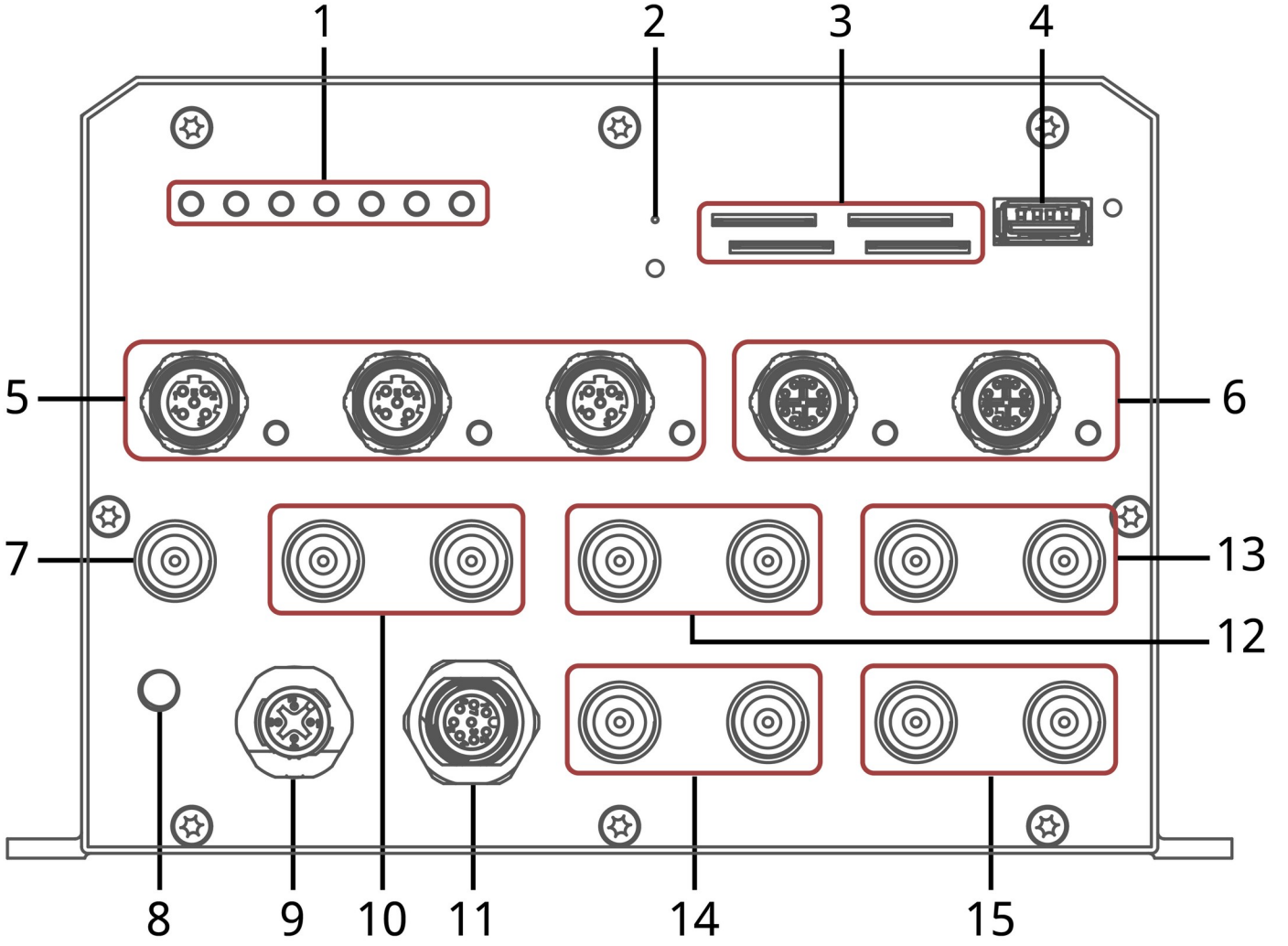
Tablo 4.1.: Çevresel Koşullar


**Dikkat:**

- NB3800-*****Pb-* Varyantı işlevsel yalıtım olarak kabul edilir ve takviyeli veya çift yalıtımla şebeke ES3 devresinden ayrılmış izole şebeke dışı ES3 (elektrik enerjisi kaynağı sınıfı 3) devresine takılması amaçlanmıştır
- Pb varyantını 60 VDC'den yüksek bir giriş voltajıyla kullanırken, yönlendirici bir toprak korumasına BAĞLANMALIDIR.

4.4. Arayüzler

4.4.1. Genel Bakış



No	Etiket	İşlev
1	LED Göstergeler	Farklı arayüzler için LED göstergeleri
2	Reset	Yeniden başlatma ve fabrika ayarlarına sıfırlama düğmesi
3	SIM 1-4	SIM 1-4 (2FF), yapılandırma ile herhangi bir modeme dinamik olarak atanabilir.
4	USB	USB 2.0 ana bilgisayar portu, yazılım/yapılandırma güncellemeleri için kullanılabilir.
5	ETH 1-3	Fast Ethernet portları, LAN veya WAN arayüzü içindir.
6	ETH 4-5	Gigabit Ethernet portları, LAN veya WAN arayüzü içindir.
7	GNSS	GPS/GLONASS anteni için TNC dişi konektör
8		M6 topraklama koruma konektörü, sistem GND'sine bağlanır. Güç kaynağına galvanik olarak izole edilir. Kullanılırsa, en az 6mm ² bakır alanlı sarı-yeşil işaretli bir kablo bağlayın. Korozyondan kaçının ve vidaları gevşemeye karşı koruyun.
9	PWR	Galvanik izolosayonlu güç kaynağı
10	MOB 1	MIMO hücresel anten için TNC dişi konektör
11	EXT	Galvanik olarak izole edilmiş uzatma portu M12 konektörü
12	MOB 2	MIMO hücresel anten için TNC dişi konektör
13	MOB 3	MIMO hücresel anten için TNC dişi konektör
14	MOB 4/WLAN 2	MIMO Mobil/WLAN anteni için TNC dişi konektörler
15	MOB 5/WLAN 1	MIMO Mobil/WLAN anteni için TNC dişi konektörler

Tablo 4.2.: NB3800 Arayüzleri

4.4.2. LED Göstergeler

Aşağıdaki tabloda NB3800 durum göstergeleri açıklanmaktadır.

Etiket	Renk	Durum	İşlev
STAT	●	Yanıp sönüyor	Cihaz başlatma, yazılım veya yapılandırma güncellemesiyle meşgul.
	●	Sürekli	Cihaz hazır. Üst sıradaki açıklamalar geçerlidir.
	●	Sürekli	Cihaz hazır. Alt sıradaki açıklamalar geçerlidir.
MOB 1	●●● ^[1]	Sürekli	Mobil bağlantı 1 aktif
	●	Yanıp sönüyor	Mobil bağlantı 1 kuruluyor
	○	Kapalı	Mobil bağlantı 1 kapalı
MOB 2	●●● ^[1]	Sürekli	Mobil bağlantı 2 aktif
	●	Yanıp sönüyor	Mobil bağlantı 2 kuruluyor
	○	Kapalı	Mobil bağlantı 2 kapalı
WLAN 1	●●● ^[1]	Sürekli	WLAN1 bağlantısı aktif
	●	Yanıp sönüyor	WLAN1 bağlantısı kuruluyor
	○	Kapalı	WLAN1 bağlantısı kapalı
WLAN 2	●●● ^[1]	Sürekli	WLAN2 bağlantısı aktif
	●	Yanıp sönüyor	WLAN2 bağlantısı kuruluyor
	○	Kapalı	WLAN2 bağlantısı kapalı
GNSS	●	Sürekli	GNSS açık ve geçerli bir NMEA akışı mevcut
	●	Yanıp sönüyor	GNSS uydularını arıyor
	○	Kapalı	GNSS kapalı
SES	●	Sürekli	Şu anda sesli arama etkin
	○	Kapalı	Aktif sesli arama yok
USR 1-5	●	Sürekli	Kullanıcı tanımlı
	○	Kapalı	Kullanıcı tanımlı
EXT 1-2	●	Sürekli	Genişletme yuvası 1 etkin
	○	Kapalı	Genişletme yuvası 1 kapalı

Tablo 4.3.: NB3800 Durum Göstergeleri

1 LED'in rengi kablosuz bağlantılar için sinyal kalitesini temsil eder.

● kırmızı düşük anlamına gelir

● sarı orta anlamına gelir

● yeşil iyi veya mükemmel anlamına gelir



4.4.2. Ethernet LED Göstergeleri

Aşağıdaki tabloda Ethernet durum göstergeleri açıklanmaktadır.

Etiket	Renk	Durum	İşlev
ETH 1-5	●	Sürekli	Bağlantı var (10 Mbit/s, 100 Mbit/s or 1000 Mbit/s)
	●	Yanıp sönüyor	Bağlantı var, aktivite var
	○	Kapalı	Bağlantı yok, aktivite yok

Tablo 4.4.: Ethernet Durum Göstergeleri

4.4.3. Yeniden Başlatma

Sıfırlama düğmesinin iki işlevi vardır:

1. Sistemi yeniden başlatma:
Sistemin yeniden başlatılmasını tetiklemek için en az 3 saniye basın.
Yeniden başlatma, kırmızı yanıp sönen STAT LED'yle gösterilir.
2. Fabrika ayarlarına sıfırlama:
Fabrika ayarlarına sıfırlamayı tetiklemek için en az 10 saniye basın.
Fabrika ayarlarına sıfırlamanın başlangıcı, tüm LED'lerin bir saniyeliğine yanması ile doğrulanır.

4.4.4. Mobil

NB3800'ün çeşitli varyantları mobil iletişim için 4'e kadar WWAN modülünü destekler. LTE modülleri 2x2 MIMO'yu destekler. 5G'li Variant, 4x4 MIMO'lu 2'ye kadar WWAN modülünü destekler. Farklı modemler ve bantlar hakkında bilgilere erişmek için [tıklayınız](#).

Mobil anten portları aşağıdaki özelliklere sahiptir:

Özellik	Değer
İzin verilen azami kablo uzunluğu (m)	30
4G-LTE için gerekli asgari anten sayısı	2
5G için gerekli asgari anten sayısı	4
Mobil radyo (600 MHz .. 1 GHz) < 3,2 dBi kablo zayıflaması dahil olmak üzere izin verilen azami anten kazancı	Mobil radyo (600MHz .. 1GHz) < 3,2dBi Mobil radyo (1,7GHz .. 2GHz) < 6,0dBi Mobil radyo (2,5GHz .. 4,2GHz) < 6,0dBi
Birlikte yerleştirilen radyo verici antenleri arasındaki minimum mesafe (cm)	20
İnsanlar ve antenler arasındaki minimum mesafe (cm)	40
Konnektör tipi	TNC

Tablo 4.5.: Mobil Anten Portu Spesifikasyonu

4.4.5. WLAN

NB3800'ün varyantları 2 adede kadar 802.11 a/b/g/n/ac WLAN modülünü destekler.

Standart	Frekans	Bant Genişliği	Azami Veri Transefer Hızı
802.11a	5 GHz	20 MHz	54 Mbit/s
802.11b	2.4 GHz	20 MHz	11 Mbit/s
802.11g	2.4 GHz	20 MHz	54 Mbit/s
802.11n	2.4/5 GHz	20/40 MHz	300 Mbit/s
802.11ac	5 GHz	20/40/80 MHz	867 Mbit/s

Tablo 4.6.: IEEE 802.11 Standartları

Not: 802.11n ve 802.11ac 2x2 MIMO'yu destekler.

WLAN anten portları aşağıdaki özelliklere sahiptir:

Özellik	Spesifikasyon
İzin verilen azami kablo uzunluğu	30 m
Kablo zayıflaması dahil izin verilen azami anten kazancı	3.2dBi (2,4 GHz) ve 4.5dBi (5 GHz) ¹
Yakın yerleştirilmiş radyo verici antenleri arasındaki asgari mesafe (Örnek: WLAN1 ila MOB1)	20 cm
İnsanlarla anten arasında korunması gereken asgari mesafe	40 cm
Konektör tipi	TNC

Tablo 4.7.: WLAN Bağlantı Noktası Spesifikasyonu

¹ **Not:** NetModule yönlendiricinin "Gelişmiş-RF-Yapılandırması" yazılım lisansı ve sertifikalı uzman personel tarafından doğru şekilde yapılandırılmış anten kazancı ve kablo zayıflaması ile daha yüksek amplifikasyona sahip WLAN antenleri kullanılabilir.

4.4.6. GNSS

GNSS (Opsiyon “G”)

GNSS WWAN Modülünden kullanılmaktadır.

Özellik	Spesifikasyon
Sistemler	GPS/GLONASS/GALILEO/BEIDOU
Veri akışı	JSON veya NMEA
İzleme hassasiyeti	-165 dBm’e kadar
Desteklenen antenler	Aktif veya Pasif

Tablo 4.8.: GNSS Spesifikasyonları (Seçenek “G”)

GNSS (Opsiyon “Gd”)

Özellik	Spesifikasyon
Sistemler	GPS/GLONASS/GALILEO/BEIDOU
Veri akışı	NMEA veya UBX
Kanal sayısı	72
İzleme hassasiyeti	-160 dBm’e kadar
Doğruluk	Azami 2.5m CEP
“Dead Reckoning” modları	UDR: Bağlanmamış Dead Reckoning ADR: Otomotiv Dead Reckoning
Desteklenen antenler	Aktif veya Pasif

Tablo 4.9.: GNSS Spesifikasyonları (Seçenek “Gd”)

GNSS anten portu aşağıdaki özelliklere sahiptir:

Özellik	Spesifikasyon
İzin verilen azami kablo uzunluğu	30 m
Anten LNA kazancı	15-20 dB tipik, 30 dB azami
Yakın yerleştirilmiş radyo verici antenleri arasındaki asgari mesafe (Örnek: GNSS ila MOB1)	20 cm
Konektör tipi	TNC

Tablo 4.10.: GNSS / GPS Anten Bağlantı Noktası Spesifikasyonu

4.4.7. USB 2.0 Host Port

USB 2.0 ana bilgisayar bağlantı noktası aşağıdaki özelliklere sahiptir:

Özellik	Spesifikasyon
Hız	Düşük, Tam ve Yüksek Hız
Akım	Azami 500 mA
Azami kablo uzunluğu	3 m
Kablo blendajı	Zorunlu
Konektör tipi	Tip A

Tablo 4.11.: USB 2.0 Ana Bilgisayar Bağlantı Noktası Özellikleri

4.4.8. M12 Ethernet Konektör

Spesifikasyon

Özellik	Spesifikasyon
İzolasyon	1500 V _{DC}
Hız	Fast Ethernet: 10/100 Mbit/s Gigabit Ethernet: 10/100/1000 Mbit/s
Mod	Half- & Full-Duplex
Geçiş	Otomatik MDI/MDI-X
Azami uzunluk	100 m
Kablo tipi	CAT5e veya data iyisi
Kablo blendajı	Zorunlu
Konektör tipi	Fast Ethernet: M12 d-coded Gigabit Ethernet: M12 x-coded

Tablo 4.12.: Ethernet Bağlantı Noktası Özellikleri

Kablo uçları (M12, 4 kutuplu, D kodlu dişi konektör)

Uç	Sinyal	Konektör
1	Tx+	
2	Rx+	
3	Tx-	
4	Rx-	

Tablo 4.13.: Ethernet Bağlantı Noktası Kablo Uçları (M12, 4 kutuplu, D kodlu dişi konektör)

Kablo uçları (M12, 8 kutuplu, X kodlu diři konektör)

Uç	Sinyal	Konektör
1	M1+ / DA+	
2	M1- / DA-	
3	M0+ / DB+	
4	M0- / DB-	
5	M2+ / DD+	
6	M2- / DD-	
7	M3- / DC-	
8	M3+ / DC+	

Tablo 4.14.: Ethernet Bağlantı Noktası Kablo Uçları (M12, 8 kutuplu, X kodlu diři konektör)

4.4.9. Güç Kaynağı

Standart varyant “Pa” (24 V_{DC} – 48 V_{DC})

Özellik	Spesifikasyon
Güç kaynağı nominal voltajları	24 V _{DC} , 36 V _{DC} ve 48 V _{DC} (EN 50155’e göre)
Voltaj aralığı	12 V _{DC} ve 48 V _{DC} ($\pm 30\%$)
Azami güç tüketimi	25 W
Tipik Ani Akım İntegrali	0.23 A ² s @ 24 V _{in} , 0.57 A ² s @ 36 V _{in} , 1.05 A ² s @ 48 V _{in}
Azami kablo uzunluğu	30 m
Kablo blendajı	Zorunlu değil
Galvonik izolasyon	Var, 1500 V _{DC} (EN 50155 ve EN 62368-1'e göre)
Elektrik kesintisi	Sınıf S2: 10 ms'ye kadar elektrik kesintilerine dayanır, pil dahil değildir
Tedarik değişimi	Sınıf C1: 100 ms boyunca 0,6 U _n (kesintisiz)
Konektör tipi	M12, 4 kutuplu, A kodlu erkek

Tablo 4.15.: Güç Giriři Özellikleri Varyant Pa

Standart varyant “Pb” (72 V_{DC} – 110 V_{DC})

Özellik	Spesifikasyon
Güç kaynağı nominal voltajları	72 V _{DC} , 96 V _{DC} ve 110 V _{DC} (EN 50155’e göre)
Voltaj aralığı	72 V _{DC} ve 110 V _{DC} ($\pm 30\%$)
Azami güç tüketimi	25 W
Tipik Ani Akım İntegrali	0.13 A ² s @ 72 V _{in} , 0.27 A ² s @ 96 V _{in} , 0.35 A ² s @ 110 V _{in}
Azami kablo uzunluğu	30 m
Kablo blendajı	Zorunlu değil
Galvonik izolasyon	Var, 1500 V _{DC} (EN 50155 ve EN 62368-1'e göre)
Elektrik kesintisi	Sınıf S2: 10 ms'ye kadar elektrik kesintilerine dayanır, pil dahil değildir
Tedarik değişimi	Sınıf C1: 100 ms boyunca 0,6 U _n (kesintisiz)
Konektör tipi	M12, 4 kutuplu, A kodlu erkek

Tablo 4.16.: Güç Girişi Özellikleri Varyant Pb

Kablo uçları (M12, 4 kutuplu, A kodlu erkek konektör)

Uç	Sinyal	Konektör
1	V ₊ (24–48 V _{DC} veya 72–110 V _{DC})	
2	Bağlantı yok	
3	V ₋	
4	Bağlantı yok	

Tablo 4.17.: Güç Bağlantı Noktası Kablo Uçları

4.4.10. Genişletme Yuvaları

Mevcut Seçenekler

NB3800, 8 pinli M12 A kodlu dişi uzatma konnektörüne sahiptir. 8 pin iki mantıksal porta ayrılmıştır: 1 ila 4 pinler Uzatma Portu 1'i (EP1) ve 5 ila 8 pinler Uzatma Portu 2'yi (EP2) temsil eder. Hem EP1 hem de EP2'de aşağıdaki arayüzler mevcut olabilir:

- Ses (Seçenek "A")
- CAN (Seçenek "C")
- IBIS (Seçenek "I")
- Yalıtılmamış RS-232 (EP1'de varsayılan yapılandırma)
- Yalıtılmış RS-232 (Seçenek "Sb")
- Yalıtılmış RS-485 (Seçenek "Sa")



Dikkat:

- EP1 ve EP2 için iki farklı arayüz kullanılıyorsa, ikisinin daha küçük izolasyonu zorunludur. Konnektörün kendisi 800VDC'nin pinleri arasında bir izolasyona sahiptir.

Uç	Sinyal	Konnektör
1	EP1 - Pin 1	
2	EP1 - Pin 2	
3	EP1 - Pin 3	
4	EP1 - Pin 4	
5	EP2 - Pin 1	
6	EP2 - Pin 2	
7	EP2 - Pin 3	
8	EP2 - Pin 4	

Tablo 4.18.: Dijital Giriş ve Çıkışların Pin Atamaları

Ses Port Özellikleri (Opsiyon "A")

Ses bağlantı noktasının özellikleri şunlardır:

Özellik	Spesifikasyon
Protokol	Audio hattı giriş/çıkış
Giriş referans seviyesi @0dBFS	Sinyal seviyesi 1.9 V _{PP}
Giriş empedans	21kΩ
Giriş bant genişliği	100 Hz - 15 kHz
Giriş galvanik izolasyonu	İşlevsel (azami 100 V _{DC})
Çıkış voltajı @0dBFS	600 Ω, sinyal seviyesi 3.7 V _{PP}
Çıkış bant genişliği	300 Hz - 4 kHz
Çıkış galvanik izolasyonu	İşlevsel (azami 100 V _{DC})
Azami kablo uzunluğu (m)	30
Kablo koruma	Zorunlu

Tablo 4.19.: Audio Port Özellikleri

Uçlar	Sinyal
1 / 5	Giriş Kanal +
2 / 6	Giriş Kanal -
3 / 7	Çıkış Kanal -
4 / 8	Çıkış Kanal +

Tablo 4.20.: Ses Portu Sinyallerinin Pin Atamaları (EP1 / EP2)

Not: Stereo çalışma durumunda sol kanal EP1'dedir.

CAN Portu Spesifikasyonu (Opsiyon “C”)

CAN portunun aşağıdaki spesifikasyonu vardır:

Özellik	Spesifikasyon
Protokol	CAN V2.0B
Hız	Azami: 1 Mbit/s, Varsayılan: 125 kbit/s
Galvonik izolasyon	1500 V _{DC}
Dahili veriyolu sonlandırıcı	Yok
Harici veriyolu sonlandırıcı ²	120 Ω
Azami kablo uzunluğu (m)	100
Kablo koruma	Zorunlu
Kablo tipi	bükülü çift (twisted pair)
Azami düğüm sayısı	110
Tepki	Opsiyon “Cm”: CAN-Pasif (sadece izleme) Opsiyon “Cn”: CAN-Aktif (rx ve tx etkin)

Tablo 4.21.: CAN Port Özellikleri

Uçlar	Sinyal
1 / 5	CAN GND
2 / 6	L
3 / 7	H
4 / 8	-

Tablo 4.22.: CAN Port Sinyallerinin Pin Atamaları (EP1 / EP2)

² CAN veri yolunun her iki ucunda 120 Ω'luk bir sonlandırma zorunludur

**IBIS Port Spesifikasyonu (Opsiyon "I")**

IBIS portunun özellikleri şu şekildedir:

Özellik	Spesifikasyon
Protokol	VDV 300 ve VDV 301'e göre 'IBIS Wagenbus'
Cihaz tipi	VDV 300 ve VDV 301'e göre 'IBIS Peripheriegerät'
Hız	1200 Baud
Galvonik izolasyon	1500 V _{DC}
Kablo uzunluğu (m)	100
Kablo koruma	Zorunlu değil

Tablo 4.23.: IBIS Port Özellikleri

Uçlar	Sinyal
1 / 5	WBSD (Signal Call/Aufrufbus)
2 / 6	WBMS (GND Call/Aufrufbus)
3 / 7	WBED (Signal Reply/Antwortbus)
4 / 8	WBME (GND Reply/Antwortbus)

Tablo 4.24.: IBIS Port Sinyallerinin Pin Atamaları (EP1 / EP2)



Yalıtılmış 3-kablolu RS-232 Portu Spesifikasyonu (Opsiyon “S”)

İzole edilmiş 3 kablolu RS-232 portu aşağıdaki özelliklere sahiptir (kalın karakterler varsayılan yapılandırmayı gösterir):

Özellik	Spesifikasyon
Protokol	3-tel RS-232: GND, TXD, RXD
Veri transfer hızları	600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Veri bitleri	7 bit, 8 bit
Parite	Yok , tek, çift (none , odd, even)
Duruş bitleri	1, 2
Yazılım akış kontrolü	none , XON/XOFF
Donanım akış kontrolü	none
Galvonik izolasyon	yok
Azami kablo uzunluğu (m)	10
Kablo koruma	Zorunlu

Tablo 4.25.: Yalıtılmamış RS-232 Port Özellikleri

Uçlar	Sinyal
1 / 5	GND
2 / 6	TxD
3 / 7	RxD
4 / 8	-

Tablo 4.26.: RS-232 Port Sinyallerinin Pin Atamaları (EP1 / EP2)



Yalıtılmış 5-kablolu RS-232 Portu Spesifikasyonu (Opsiyon “Sb”)

İzole edilmiş 5 kablolu RS-232 portu aşağıdaki özelliklere sahiptir (kalın karakterler varsayılan yapılandırmayı gösterir):

Özellik	Spesifikasyon
Protokol	5-tel RS-232: GND, TXD, RXD
Veri transfer hızları	600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Veri bitleri	7 bit, 8 bit
Parite	Yok , tek, çift (none , odd, even)
Duruş bitleri	1, 2
Yazılım akış kontrolü	none , XON/XOFF
Donanım akış kontrolü	none
Galvonik izolasyon	1500 V _{DC}
Azami kablo uzunluğu (m)	10
Kablo koruma	Zorunlu

Tablo 4.27.: Yalıtılmış RS-232 Port Özellikleri

Uç	Sinyal
1	GND
2	TxD
3	RxD
4	-
5	CTS
6	RTS
7	-
8	-

Tablo 4.28.: RS-232 Port Sinyallerinin Pin Atamaları (EP1 ve EP2)



Yalıtılmış RS-485 Portu Spesifikasyonu (Opsiyon “Sa”)

RS-485 portu aşağıdaki spesifikasyona sahiptir (kalın karakterler varsayılan yapılandırmayı gösterir):

Özellik	Spesifikasyon
Protokol	3-tel RS-485: GND, A, B
Veri transfer hızları	600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Veri bitleri	7 bit, 8 bit
Parite	Yok , tek, çift (none , odd, even)
Duruş bitleri	1 , 2
Yazılım akış kontrolü	none , XON/XOFF
Donanım akış kontrolü	none
Galvonik izolasyon	1500 V _{DC}
Azami kablo uzunluğu (m)	10
Kablo koruma	Zorunlu
Kablo tipi	Twisted pair
Veriyolundaki alıcı/verici sayısı	256 (azami)
Azami düğüm sayısı	256

Tablo 4.29.: RS-485 Port Özellikleri

Uçlar	Sinyal
1 / 5	GND
2 / 6	TxD-/RxD- (A)
3 / 7	TxD+/RxD+ (B)
4 / 8	-

Tablo 4.30.: RS-485 Port Sinyallerinin Pin Atamaları (EP1 / EP2)

Dijital Girişler ve Çıkışlar (Opsiyon “2D”)

İzole giriş ve çıkış portları sinyali aşağıdaki özelliklere sahiptir:

Özellik	Spesifikasyon
Şaseye izole/GND	1500V _{DC}
Azami kablo uzunluğu (m)	30
Kablo blendajı	Zorunlu değil

Tablo 4.31.: Ortak Dijital G/Ç Spesifikasyonu

Dijital Giriş sinyali aşağıdaki özelliklere sahiptir:

Özellik	Spesifikasyon
Port sayısı	1x Sayısal Giriş
Giriş voltajı (azami)	60 V _{DC}
Giriş akımı (azami)	2 mA
Ters polarite koruması	Evet
Seviye 1 için min. voltaj (set)	7.2 V _{DC}
Seviye 0 için min. voltaj (not set)	5.0 V _{DC}

Tablo 4.32.: Yalıtılmış Sayısal Giriş Özellikleri

Not: Negatif giriş voltajı tanınmaz.

Dijital Çıkış sinyali aşağıdaki özelliklere sahiptir:

Özellik	Spesifikasyon
Port sayısı	1x NO / 1x NC
Azami sürekli çıkış akımı	1 A
Azami anahtarlama çıkış voltajı	60 V _{DC} , 42 V _{AC} (V _{RMS})
Azami anahtarlama kapasitesi	60 W

Tablo 4.33.: İzole Sayısal Çıkış Özellikleri

Uç	Sinyal
1	DI1+
2	DI1-
3	DI2+
4	DI2-
5	DO1: Normally open (NO)
6	DO1: Normally open (NO)
7	DO2: Normally closed (NC)
8	DO2: Normally closed (NC)

Tablo 4.34.: İki DIO Portlu Varyantın Pin Atamaları

Not: İstek üzerine: 1xDin, 1xDOut

4.5. Veri Depolama (Seçenek “Dx”)

Entegre toplu depolama, herhangi bir yönlendirici işlevinden bağımsız olarak çalışır ve veri toplama veya yolcu eğlencesi gibi müşteri uygulamalarına ayrılmıştır. Depolamaya SDK üzerinden erişilebilir. Daha fazla ayrıntı için lütfen SDK API Kılavuzu'na, 2.2 Medya Montajı bölümüne bakın. Aşağıdaki seçenekler mevcuttur:



Opsiyon	Kapasite
Da	32 GB
Db	64 GB
Dc	128 GB
Dd	256 GB
De	512 GB
Df	1 TB

Tablo 4.35.: Depolama Özellikleri

5. Kurulum

NB3800, bir tezgah veya duvara monte edilmek üzere tasarlanmıştır (Yalnızca 2 m'den daha küçük yüksekliklere monte edilmeye uygundur), <https://www.netmodule.com/support/downloads/drawings>

Lütfen 2. bölümdeki güvenlik talimatlarını ve 4.3. bölümdeki çevre koşullarını dikkate alın. Bir NB3800 yönlendiricisi kurmadan önce aşağıdaki önlemler alınmalıdır:

- Doğrudan güneş radyasyonundan kaçının
- Cihazı nemden, buhardan ve agresif sıvılardan koruyun
- Cihazın etrafında yeterli hava sirkülasyonu sağlayın
- Cihaz yalnızca iç mekanda kullanıma yöneliktir



Dikkat:

- NetModule cihazları son tüketici pazarı için tasarlanmamıştır. Cihaz sertifikalı bir uzman tarafından kurulmalı ve devreye alınmalıdır.

5.1. Micro-SIM (3FF) Kart Kurulumu

Bir NB3800 yönlendiriciye en fazla dört Mini-SIM kart (2FF) takılabilir. 2FF, 3FF ve 4FF formatlı, çok formatlı bir kart olan, 3'ü 1 arada kart (All-in-One SIM veya Triple-SIM) olarak adlandırılan bir SIM kart desteklenmez.

SIM kartlar, ön paneldeki belirlenmiş yuvalardan birine kaydırılarak takılabilir. SIM kartını yerine oturana kadar küçük bir ataç (veya benzeri) kullanarak itmeniz gerekir. SIM kartı çıkarmak için, aynı şekilde tekrar itmeniz gerekecektir. SIM kart daha sonra geri sıçrayacak ve çekilebilir hale gelecektir.

SIM'ler sistemdeki herhangi bir modeme esnek bir şekilde atanabilir. Ayrıca, örneğin belirli bir koşulda başka bir sağlayıcı kullanmak istiyorsanız, çalışma sırasında bir SIM'i farklı bir modeme geçirmek de mümkündür. Ancak, SIM geçişi genellikle yaklaşık 10-20 saniye sürer ve SIM'ler makul bir şekilde takılırsa (örneğin önyükleme sırasında) atlanabilir. Tek bir modemle yalnızca tek bir SIM kullanıldığında, tercihen SIM 1 tutucusuna yerleştirilmelidir. İki SIM ile paralel olarak iki modemi çalıştırması gereken sistemler için, **MOB1**'i SIM 1'e, **MOB2**'yi SIM 2'ye vb. atamanızı öneririz. SIM yapılandırması hakkında daha fazla bilgi 6.3.3 bölümünde bulunabilir.



Dikkat:

- SIM değişiminden sonra NB3800 router'ın SIM Kapağı tekrar monte edilmeli ve vidalanarak IP40 koruma sınıfına kavuşturulmalıdır.

5.2. WWAN Antenlerinin Kurulumu

NetModule yönlendiricisinin mobil ağ üzerinden güvenilir bir şekilde çalışması için, NetModule yönlendiricilerinin etkili bir sinyale ihtiyacı vardır. Yeterli sinyale sahip optimum bir konum elde etmek ve diğer antenlere olan mesafeleri (birbirlerine en az 20 cm) korumak için uzatılmış kablolarla sahip uygun uzak antenler kullanın.

Anten üreticisinin talimatlarına uyun." Faraday kafeslerinin neden olduğu büyük metal yüzeyler (asansörler, makine muhafazaları, vb.), sıkı örgülü demir yapılar ve diğerleri gibi etkilerin sinyal alımını önemli ölçüde azaltabileceğini unutmayın.

Monte edilmiş antenler veya anten kabloları bir anahtarla sabitlenmelidir.



Aşağıdaki tablo hücrel antenlerin nasıl bağlanacağını göstermektedir. Genellikle LTE antenleri hem ana hem de yardımcı portları kullanır, ancak UMTS yalnızca ana portları gerektirir. 5G modül başına 4 Anten gerektirir.

Anten Portu	Tip
MOB 1 A2	Ana (Main)
MOB 1 A3	Ek (Auxiliary)
MOB 2 A4	Ana (Main)
MOB 2 A5	Ek (Auxiliary)
MOB 3 A6	Ana (Main)
MOB 3 A7	Ek (Auxiliary)
MOB 4 A8	Ana (Main)
MOB 4 A9	Ek (Auxiliary)
MOB 5 A10	Ana (Main)
MOB 5 A11	Ek (Auxiliary)

Tablo 5.1.: WWAN Anten Port Tipleri

	MOB 1		MOB 2		MOB3		MOB4		MOB5	
Anten Portu	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11
NB3800-2L2Wac-G	LTE Mobil 1		LTE Mobil 2		n/a		WLAN 2		WLAN 1	
NB3800-3L2Wac-G	LTE Mobil 1		LTE Mobil 2		LTE Mobil 3		WLAN 2		WLAN 1	
NB3800-4LWac-G	LTE Mobil 1		LTE Mobil 2		LTE Mobil 3		LTE Mobil 4		WLAN 1	
NB3800-2Lp2Wac-G	LTE Mobil 1		LTE Mobil 2		n/a		WLAN 2		WLAN 1	
NB3800-3LpWac-G	LTE Mobil 1		LTE Mobil 2		LTE Mobil 3		n/a		WLAN 1	

Tablo 5.2.: LTE modüllü varyant, anten ataması

	MOB 1		MOB 2		MOB3		MOB4		MOB5	
Anten Portu	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11
NB3800-2NWac-G	5G Mobil 1		5G Mobil 2		5G Mobil 1		5G Mobil 2		WLAN 1	
NB3800-NWac-G	5G Mobil 1		5G Mobil 1		n/a		n/a		WLAN 1	
NB3800-N2Wac-G	5G Mobil 1		5G Mobil 1		n/a		WLAN 2		WLAN 1	
NB3800-NLWac-G	5G Mobil 1		LTE Mobil 2		5G Mobil 1		n/a		WLAN 1	
NB3800-N2L-G	5G Mobil 1		LTE Mobil 2		LTE Mobil 3		5G Mobil 1		n/a	

Tablo 5.3.: 5G modüllü varyant, anten ataması

5G modülleri hücrel için dört anten yoluna sahiptir (GNSS dikkate alınmaz), 3x RX/TX ve 1x RX-only (TX=Transmit, RX=Receive). İlk üç düşük anten portu numarası RX/TX ve en yüksek RX'tir, örneğin NB3800-NWac-G için: Anten portu A2 / A3 / A4 RX/TX ve A5 RX-only veya NB3800-NLWac-G için: Anten portu A2 / A3 / A6 RX/TX ve A7 RX-only.



Dikkat: Antenlerin montajı sırasında aşağıdaki noktalara dikkat edilmelidir:

- İnsanlar ve antenler arasında her zaman en az 40 cm'lik bir minimum boşluk sağlanmalıdır.
- Bir mobil arayüz diğer aynı yerde bulunan radyo vericileriyle aynı anda iletim yapıyorsa, antenler arasında her zaman 20 cm'lik bir ayırma mesafesi korunmalıdır. Sonuç olarak, farklı modemlerin anten portları asla tek bir birleşik antenin portlarına bağlanmamalıdır.
- Bir binanın veya araç gövdesinin dışına kurulan antenler, geçici aşırı gerilimleri (IEC 62368-1'e göre) harici koruma devreleri aracılığıyla 1500 V'luk bir tepe noktasının altında sınırlanmalıdır.
- Bir antenin maksimum kazancı (bağlantı kablolarının zayıflaması dahil) ilgili frekans aralığında aşağıdaki değerleri aşmamalıdır:
 - Mobil radyo (600MHz .. 1GHz) < 3,2dBi
 - Mobil radyo (1,7GHz .. 2GHz) < 6,0dBi
 - Mobil radyo (2,5GHz .. 4,2GHz) < 6,0dBi

5.3. WLAN Antenlerinin Kurulumu

Aşağıdaki tablo WLAN antenlerinin nasıl bağlanacağını göstermektedir. Takılan anten sayısı yazılımda yapılandırılabilir. Yalnızca bir anten kullanılıyorsa, ana porta takılmalıdır. Ancak, daha iyi çeşitlilik ve dolayısıyla daha iyi verim ve kapsama için iki anten kullanmanızı şiddetle öneririz. Not: 5G modülü ve WLAN modülüne sahip NB3800 varyantı için anten atamasını "4.2. WWAN Antenlerinin Kurulumu" bölümünde bulabilirsiniz.

Anten Portu	Tip
WLAN 1 A10	Ana (Main)
WLAN 1 A11	Ek (Auxiliary)
WLAN 2 A8	Ana (Main)
WLAN 2 A9	Ek (Auxiliary)

Tablo 5.4.: WLAN Anten Portu Tipleri



Dikkat: Antenlerin montajı sırasında aşağıdaki noktalara dikkat edilmelidir.

- İnsanlar ile antenler arasında her zaman en az 40 cm'lik bir minimum boşluk sağlanmalıdır.
- Bir WLAN arayüzü diğer aynı yerde bulunan radyo vericileriyle aynı anda iletim yapıyorsa, antenler arasında her zaman 20 cm'lik bir ayırma mesafesi korunmalıdır.
- WLAN antenleri yalnızca binalara veya araç gövdelerine monte edilmelidir.
- WLAN antenleri sırasıyla 4,5 dBi (5GHz) veya maksimum 3,2 dBi (2,4GHZ) amplifikasyona sahip olabilir. Daha yüksek amplifikasyona sahip WLAN antenleri, sertifikalı uzman personel tarafından doğru şekilde yapılandırılmış NetModule yönlendirici "Enhanced-RF-Configuration" yazılım lisansı ve anten kazancı ve kablo zayıflaması ile kullanılabilir.

5.5. GNSS Anteni Kurulumu

GNSS anteni **GNSS** konnektörüne monte edilmelidir. Antenin aktif veya pasif GNSS anteni olup olmadığı yazılımda yapılandırılmalıdır. Yüksek doğruluklu GNSS takibi için aktif GNSS antenlerini öneriyoruz.



Dikkat: Anten kurulumu sırasında aşağıdaki noktalara dikkat edilmelidir.

- İnsanlar ile anten arasında her zaman en az 40 cm'lik bir minimum mesafe sağlanmalıdır.
- Bir binanın veya araç gövdesinin dışına kurulan antenler, geçici aşırı gerilimleri (IEC 62368-1'e göre) harici koruma devreleri aracılığıyla 1500 V'luk bir tepe noktasının altında sınırlanmalıdır.

5.6. Yerel Alan Ağı (LAN) Kurulumu

Yönlendiriciye doğrudan üç adet 10/100 Mbps ve iki adet 10/100/1000 Mbps Ethernet cihazı bağlanabilir, ek bir Ethernet anahtarıyla diğer cihazlar da bağlanabilir. Lütfen konektörün **ETH1** portuna düzgün bir şekilde takıldığından ve sabit bir durumda kaldığından emin olun, aksi takdirde çalışma sırasında ara sıra bağlantı kaybı yaşayabilirsiniz. L/A (Link/Activity) LED'i cihaz senkronize olur olmaz yanacaktır. Aksi takdirde, 6.3.2 bölümünde açıklandığı gibi farklı bir bağlantı ayarı yapılandırmak gerekebilir. Varsayılan olarak, yönlendirici bir DHCP sunucusu olarak yapılandırılmıştır ve IP adresi 192.168.1.1'dir.



Dikkat:

- Sadece blendajlı Ethernet kablosu kullanılmalıdır.

5.6. Güç Kaynağının Kurulumu

Yönlendirici, sırasıyla 24 VDC ve 48 VDC veya 72 VDC ve 110 VDC arasında bir harici kaynakla çalıştırılabilir. Sınırlı ve SELV devre çıkışına sahip olması gereken sertifikalı (CE veya eşdeğeri) bir güç kaynağıyla kullanılmalıdır. Yönlendirici artık devreye girmeye hazırdır. "Gecikmeli güç kapatma" gerekmediğinde, besleme voltajını hem IGN hem de V+ pinine bağlayın. "Gecikmeli güç kapatma" işlevi kullanıldığında, V+ doğrudan akü devresine bağlanır ve IGN aracın ateşleme devresine bağlanır. Bu özelliği kullanarak, yönlendirici araç kapatıldıktan sonra anında kapanma yerine belirli bir süre (SW yapılandırılabilir) sonra kapanır.



Dikkat: Aşağıdaki hususlara dikkat edilmelidir.

- NetModule yönlendiricilerle birlikte yalnızca akım sınırlı SELV çıkış voltaj aralığına sahip CE uyumlu güç kaynakları kullanılabilir ("Pb" seçeneğine sahip NetModule yönlendiriciler için buna uygun olarak daha yüksek çıkış voltaj aralığı ve uygun karşılaştırılabilir güvenlik önlemlerine uygun olarak)
- Güç Kaynağı Sınıfı 3 (PS3) güç kaynağı (100 W veya daha fazla) yalnızca yönlendiriciye giden güç kablosunda bir kablo gerginlik gidericisinin uygulanması koşuluyla kullanılabilir. Bu tür bir kablo gerginlik gidericisi, yönlendirici vida terminali konektöründeki tellerin bağlantısının kesilmemesini sağlar (örneğin, bir hata koşulu altında yönlendirici kabloya dolanacaktır). Kablo gerginlik gidericisi, yönlendiricinin kablosuna uygulanan 60 N'luk (4 kg'a kadar yönlendirici ağırlığı için) bir çekme kuvvetine dayanmalıdır.

5.7. Ses Arayüzünün Kurulumu

Ses arayüzü (hat çıkışı) PTT (Opsiyon "Ap") ve Ses (Opsiyon "A") uzantısında mevcuttur.



Dikkat:

- İşitme hasarı riski: Kulaklık veya mikrofonlu kulaklığı yüksek sesle veya uzun süre kullanmaktan kaçının.

6. Yapılandırma

Aşağıdaki bölümlerde, sistem yazılımı 4.8.0.104 sürümü ile sağlanan yönlendiricinin kurulumu ve işlevlerinin yapılandırılması hakkında bilgi verilmektedir.



NetModule, yeni işlevler, hata düzeltmeleri ve kapatılmış güvenlik açıkları ile düzenli olarak güncellenen yönlendirici yazılımı sağlar. Lütfen yönlendirici yazılımınızı güncel tutun.
<ftp://share.netmodule.com/router/public/system-software/>

6.1. İlk Adımlar

NetModule AG yönlendiricileri, Web Yöneticisi adı verilen HTTP tabanlı yapılandırma arayüzü kullanılarak kolayca kurulabilir. En son web tarayıcıları tarafından desteklenir. Lütfen JavaScript'in açık olduğundan emin olun.

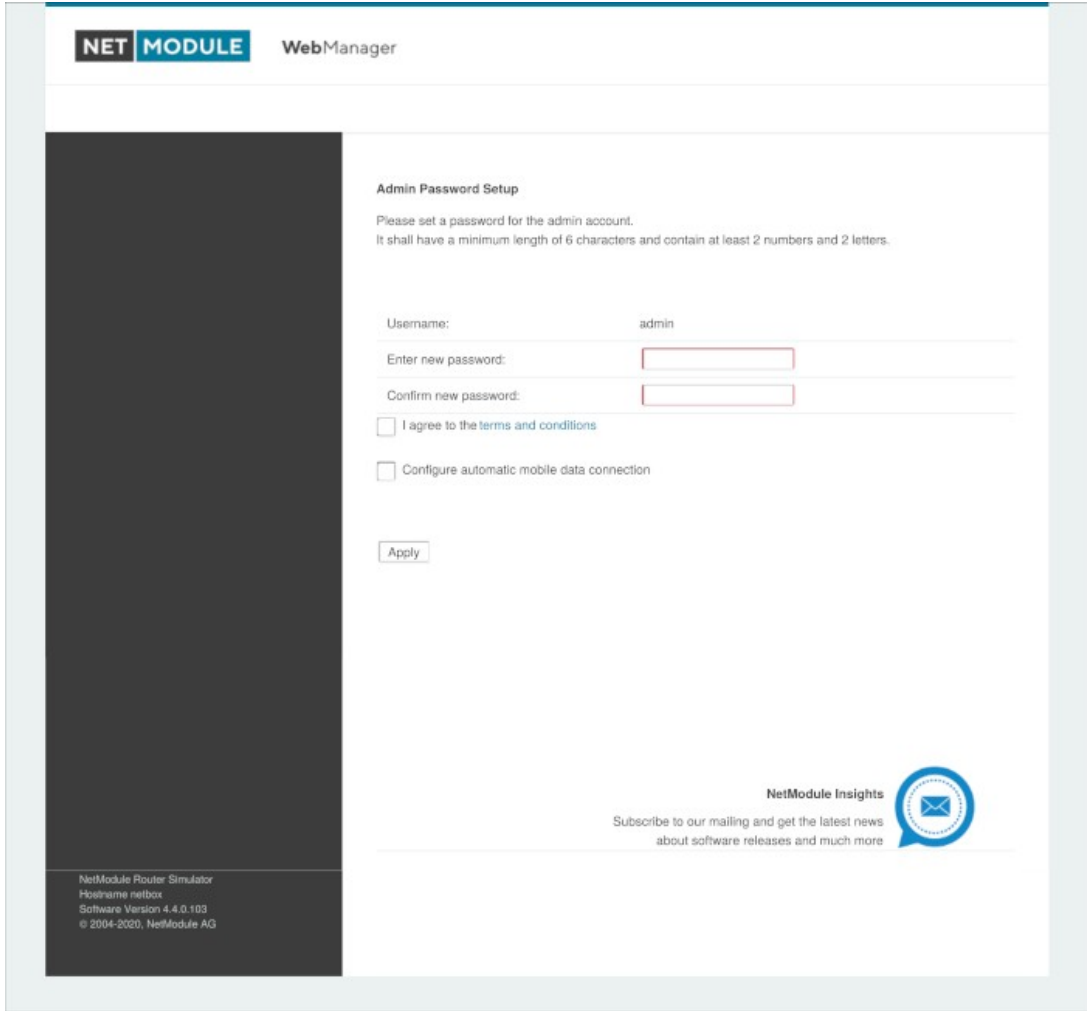
Web Yöneticisi aracılığıyla gönderilen herhangi bir yapılandırma, Uygula düğmesine basıldığında sisteme hemen uygulanacaktır. Birden fazla adım gerektiren alt sistemleri (örneğin WLAN) yapılandırırken, herhangi bir ayarı geçici olarak depolamak ve daha sonra uygulamak için Devam düğmesini kullanabilirsiniz. Lütfen bu ayarların uygulanmadığı takdirde oturum kapatma sırasında göz ardı edileceğini unutmayın. Daha fazla sayıda yönlendirici dağıtmayı planlıyorsanız, yapılandırma dosyalarını SNMP, SSH, HTTP veya USB aracılığıyla da yükleyebilirsiniz. Gelişmiş kullanıcılar ayrıca Komut Satırı Arayüzünü (CLI) kullanabilir ve yapılandırma parametrelerini doğrudan ayarlayabilir.

Ethernet 1'in IP adresi 192.168.1.1'dir ve DHCP varsayılan olarak arayüzde etkinleştirilir. İlk Web Yöneticisi oturumunuzu oluşturmak için aşağıdaki adımların atılması gerekir:

1. Bilgisayarınızın Ethernet portunu, RJ45 (veya M12) konnektörlü korumalı bir CAT5 kablosu kullanarak yönlendiricinin ETH1 (FastEthernet) portuna bağlayın.
2. Henüz etkinleştirilmediyse, yönlendiriciden otomatik olarak bir IP adresi alınabilmesi için bilgisayarınızın Ethernet arayüzünde DHCP'yi etkinleştirin. Bu, genellikle PC'nizin ilgili parametreleri (IP adresi, alt ağ maskesi, varsayılan ağ geçidi, ad sunucusu) almasına kadar kısa bir süre alır. Ağ kontrol panelinize bakarak ve PC'nizin 192.168.1.100 ila 192.168.1.199 aralığında bir IP adresini doğru şekilde alıp almadığını kontrol ederek ilerlemeyi takip edebilirsiniz.
3. Favori web tarayıcınızı başlatın ve yönlendiricinin IP adresine yönlendirin (URL <http://192.168.1.1>'dir).
4. Lütfen yönlendiriciyi yapılandırmak için Web Yöneticisi'nin talimatlarını izleyin. Menülerin çoğu kendiliğinden açıklayıcıdır, daha detaylı bilgi sonraki bölümlerde verilmektedir.

6.1.1. İlk Erişim

Fabrika durumunda sizden yeni bir yönetici parolası istenecektir. Lütfen hem hatırlaması kolay hem de sözlük saldırılarına (örneğin sayılar, harfler ve noktalama işaretleri içeren) karşı dayanıklı bir parola seçin. Parolanın uzunluğu en az 6 karakter olmalıdır. En az 2 sayı ve 2 harf içermelidir.



Ekran 6.1.: İlk Giriş

Lütfen yönetici parolasının, seri konsol, Telnet, SSH üzerinden cihaza erişmek veya önyükleyiciye girmek için kullanılabilen kök kullanıcı için de uygulanacağını unutmayın. Ayrıca, yalnızca özet sayfasına erişme veya durum bilgilerini alma izni verilecek ancak herhangi bir yapılandırma parametresi ayarlama izni verilmeyecek ek kullanıcılar da yapılandırabilirsiniz. Bir dizi hizmet (USB Otomatik Çalıştırma, CLI-PHP) varsayılan olarak fabrika durumunda etkinleştirilir ve yönetici parolası ayarlandıktan hemen sonra devre dışı bırakılır. Daha sonra ilgili bölümlerde tekrar etkinleştirilebilirler. Diğer hizmetlere (SSH, Telnet, Konsol) boş veya parola sağlanmadan fabrika durumunda erişilebilir.

Oluşturulan ve yüklenen özel anahtarları depolamak ve bunlara erişmek için kullanılan parola ifadesi rastgele bir değere başlatılır. Bölüm 6.8.8'de açıklandığı gibi değiştirilebilir.

6.1.2. Otomatik Mobil Veri Bağlantısı

İlk SIM yuvasına PIN'i devre dışı bırakılmış bir SIM takarsanız ve 'Otomatik mobil veri bağlantısını yapılandır'ı seçerseniz, yönlendirici bilinen sağlayıcıların veritabanından eşleşen kimlik bilgilerini seçmeye ve otomatik olarak bir mobil veri bağlantısı kurmaya çalışır. Bu özellik büyük ölçüde SIM kart özelliklerine ve mevcut ağlara bağlıdır. Bu Seçenek yalnızca yönlendirici bir hücrel modülle donatılmışsa kullanılabilir.

6.1.3. Kurtarma (Recovery)

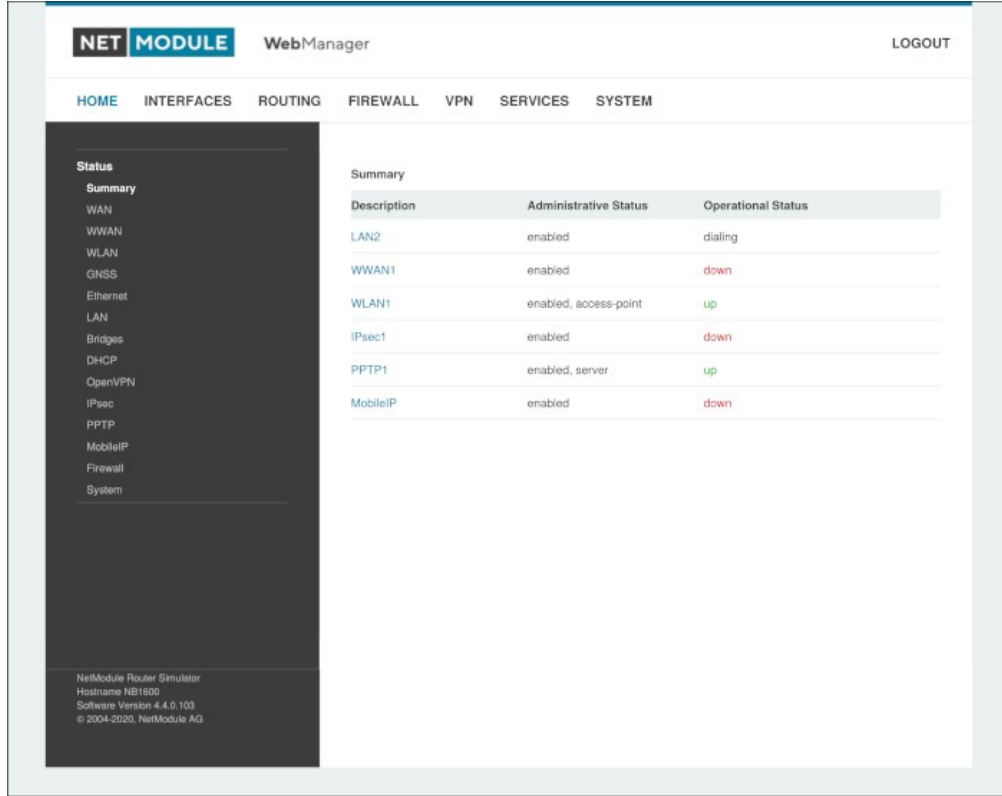
Yönlendirici yanlış yapılandırılmışsa ve artık erişilemiyorsa, aşağıdaki adımlar uygulanabilir:



1. Fabrika Ayarlarına Sıfırlama (Factory Reset):
Web Yöneticisi aracılığıyla `factory-reset` komutunu çalıştırarak fabrika ayarlarına sıfırlama işlemini başlatabilirsiniz.
2. Seri Konsol Girişi (Serial Console Login):
Sisteme seri port üzerinden de giriş yapılabilir. Bu, bir terminal emülatörü (örneğin PuTTY veya HyperTerminal) ve bilgisayarınızın seri portuna bağlı bir RS232 bağlantısı (115200 8N1) gerektirir. Açılış sırasında çekirdek (kernel) mesajlarını da bu bağlantı üzerinden görebilirsiniz.
3. Kurtarma İmajı (Recovery Image):
Ciddi durumlarda, RAM'e TFTP üzerinden yüklenip çalıştırılabilecek bir kurtarma imajı talep üzerine sağlanabilir. Bu, yazılım güncellemesi yapmak veya sistem üzerinde değişiklikler yapmak için minimal bir sistem imajı sunar. Size iki dosya verilecektir: `recovery-image` ve `recovery-dtb`. Bu dosyalar bir TFTP sunucusunun kök dizinine (LAN1 üzerinden bağlı ve IP adresi 192.168.1.254 olan) yerleştirilmelidir. Kurtarma imajı, önyükleyici (bootloader) üzerinden seri bağlantı aracılığıyla başlatılabilir. Önyükleme sürecinde s tuşuna basarak süreci durdurmanız ve bootloader'a girmeniz gerekir. Ardından `run recovery` komutunu vererek imajı yükleyip sistemi başlatabilirsiniz. Sistem daha sonra IP adresi 192.168.1.1 üzerinden HTTP/SSH/Telnet ile erişilebilir hale gelecektir. Bu işlem, fabrika ayarlarına sıfırlama düğmesine 15 saniyeden uzun süre basılı tutularak da başlatılabilir.

6.2. ANASAYFA (Home)

Bu sayfa etkinleştirilmiş özelliklerin ve bağlantıların durum özetini sağlar.



Ekran 6.2.: AnaSayfa

Özet

Bu sayfa, yönlendiricinin arayüzlerinin yönetimsel ve operasyonel durumu hakkında kısa bir özet sunar.

WAN

Bu sayfa, etkinleştirilmiş herhangi bir Geniş Alan Ağı (WAN) bağlantısı (IP adresleri, ağ bilgileri, sinyal gücü vb. gibi) hakkında ayrıntılar sunar. İndirilen/yüklenen veri miktarı hakkındaki bilgiler, kalıcı olmayan bellekte saklanır, böylece sistemin yeniden başlatılmasından sonra bile geçerliliğini korur. Sayaçlar, “Reset” düğmesine basılarak sıfırlanabilir.

WWAN

Bu sayfa, modemler ve ağ durumları hakkında bilgi gösterir.

AC

Bu sayfa, Erişim Denetleyicisi (AC) WLAN-AP hakkında bilgi gösterir. Buna, keşfedilen ve yönetilen AP3400 cihazlarının geçerli durumları ve durum bilgileri dahildir.

WLAN

WLAN sayfası, erişim noktası modunda çalışırken etkinleştirilen WLAN arayüzleri hakkında ayrıntılar sunar. Buna, SSID, IP ve MAC adresi ve arayüzün şu anda kullanılan frekansı ve iletim gücü ile ilişkili istasyonların listesi dahildir.

GNSS

Bu sayfa enlem/boylam gibi konum durumu değerlerini, görüntülenen uyduları ve kullanılan uydular hakkında daha fazla ayrıntıyı görüntüler.

Ethernet

Bu sayfa Ethernet arayüzleri ve paket istatistikleri bilgileri hakkında bilgi gösterir.

LAN

Bu sayfa LAN arayüzleri ve ağ komşuluğu bilgileri hakkında bilgi gösterir.



Köprüler

Bu sayfa yapılandırılmış sanal köprü cihazları hakkında bilgi gösterir.

Bluetooth

Bu sayfa Bluetooth arayüzleri hakkında bilgi gösterir.

DHCP

Bu sayfa, verilen DHCP kiralamalarının bir listesi de dahil olmak üzere etkinleştirilmiş herhangi bir DHCP hizmeti hakkında ayrıntılar sunar.

OpenVPN

Bu sayfa OpenVPN tünel durumu hakkında bilgi sağlar.

IPSec

Bu sayfa IPsec tünel durumu hakkında bilgi sağlar.

PPTP

Bu sayfa PPTP tünel durumu hakkında bilgi sağlar.

GRE

Bu sayfa GRE tünel durumu hakkında bilgi sağlar.

L2TP

Bu sayfa L2TP tünel durumu hakkında bilgi sağlar.

MobileIP

Bu sayfa Mobil IP bağlantıları hakkında bilgi sağlar.

Güvenlik Duvarı

Bu sayfa, güvenlik duvarı kuralları ve bunların eşleşen istatistikleri hakkında bilgi sunar. Güvenlik duvarını hata ayıklamak için kullanılabilir.

QoS

Bu sayfa, kullanılan QoS kuyrukları hakkında bilgi sağlar.

BGP

Bu sayfa, Sınır Geçidi Protokolü (Border Gateway Protocol) hakkında bilgi sağlar.

OSPF

Bu sayfa, Açık En Kısa Yol Önce yönlendirme protokolü (Open Shortest Path First) hakkında bilgi sağlar.

DynDNS

Bu sayfa, Dinamik DNS hakkında bilgi sağlar.

Sistem Durumu

Sistem durumu sayfası, sistem ayrıntıları, takılı modüller hakkında bilgi ve yazılım sürümü bilgileri dahil olmak üzere NB180 yönlendiricinizin çeşitli ayrıntılarını görüntüler.

SDK

Bu bölüm, SDK (Software Development Kit) betikleri (script) tarafından oluşturulan tüm web sayfalarını listeleyecektir.

6.3. ARAYÜZLER

6.3.1. WAN

Bağlantı Yönetimi (Link Management)

Donanım modelinize bağlı olarak, WAN (Geniş Alan Ağı) bağlantıları Kablosuz Geniş Alan Ağı (WWAN), Kablosuz Yerel Alan Ağ (WLAN), Ethernet veya Ethernet üzerinden PPP (PPPoE) bağlantılarından oluşabilir. Lütfen her WAN bağlantısının bu sayfada görünmesi için yapılandırılması ve etkinleştirilmesi gerektiğini unutmayın.

The screenshot displays the NET MODULE WebManager interface. The top navigation bar includes 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. The left sidebar lists various configuration categories: WAN (Link Management, Supervision, Settings), Ethernet (Port Setup, VLAN Management, IP Settings), Mobile (Modems, SIMs, Interfaces), WLAN (Administration, Configuration, IP Settings), Bridges, USB, Serial, Digital I/O, and GNSS. The main content area is titled 'WAN Link Management' and contains the following text: 'In case a WAN link goes down, the system will automatically switch over to the next link in order of priority. A link can be either established when the switch occurs or permanently to minimize link downtime. Outgoing traffic can also be distributed over multiple links on a per IP session basis.' Below this text is a table with two columns: 'Priority Interface' and 'Operation Mode'. The table lists two interfaces: '1st LAN2' with 'permanent' operation mode, and '2nd WWAN1' with 'permanent' operation mode. Each row has up and down arrow icons for reordering and an edit icon. An 'Apply' button is located below the table. The bottom of the interface shows 'NetModule Router Simulator', 'Hostname: NB1600', 'Software Version: 4.4.0.103', and '© 2004-2020, NetModule AG'.

Ekran 6.3.: WAN Bağlantıları



Genel olarak, bir bağlantı yalnızca aşağıdaki ön koşullar karşılandığında çevrilecek veya kuruldu olarak bildirilecektir:

Koşul	WWAN	WLAN	ETH.	PPPoE
Modem kayıt oldu	X			
Geçerli bir servis tipi ile kayıt oldu	X			
Geçerli SIM adımı	X			
Yeterli sinyal gücü	X	X		
İstemci ilişkilendirildi		X		
İstemci yetkilendirildi		X		
Geçerli DHCP adresi alındı	X	X	X	X
Bağlantı çalışıyor ve adresi tutuyor	X	X	X	X
Ping kontrolü başarılı oldu	X	X	X	X

Menü, WAN bağlantılarınızı önceliklendirmek için daha fazla kullanılabilir. Başarıyla kurulan en yüksek öncelikli bağlantı, giden paketler için varsayılan rotayı tutan sözde sıcak bağlantı (**hot link**) haline gelir.

Bir bağlantı kesilirse, sistem otomatik olarak öncelik listesindeki bir sonraki bağlantıya geçer. Bağlantı kesintisini en aza indirmek için her bağlantıyı, geçiş gerçekleştiğinde veya kalıcı olarak kurulacak şekilde yapılandırabilirsiniz.

Öncelik	WAN Bağlantısı Önceliklendirmesi
1	Mümkün olduğunda kullanılacak birincil bağlantı.
2	İlk yedek bağlantı, kalıcı olarak etkinleştirilebilir veya Bağlantı 1 kesilir kesilmez çevrilebilir.
3	İkinci yedek bağlantı, kalıcı olarak etkinleştirilebilir veya Bağlantı 2 kesilince çevrilebilir.
4	Üçüncü yedek bağlantı, kalıcı olarak etkinleştirilebilir veya Bağlantı 3 kesilince çevrilebilir.

Bağlantılar periyodik olarak tetiklenir ve belirli bir süre içinde kurulmaları mümkün olmadığında uyku moduna alınır. Bu nedenle, kalıcı bağlantıların arka planda çevrilmesi ve kuruldukları anda daha düşük önceliğe sahip bağlantıların yerini tekrar alması söz konusu olabilir. Aynı kaynakları paylaşan karışık bağlantılar durumunda (örneğin çift SIM işleminde), daha yüksek öncelikli bağlantının tekrar çevrilmesine izin vermek için etkin bir sıcak bağlantının kapanmaya zorlandığı bir geri geçiş aralığı tanımlayabilirsiniz.

Genel olarak WAN bağlantıları için kalıcı (“permanent”) çalışma modunu kullanmanızı öneririz. Ancak, örneğin zaman sınırlı mobil tarifeler durumunda, geçiş (“switchover”) modu uygulanabilir. Dağıtılmış modu kullanarak, giden trafiği ağırlık oranlarına göre birden fazla WAN bağlantısına dağıtmak mümkündür.

**Dikkat:**

- Farklı sağlayıcıların SIM kartlarını kullanarak bir WWAN modülü gibi ortak bir kaynağı paylaşan eş zamanlı WWAN bağlantılarınız olabilir. Bu durumda, düşük öncelikli bağlantıyı kapatmadan daha yüksek önceliğe sahip bağlantının kullanılabilir olup olmadığını bulmak mümkün olmazdı. Bu nedenle, böyle bir bağlantı kalıcı olarak yapılandırılmış olsa bile bir geçiş gibi davranacaktır.

Mobil bağlantılar için, WAN adresini yerel bir ana bilgisayara (ayrıca “Drop-In” veya “IP Pass-through” olarak da adlandırılır) geçirmek daha da mümkündür. Özellikle, ilk DHCP istemcisi genel IP adresini alacaktır. Sistem, güvenlik duvarı sorunları durumunda yardımcı olabilecek bir modem gibi davranır. Kurulduktan sonra, Web



Yöneticisine WAN adresini kullanarak 8080 portu üzerinden ancak yine de 80 portu kullanılarak LAN1 arayüzü üzerinden ulaşılabilir.

Parametre	WAN Bağlantısı Çalışma Modları
Kapalı (disabled)	Bağlantı kapalı
Kalıcı (permanent)	Bağlantı kalıcı olarak kuruldu
Geçiş (on switchover)	Geçiş bağlantısı kuruluyor, önceki bağlantılar başarısız olursa tekrar aranacak
Dağıtık (distributed)	Bağlantı bir yük dağıtım grubunun üyesidir

Parametre	WAN Bağlantısı Ayarları
Çalıştırma modu (Operation Mode)	Bağlantının işletme şekli
Ağırlık (Weight)	Dağıtılmış bir bağlantının ağırlıklı kullanılma oranı
Geri dönüş (Switch-back)	Geçiş bağlantısının durumu ve aktif bir bağlantının kesilmesinden ardından geçecek zaman
Köprü modu (Bridge Mode)	WLAN istemci için kullanılacak köprü modunu belirtir
Köprü arayüzü (Bridging interface)	WLAN istemci için WAN bağlantısının köprülenmesi gereken LAN arayüzü.

Bir WLAN istemcisi için aşağıdaki köprü modları yapılandırılabilir:

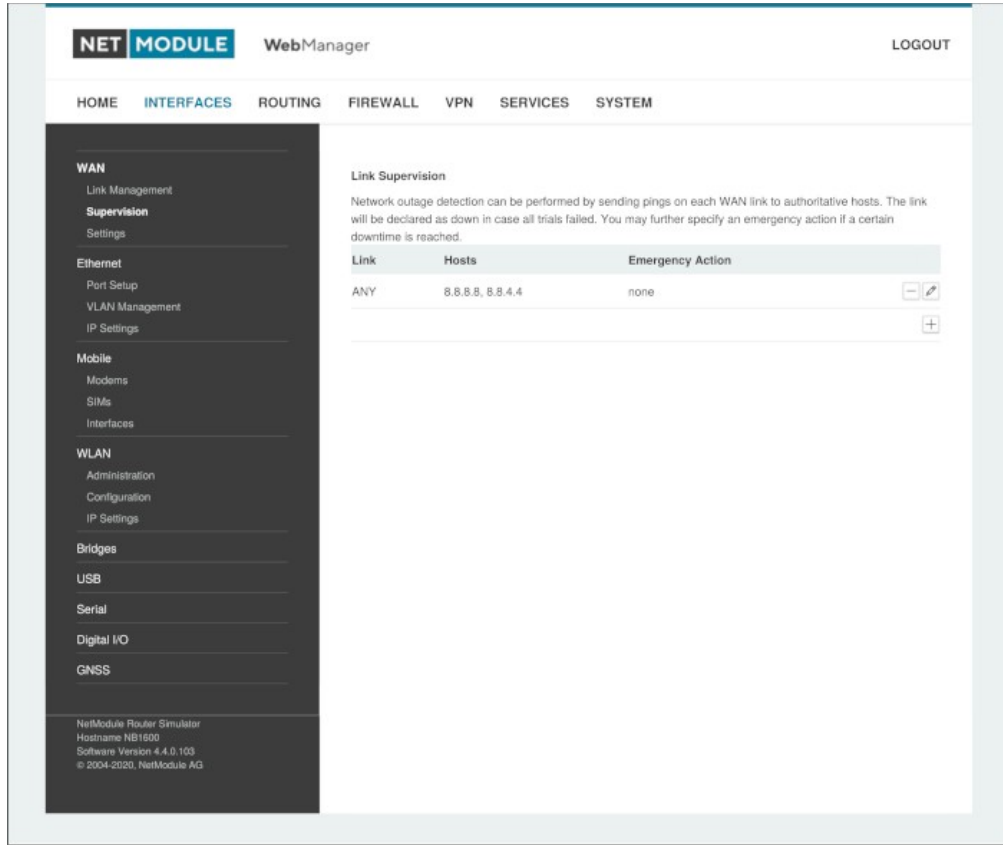
Parametre	WAN Bağlantısı Çalışma Modları
Kapalı (disabled)	Köprü modunu devre dışı bırakır
4addr frame*	4 adresli çerçeve biçimini etkinleştirir. (*: Erişim noktası gerektirir)
Sözde köprü (pseudo bridge)	DHCP ve yayın mesajlarını aktararak köprü gibi davranır

NetModule AG yönlendiricileri IP geçişi (diğer adıyla Drop-In modu) adı verilen bir özellik sunar. Etkinleştirilirse, WAN adresi belirtilen LAN arayüzünün ilk DHCP istemcisine geçirilecektir. Ethernet tabanlı iletişim ek adresler gerektirdiğinden, LAN ana bilgisayarını ile konuşmak için uygun bir alt ağ seçilir. WAN ağınızın diğer adresleriyle çakışmasını önlemek için isteğe bağlı olarak sağlayıcınız tarafından verilen ağ belirtebilirsiniz.

Parametre	IP Geçiş (Pass-Through) Ayarları
IP geçiş (Pass-through)	IP geçişini etkinleştirir veya devre dışı bırakır
Arayüz	Adresin geçirileceği arayüzü belirtir
WAN ağı (WAN network)	WAN ağını belirtir
WAN ağ maskesi (WAN netmask)	WAN ağ maskesini belirtir

Denetim

Bağlantı bazında ağ kesintisi tespiti, her bağlantıda yetkili bazı ana bilgisayarlara ping gönderilerek gerçekleştirilebilir. Tüm denemeler başarısız olursa bir bağlantı kapalı olarak ilan edilir ve yalnızca en az bir ana bilgisayara ulaşabiliyorsa açık olarak ilan edilir.

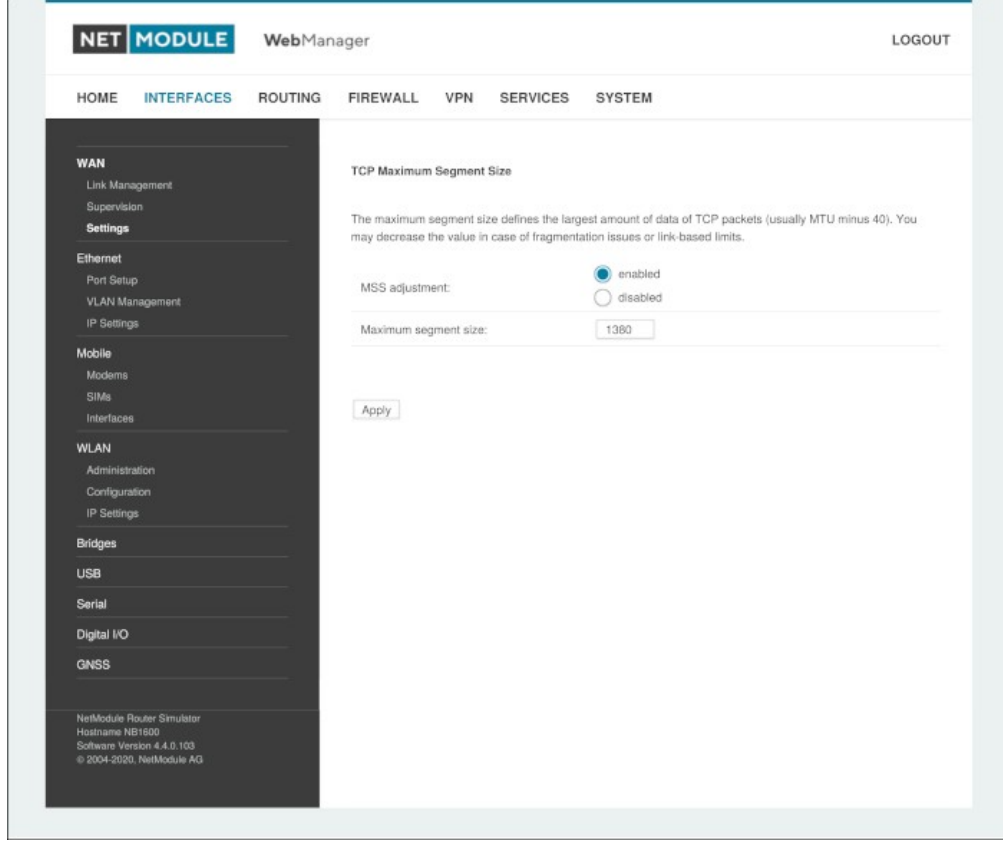


Ekran 6.4.: Bağlantı Denetimi (Link Supervision)

Parametre	Bağlantı Denetimi (Link Supervision) Ayarları
Bağlantı (Link)	İzlenecek WAN bağlantısı (HERHANGİ BİRİ olabilir)
Mode	Bağlantının yalnızca çalışır durumdayken mi (örneğin bir VPN tüneli kullanmak için) izleneceğini yoksa bağlantının kurulması sırasında bağlantının da doğrulanıp doğrulanmayacağını (varsayılan) belirtir
Birincil ana bilgisayar (Primary host)	İzlenecek birincil ana bilgisayar
İkincil ana bilgisayar (Secondary host)	İzlenecek ikincil ana bilgisayar (isteğe bağlı)
Ping zaman aşımı (Ping timeout)	Tek bir ping için bir yanıtın alabileceği milisaniye cinsinden süre, yavaş ve gecikmiş bağlantılar (örneğin 2G bağlantıları) durumunda bu değeri artırmayı düşünün
Ping aralığı (Ping interval)	Her arayüzde pinglerin iletildiği saniye cinsinden aralık
Yeniden deneme aralığı (Retry interval)	İlk ping başarısız olduğunda pinglerin yeniden iletileceği saniye cinsinden aralık
Maksimum başarısız deneme sayısı (Max. number of failed trials)	Bağlantının kapalı olduğu ilan edilene kadar başarısız ping denemelerinin maksimum sayısı
Acil eylem (Emergency action)	Maksimum kesinti süresine ulaşıldıktan sonra alınması gereken acil eylem. Yeniden başlatmayı kullanmak sistemin yeniden başlatılmasını sağlar, yeniden başlatma bağlantı hizmetleri modemın sıfırlanması dahil olmak üzere tüm bağlantıyla ilgili uygulamaları yeniden başlatır.

WAN Ayarları

Bu sayfa, Maksimum Segment Boyutu (MSS) gibi WAN'a özgü ayarları yapılandırmak için kullanılabilir. MSS, yönlendiricinin tek bir parçalanmamış TCP segmentinde işleyebileceği en büyük veri miktarına (bayt cinsinden) karşılık gelir. Herhangi bir olumsuz yan etkiyi önlemek için, veri segmentindeki ve başlıklardaki bayt sayısı Maksimum İletim Birimi'ndeki (MTU) bayt sayısından fazla olmamalıdır. MTU, her arayüz için yapılandırılabilir ve iletilebilecek en büyük paket boyutuna karşılık gelir.



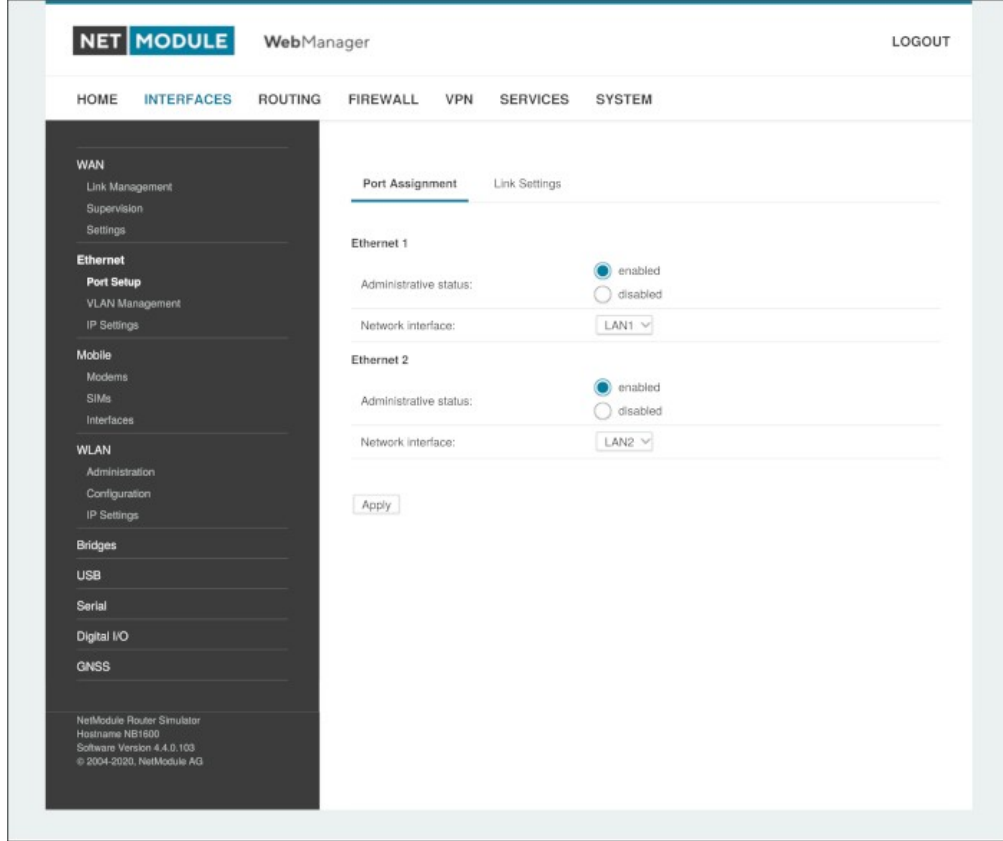
Ekran 6.5.: WAN Ayarları

Parametre	Bağlantı Denetimi (Link Supervision) Ayarları
MSS ayarlaması (MSS adjustment)	WAN arayüzlerinde MSS ayarını etkinleştirin veya devre dışı bırakın.
Maksimum segment boyutu (Maximum segment size)	Bir TCP veri segmentindeki azami bayt sayısı.

6.3.2. Ethernet

NB3800 yönlendiricileri, M12 konektörleri aracılığıyla bağlanabilen 2 Gigabit Ethernet portu (ETH4/ETH5) içeren bir Ethernet anahtarıyla (ETH1-ETH5) birlikte gelir. ETH1 genellikle LAN amaçları için kullanılması gereken LAN1 arayüzünü oluşturur. Diğer arayüzler, diğer LAN segmentlerini bağlamak veya bir WAN bağlantısı yapılandırmak için kullanılabilir. LAN10 arayüzü, önceden yapılandırılmış bir USB Ethernet cihazı takıldığında kullanılabilir olacaktır.

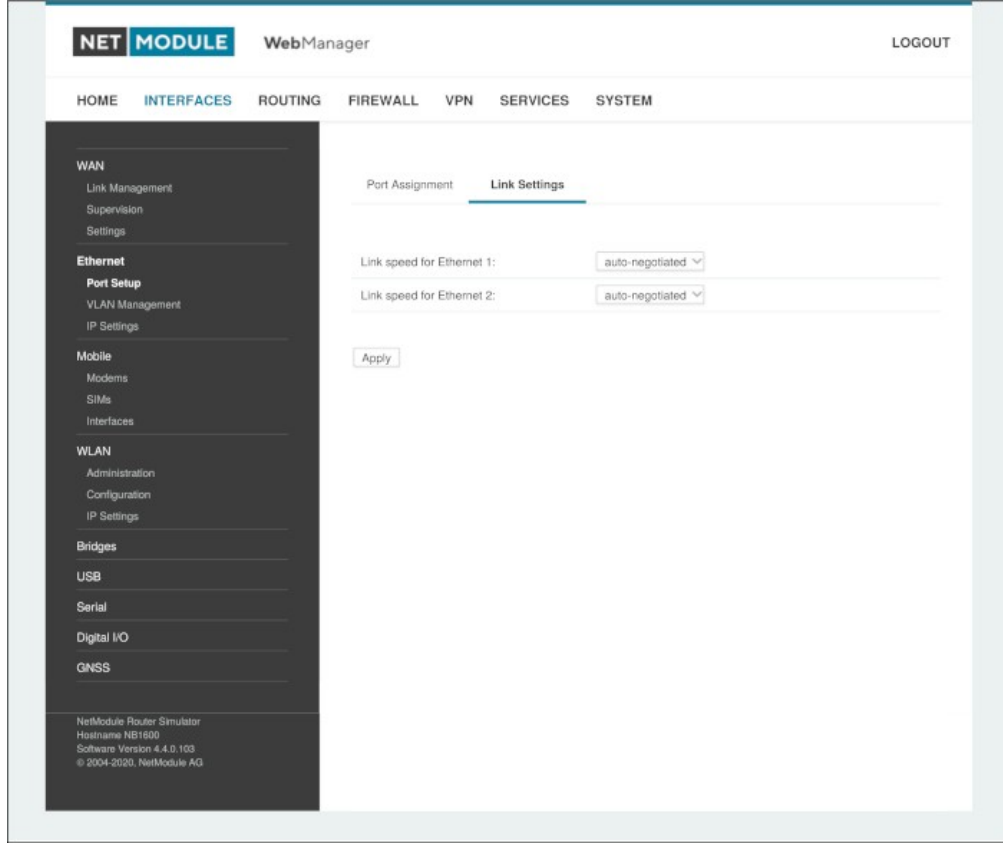
Ethernet Portu Atama



Ekran 6.6.: Ethernet Bağlantı Noktaları

Bu menü, her Ethernet portunu ayrı ayrı bir LAN arayüzüne atamak için, her port için farklı alt ağlar kullanmak için veya bir portu WAN arayüzü olarak kullanmak istemeniz durumunda kullanılabilir. Aynı arayüze birden fazla port atayabilirsiniz.

Ethernet Bağlantı Ayarları



Ekran 6.7.: Ethernet Bağlantı Ayarları

Bağlantı müzakeresi her Ethernet portu için ayrı ayrı ayarlanabilir. Çoğu cihaz, bağlantı hızını ağdaki diğer cihazlarla uyumlu olacak şekilde otomatik olarak yapılandırarak otomatik müzakereyi destekler. Müzakere sorunları durumunda, modları manuel olarak atayabilirsiniz ancak ağdaki tüm cihazların aynı ayarları kullandığından emin olunmalıdır.

IEEE 802.1X üzerinden kimlik doğrulama

LOGOUT

HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM

Port Assignment Link Settings **Wired 802.1X**

Ethernet 1

Wired 802.1X status: disabled
 Client
 Authenticator

Ethernet 2

Wired 802.1X status: disabled
 Client
 Authenticator

EAP type: PEAP

Anonymous identity: Netmodule-Anon

Identity: testid

Password: ***** show

Certificates: missing
[Manage keys and certificates](#)

Ethernet 3

Wired 802.1X status: disabled
 Client
 Authenticator

Reauthentication Period: 3600

Authenticator ID: Netmodule-Auth

Use MAB:

Ethernet 4

Wired 802.1X status: disabled
 Client
 Authenticator

Ethernet 5

Wired 802.1X status: disabled
 Client
 Authenticator

Apply

NB3800 NetModule Router
Hostname: nb
Software Version: 4.7.0.100
© 2004-2022, NetModule AG

Ekran 6.8.: IEEE 802.1X ile Kimlik Doğrulama

NetModule AG yönlendiricileri IEEE 802.1X standardı üzerinden kimlik doğrulamayı destekler. Bu, her Ethernet portu için ayrı ayrı yapılandırılabilir. Aşağıdaki seçenekler mevcuttur:

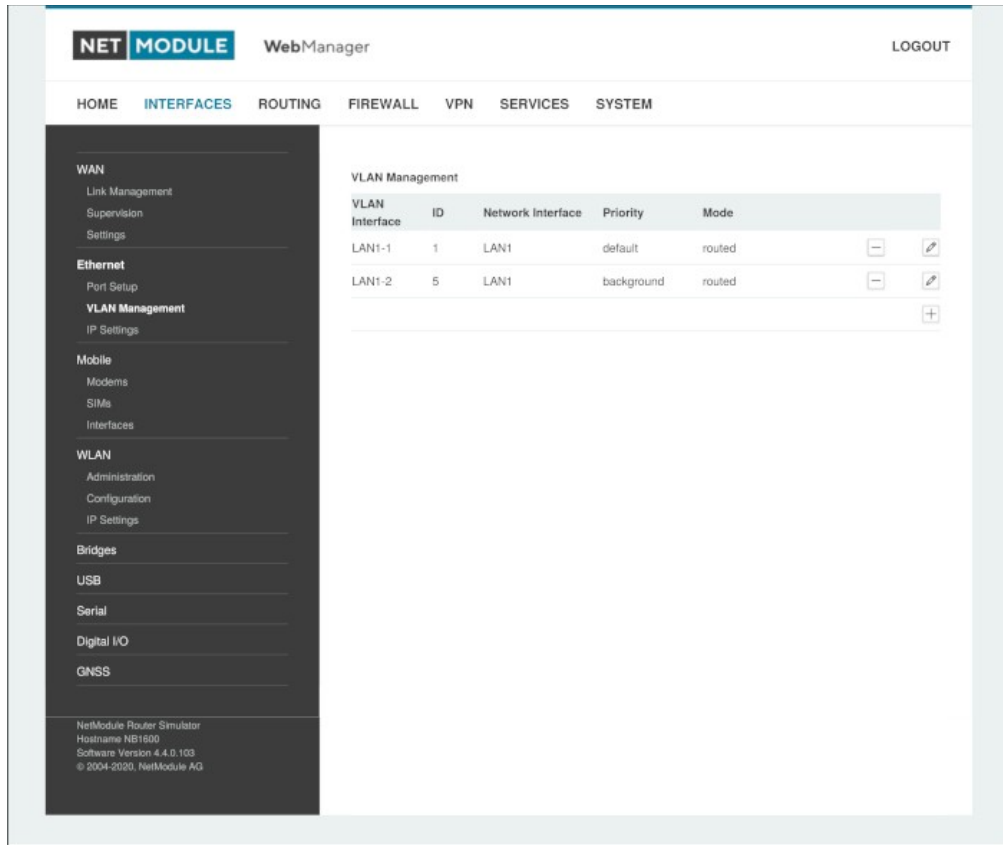


Parametre	Bağlantı Denetimi (Link Supervision) Ayarları
Kablolu 802.1X durumu (Wired 802.1X status)	İstemci ise, yönlendirici bu portta IEEE 802.1X ile kimlik doğrulaması yapar
EAP tipi (EAP type)	Kimlik doğrulaması için hangi protokol kullanılmalı
Anonim kimlik (Anonymous identity)	PEAP kimlik doğrulaması için anonim kimlik
Kimlik (Identity)	EAP-TLS veya PEAP kimlik doğrulaması için kimlik (gerekli)
Parola (Password)	PEAP kimlik doğrulaması için parola (gerekli)
Sertifikalar (Certificates)	EAP-TLS veya PEAP üzerinden kimlik doğrulaması için sertifikalar. Bölüm 6.8.8'de yapılandırılabilir

Parametre	IEEE 802.1X Kimlik Doğrulayıcı Ayarları
Kablolu 802.1X durumu (Wired 802.1X status)	Kimlik Doğrulayıcı olarak ayarlanırsa, yönlendirici bu bağlantı noktasındaki IEEE 802.1X kimlik doğrulama isteklerini yapılandırılmış bir RADIUS sunucusuna yayar (bkz. bölüm 6.8.2)
Yeniden Doğrulama Süresi (Reauthentication Period)	Bağlı bir istemcinin yeniden kimlik doğrulaması yapması gereken saniye cinsinden süre
Kimlik Doğrulayıcı Kimliği (Authenticator ID)	Bu benzersiz ad, RADIUS sunucusundaki kimlik doğrulayıcıyı tanımlar
MAB'ı kullan (Use MAB)	MAC Kimlik Doğrulama Baypası aracılığıyla IEEE 802.1X yeteneğine sahip olmayan cihazların kimlik doğrulamasına izin vermek istiyorsanız bu seçeneği etkinleştirin. Bunlar, kullanıcı adı ve parola olarak MAC adresleriyle RADIUS sunucusuna bildirilir

VLAN Yönetimi

NetModule AG yönlendiricileri, bir Ethernet arayüzünün üstünde sanal arayüzler oluşturmak için kullanılabilen IEEE 802.1Q'ya göre Sanal LAN'ı destekler. VLAN protokolü, paketleri ilişkili sanal arayüze dağıtmak için kullanılan bir VLAN Tanımlayıcısı (VLAN Kimliği) taşıyan Ethernet çerçevelerine ek bir başlık ekler. Etiketlenmemiş paketler ve atanmamış bir kimliğe sahip paketler yerel arayüze dağıtılacaktır.



Ekran 6.9.: VLAN Yönetimi

Ayrık bir alt ağ oluşturmak için, uzak bir LAN ana bilgisayarının ağ arayüzü, yönlendiricide tanımlananla aynı VLAN kimliğiyle yapılandırılmalıdır. Ayrıca, 802.1P, TCP/IP yığımında paket planlamasını etkileyen bir öncelik alanı sunar.

Parametre	VLAN Öncelik Seviyeleri
0	Arka plan (Background)
1	En İyi Çaba (Best Effort)
2	Mükemmel Çaba (Excellent Effort)
3	Kritik Uygulamalar (Critical Applications)
4	Video (< 100 ms gecikme ve titreme)
5	Ses (< 10 ms gecikme ve titreme)
6	İnternet Ağı Kontrolü (Internetwork Control)
7	Ağ Kontrolü (Network Control)

IP Ayarları

Bu sayfa LAN/WAN Ethernet arayüzleriniz için IP adreslemesini yapılandırmak için kullanılabilir.

Parametre	LAN IP Ayarları
Mode	Bu arayüzün LAN veya WAN arayüzü olarak kullanılıp kullanılmadığını tanımlar.
MTU	Arayüz için Maksimum İletim Birimi (Maximum Transmission Unit), sağlandığı takdirde arayüzde iletilen paketin en büyük boyutunu belirtir.

The screenshot displays the web interface for IP Address Management. The top navigation bar includes HOME, INTERFACES, ROUTING, FIREWALL, VPN, SERVICES, and SYSTEM. The left sidebar lists various configuration categories: WAN, Ethernet, Mobile, WLAN, Bridges, USB, Serial, and GNSS. The main content area is titled 'IP Address Management' and contains a table with the following data:

Network Interface	Mode	IP Address Mode	IP Address	Netmask	
LAN1	LAN	STATIC	192.168.1.1	255.255.255.0	
LAN1-1	LAN	STATIC	192.168.101.1	255.255.255.0	
LAN1-2	LAN	STATIC	192.168.102.1	255.255.255.0	
LAN2	WAN	DHCP	-	-	

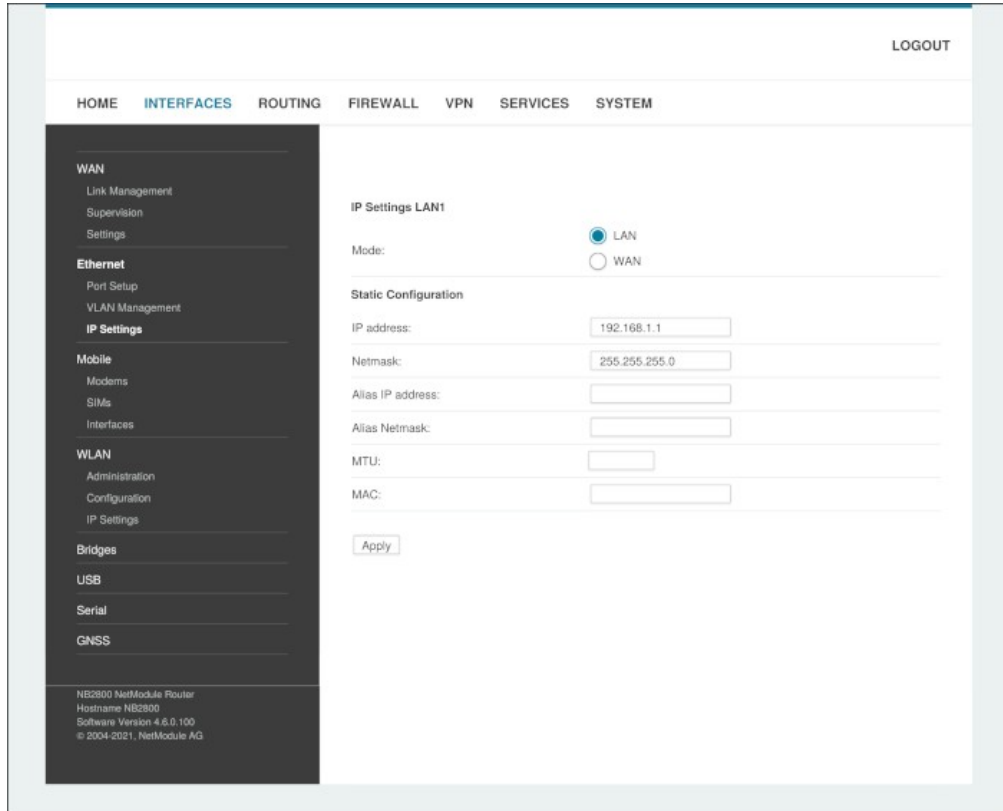
At the bottom of the sidebar, the following information is displayed: NB2800 NetModule Router, Hostname NB2800, Software Version 4.8.0.104, © 2004-2021, NetModule AG.

Ekran 6.10.: LAN IP Yapılandırma

LAN-Modu

LAN modunda çalışırken, arayüz aşağıdaki ayarlarla yapılandırılabilir:

Parametre	LAN IP Ayarları
IP Adresi (IP address)	IP arayüzü adresi
Ağ maskesi (Netmask)	Bu arayüz için ağ maskesi
Takma ad IP adresi (Alias IP address)	İsteğe bağlı takma ad IP arayüz adresi
Takma ad ağ maskesi (Alias Netmask)	Bu arayüz için isteğe bağlı takma ad ağ maskesi
MAC	Bu arayüz için özel MAC adresi (VLAN'lar için desteklenmez)



Ekran 6.11: LAN IP Yapılandırma - LAN Arayüzü

WAN-Modu

WAN modunda çalışırken, arayüz aşağıdaki şekilde iki IP sürümü ile yapılandırılabilir:

Parametre	LAN IP Ayarları
IPv4	Yalnızca İnternet Protokolü Sürüm 4
Ipv6	Yalnızca İnternet Protokolü Sürüm 6
Çift Yığın (Dual-Stack)	IP Sürüm 4 ve Sürüm 6'yı paralel olarak çalıştırın

The screenshot displays the WAN IP Settings LAN1 configuration page. The interface includes a navigation menu on the left with categories like WAN, Ethernet, Mobile, WLAN, Bridges, USB, Serial, and GNSS. The main content area is titled 'IP Settings LAN1' and contains the following configuration options:

- Mode:** Radio buttons for LAN, WAN (selected), IPv4, IPv6, and Dual-Stack.
- IP version:** Radio buttons for DHCP (selected), Static, and PPPoE.
- IPv4 Configuration:** Radio buttons for DHCP (selected), Static, and PPPoE.
- IPv6 Configuration:** Radio buttons for SLAAC (selected) and Static.
- MTU:** A text input field.
- MAC:** A text input field.
- Apply:** A button to save the configuration.

At the bottom left of the interface, the following information is displayed: NB2800 NetModule Router, Hostname NB2800, Software Version 4.8.0.100, © 2004-2021, NetModule AG.

Ekran 6.12.: LAN IP Yapılandırması - WAN Arayüzü



Seçtiğiniz IP sürümüne bağlı olarak arayüzünüzü aşağıdaki ayarlarla yapılandırabilirsiniz:

IPv4 Ayarları

Yönlendirici IPv4 adresini aşağıdaki yollarla yapılandırabilir:

Parametre	IPv4 WAN-Modları
DHCP	DHCP istemcisi olarak çalıştırıldığında, tüm IP ile ilgili ayarlar (adres, alt ağ, ağ geçidi, DNS sunucusu) ağdaki bir DHCP sunucusundan alınacağından başka bir yapılandırmaya gerek yoktur.
Statik (Static)	Statik değerler tanımlamanıza olanak tanır. Aksi takdirde ağda IP çakışmaları yaratacağından benzersiz bir IP adresi atamak konusunda dikkatli olunmalıdır.
PPPoE	PPPoE, genellikle başka bir WAN erişim cihazıyla (örneğin bir DSL modem) iletişim kurulurken kullanılır.

IPv4-PPPoE Ayarları

Aşağıdaki ayarlar uygulanabilir:

Parametre	PPPoE Yapılandırma
Kullanıcı Adı (User Name)	Erişim aygıtında kimlik doğrulaması için PPPoE kullanıcı adı
Parola (Password)	Erişim cihazında kimlik doğrulama için PPPoE şifresi
Servis adı (Service name)	Erişim yoğunlaştırıcısının hizmet adı kümesini belirtir ve aynı fiziksel ağda birden fazla hizmetiniz yoksa ve bağlanmak istediğinizi belirtmeniz gerekmiyorsa boş bırakılabilir.
Erişim yoğunlaştırıcısı ad (Access concentrator name)	Konsantratörün adı (PPPoE istemcisi boş bırakılırsa herhangi bir erişim konsantratörüne bağlanacaktır)

IPv6 Ayarları

Aşağıdaki ayarlar uygulanabilir:

Parametre	IPv6 WAN-Modları
SLAAC	Tüm IP ile ilgili ayarlar (adres, önek, rotalar, DNS sunucusu) komşu keşif protokolü tarafından durumsuz adres otomatik yapılandırması yoluyla alınacaktır.
Statik (Static)	Statik değerler tanımlamanıza olanak tanır. Aksi takdirde ağda IP çakışmaları yaratacağından benzersiz bir IP adresi atamak konusunda dikkatli olunmalıdır. Yalnızca genel adresleri yapılandırabilirsiniz. Bağlantı yerel adresi MAC adresi aracılığıyla otomatik olarak oluşturulur.

DNS Sunucusu

Etkinleştirilmiş tüm IP sürümleri Statik olarak ayarlandığında, arayüze özgü bir ad sunucusu yapılandırabilirsiniz. Arayüze özgü ad sunucularını geçersiz kılmak için 6.7.3. bölümüne bakın.

6.3.3. Mobil

Modemler

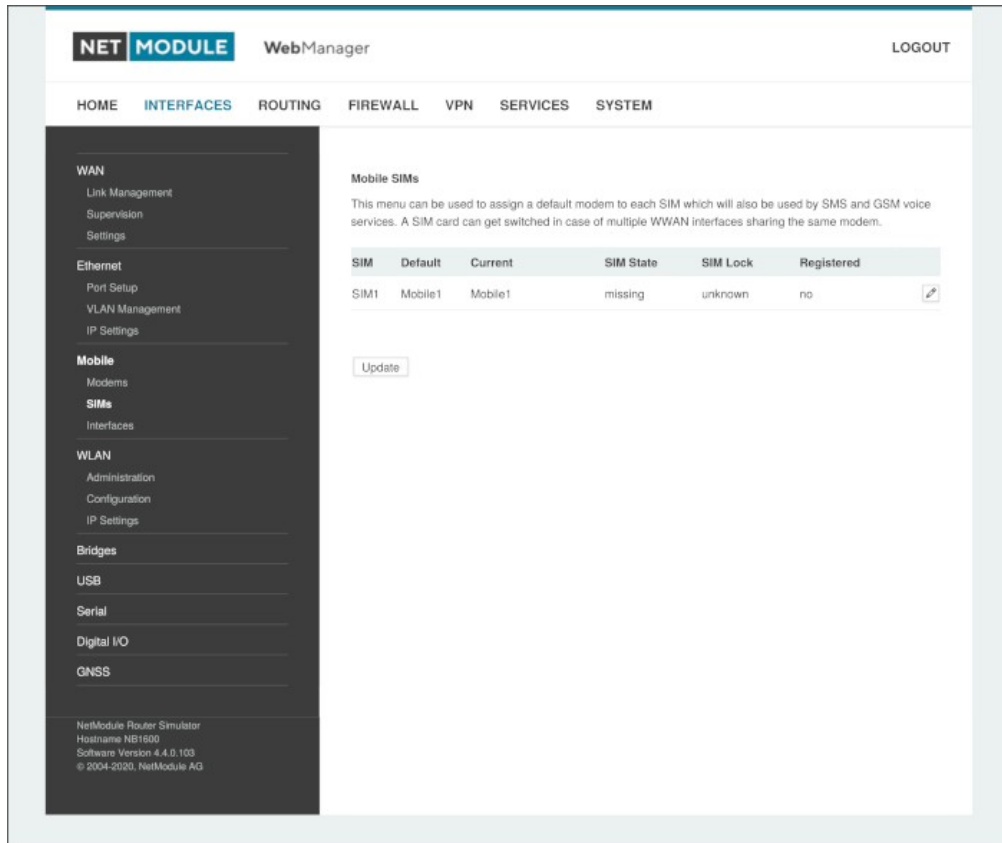
Yapılandırma

Bu sayfa tüm mevcut WWAN modemlerini listeler. İsteğe bağlı olarak devre dışı bırakılabilirler.

Sorgulama (Query)

Bu sayfa, modeme Hayes AT komutları göndermenizi sağlar. 3GPP uyumlu AT komut setinin yanı sıra, talep üzerine sağlayabileceğimiz modem-özelinde başka komutlar da uygulanabilir. Bazı modemler, örneğin ön ödemeli bir hesabın kullanılabilir bakiyesini sorgulamak için Yapılandırılmamış Ek Hizmet Verisi (Unstructured Supplementary Service Data, USSD) isteklerini çalıştırmayı da destekler.

SIM'ler



Ekran 6.13.: SIM'ler

SIM sayfası, mevcut SIM kartları, atanmış modemleri ve mevcut durum hakkında genel bir bakış sunar. Bir SIM kart takıldıktan, bir modeme atandıktan ve başarıyla kilidi açıldıktan sonra, kart hazır durumda kalmalı ve ağ kayıt durumu kayıtlı ("registered") olarak dönmelidir. Aksi takdirde lütfen PIN kodunuzu tekrar kontrol edin.

Lütfen bir ağa kaydolmanın genellikle biraz zaman aldığını ve sinyal gücüne ve olası radyo enterferanslarına bağlı olduğunu unutmayın. PIN kilidini açmayı yeniden başlatmak ve başka bir ağ kayıt girişimini tetiklemek için istediğiniz zaman "Update" (Güncelle) düğmesine basabilirsiniz.

Bazı durumlarda (örneğin modem baz istasyonları arasında geçiş yaparsa) belirli bir hizmet türü ayarlamak veya sabit bir operatör atamak gerekebilir. Çevredeki operatörlerin listesi bir ağ taraması başlatılarak elde edilebilir (60 saniyeye kadar sürebilir). Modeme doğrudan sorgu göndererek daha fazla ayrıntı alınabilir, talep üzerine uygun komutlar seti sağlanabilir.



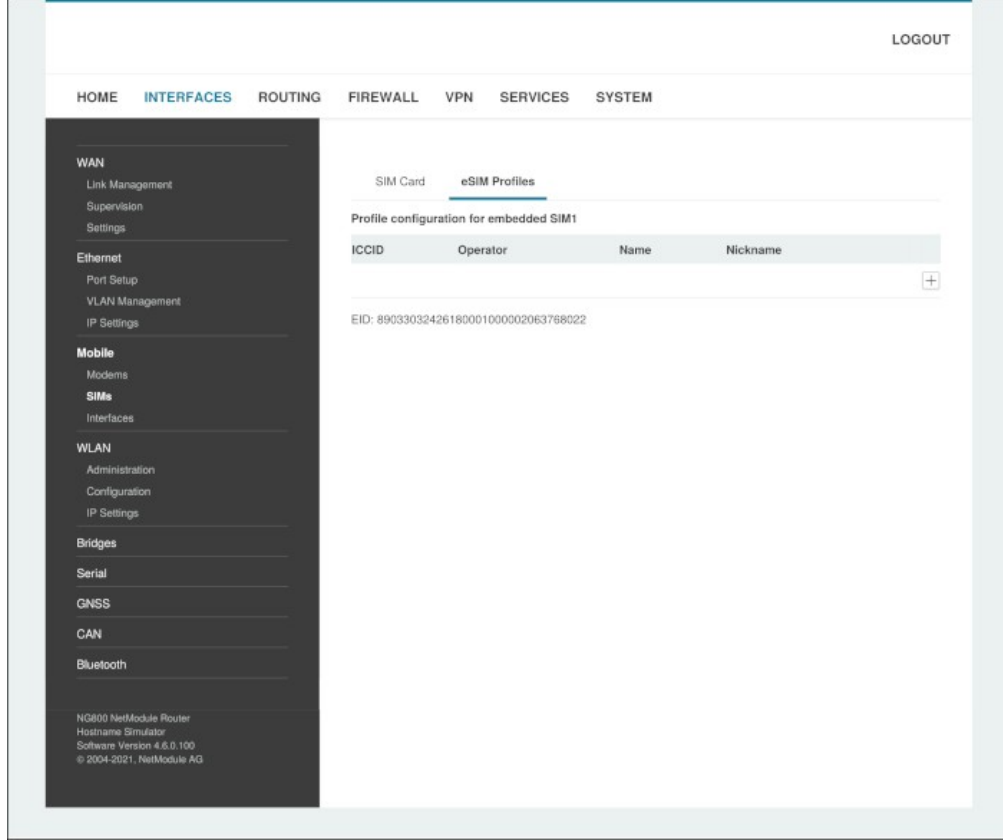
Yapılandırma

Bir SIM kart genellikle varsayılan bir modeme atanır ancak örneğin bir modemle ancak farklı SIM kartlarla iki WWAN arayüzü kurarsanız değiştirilebilir. Diğer hizmetler (SMS veya Ses gibi) o modemde çalışırken dikkatli olunmalıdır çünkü bir SIM anahtarı doğal olarak bunların çalışmasını etkileyecektir. Aşağıdaki ayarlar uygulanabilir:

Parametre	WWAN SIM Yapılandırma
PIN kodu (PIN code)	SIM kartın kilidini açmak için PIN kodu
PUK kodu (PUK code)	SIM kartın kilidini açmak için PUK kodu (isteğe bağlı)
Varsıyal modem (Default modem)	Bu SIM karta atanan varsayılan modem
Tercih edilen servis (Preferred service)	Bu SIM kartla kullanılacak tercih edilen servis. Bağlantı yöneticisinin farklı ayarlar durumunda bunu değiştirebileceğini unutmayın. Varsayılan otomatik kullanmaktır, karışan baz istasyonlarının olduğu bölgelerde, etraftaki istasyonlar arasında herhangi bir dalgalanmayı önlemek için belirli bir türü (ör. yalnızca 3G) zorlayabilirsiniz.
Kayıt modu (Registration mode)	İstenilen kayıt modu
Ağ seçimi (Network selection)	Hangi ağın seçileceğini tanımlar. Bu, bir ağ taraması çalıştırılarak alınabilen belirli bir sağlayıcı kimliğine (Public Land Mobile Network, PLMN) bağlanabilir.

**Dikkat:**

- eUICC profillerinin fabrika ayarlarına sıfırlama işleminden **ETKİLENMEDİĞİNİ** unutmayın. Bir eUICC profilini bir cihazdan kaldırmak için, fabrika ayarlarına sıfırlama işlemini gerçekleştirmeden önce manuel olarak kaldırın.



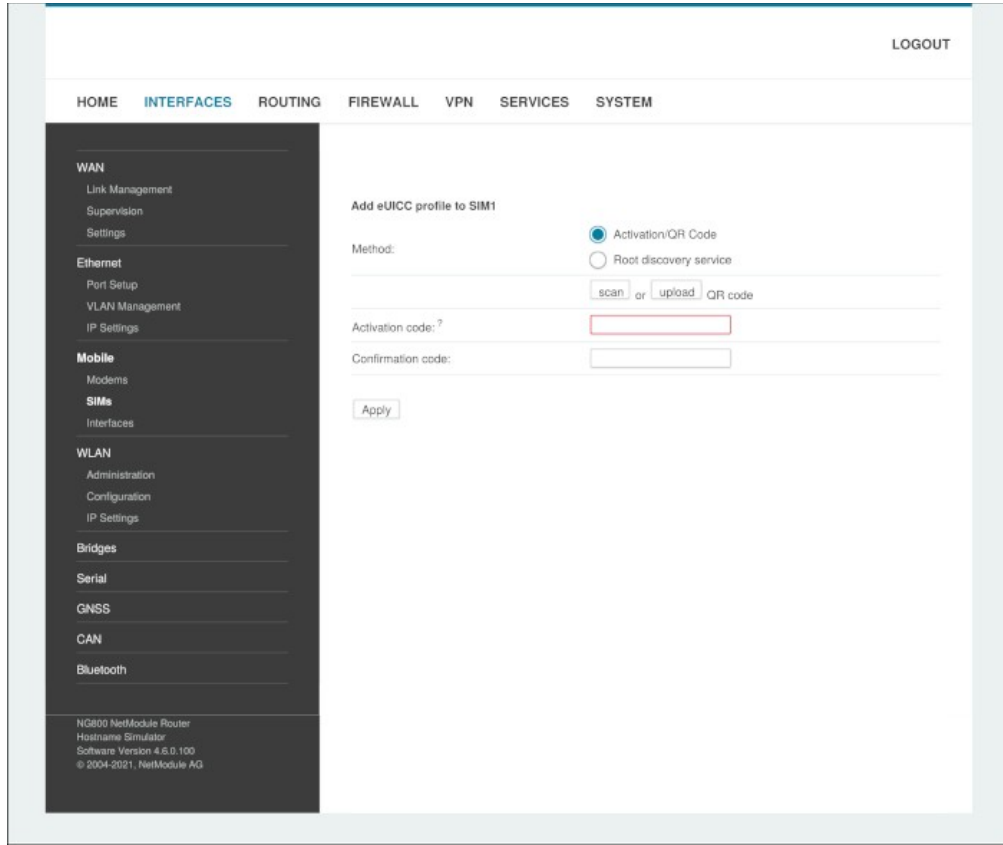
Ekran 6.14.: eSIM Profilleri

Seçili yönlendirici modelleri, yönlendiriciye fiziksel bir SIM kart takmak yerine internetten yönlendiriciye eSIM profilleri indirmenize olanak tanıyan bir eUICC (gömülü evrensel entegre devre kartı) içerir.

Kurulacak eSIM profilleri GSMA RSP Teknik Spesifikasyonu SGP.22 ile uyumlu olmalıdır. Bunlar, mevcut cep telefonlarında kullanılan eSIM profilleriyle aynıdır. Eski GSMA SGP.02 spesifikasyonuna göre profiller desteklenmez.

eSIM profilleri, "Mobil / SIM'ler" yapılandırma sayfasının "eSIM Profilleri" sekmesinden yönetilebilir. Yönetim sayfası, yüklü tüm eSIM profillerini görüntülemenize ve eSIM profillerini yüklemenize, etkinleştirmenize, devre dışı bırakmanıza ve silmenize olanak tanır. Ayrıca her profil için bir takma ad kaydetmek de mümkündür.

eUICC, profillerin boyutuna bağlı olarak yaklaşık 7 eSIM profili depolayabilir. Bu profillerden aynı anda yalnızca biri etkin olabilir. Yeni eSIM profilleri yüklemek için öncelikle yönlendiricinin profili mobil ağ operatörünün sunucusundan indirebilmesi için internete IP bağlantısı kurmanız gerekir.



Ekran 6.15.: eUICC Profili Ekleme

eSIM profillerini yüklemek için aşağıdaki iki yol desteklenir ve eSIM profilleri yapılandırma sayfasında seçilebilir:

1. Ağ operatörü tarafından sağlanan QR kodu

Bu yöntemi kullanarak eSIM profilini indirmek için mobil ağ operatörünüz size yüklenecek eSIM profili hakkında bilgi içeren bir QR kodu sağlar. Yönlendiricinin yapılandırma GUI'sine erişmek için kullandığınız cihazda bir kamera varsa, kamerayı kullanarak QR kodunu tarayabilirsiniz. Aksi takdirde QR kodunun bir görüntü dosyasını da yükleyebilirsiniz. Veya QR kodunun içeriğini ilgili giriş alanına manuel olarak girmek de mümkündür.

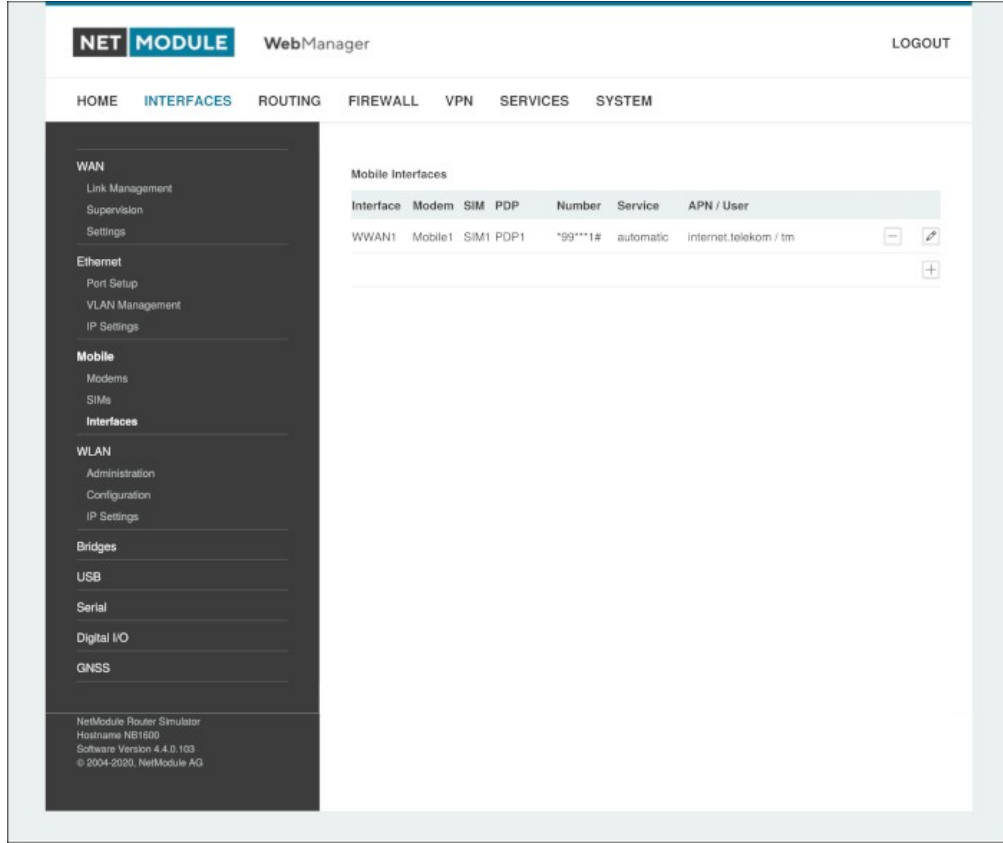
2. GSMA Kök Keşif Hizmeti

Bu yöntemi kullanırken, yönlendiricinin eUICC'sini tanımlayan benzersiz bir numara olan EID'yi mobil ağ operatörünüze sağlamanız gerekir. EID, eSIM profilleri yapılandırma sayfasında görüntülenir. Operatör daha sonra eSIM profilini kendi sağlama sunucularında yönlendiriciniz için hazırlayacaktır. Daha sonra, eSIM profilini indirmek için herhangi bir ek bilgi belirtmenize gerek kalmadan almak için GSMA Root Discovery Service yöntemini kullanabilirsiniz.

Not: Çoğu mobil şebeke operatörü bir eSIM profilinin yalnızca bir kez indirilmesine izin verir. Yani, profili bir kez indirip daha sonra silerseniz, aynı profili ikinci kez indiremezsiniz. Bu durumda operatörünüzden yeni bir eSIM profili talep etmeniz gerekir.

WWAN Arayüzleri

Bu sayfa WWAN arayüzlerinizi yönetmek için kullanılabilir. Bir arayüz eklendiğinde, ortaya çıkan bağlantı otomatik olarak WAN bağlantısı olarak açılır. Bunları nasıl yöneteceğiniz için lütfen 6.3.1 bölümüne bakın. Bağlantı kurma işlemi sırasında Mobil LED yanıp sönecek ve bağlantı kurulduğu anda yanmaya başlayacaktır. Bağlantı kurulamadıysa, sorunu gidermek için 6.8.7 bölümüne bakın veya sistem günlük dosyalarına bakın.



Ekran 6.16.: WWAN Arayüzleri

Aşağıdaki mobil ayarların yapılması gerekmektedir:

Parametre	WWAN Mobil Ayarları
Modem	Bu WWAN arayüzü için kullanılacak modem
SIM	Bu WWAN arayüzü için kullanılacak SIM kartı
Servis tipi (Service type)	İstenilen hizmet türü

Lütfen bu ayarların, bağlantı arandığı anda genel SIM tabanlı ayarların yerini alacağını unutmayın.



Genellikle, modem kayıt olduktan ve ağ sağlayıcısı veritabanımızda bulunduktan sonra bağlantı ayarları otomatik olarak türetilir. Aksi takdirde, aşağıdaki ayarların manuel olarak yapılandırılması gerekecektir:

Parametre	WWAN Bağlantı Ayarları
Telefon numarası (Phone number)	Aranacak telefon numarası, 3G+ bağlantıları için genellikle *99***1# olarak ifade edilir. Devre anahtarlamalı 2G bağlantıları için, aranacak sabit telefon numarasını uluslararası formatta (örn. +41xx) girebilirsiniz.
Erişim noktası adı	Kullanılan erişim noktası adı (Access Point Name, APN)
IP version (IP sürümü)	Hangi IP sürümünü kullanacağınız. Dual-stack, IPv4 ve IPv6'yı birlikte kullanmanıza olanak tanır. Lütfen sağlayıcınızın tüm IP sürümlerini desteklemeyebileceğini unutmayın.
Kimlik doğrulama (Authentication)	Kullanılan kimlik doğrulama şeması, gerekirse bu PAP veya/veya CHAP olabilir
Kullanıcı adı (Username)	Kimlik doğrulama için gerekli kullanıcı adı
Parola (Password)	Kimlik doğrulama için gerekli parola

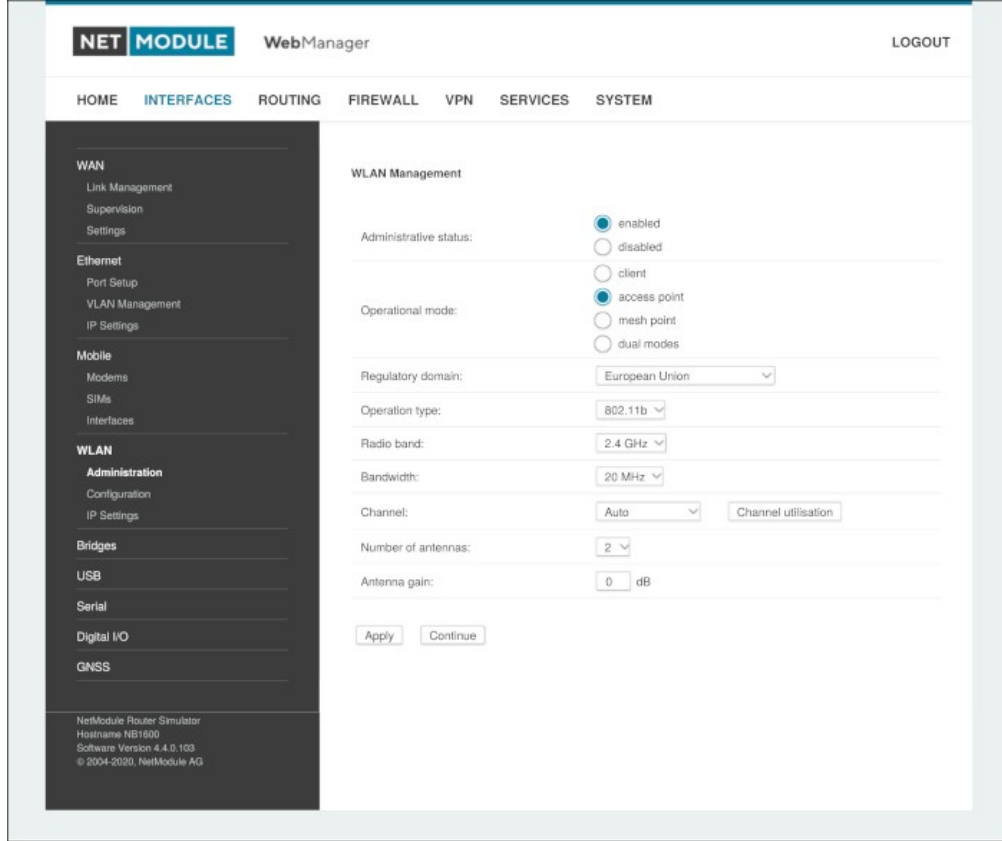
Ayrıca aşağıdaki gelişmiş ayarları yapılandırabilirsiniz:

Parametre	WWAN Gelişmiş Ayarlar
Gerekli sinyal gücü (Required signal strength)	Bağlantı çevrilmeden önce gereken minimum sinyal gücünü ayarlar
Sadece ülkenizdeki ağ (Home network only)	Bağlantının yalnızca ülkenizdeki bir mobil ağa kayıtlı olduğunda aranıp aranmayacağını belirler
DNS için anlaşılın (Negotiate DNS)	DNS müzakeresinin yapılıp yapılmayacağını ve alınan ad sunucularının sisteme uygulanıp uygulanmayacağını belirtir
ISDN'e arama (Call to ISDN)	ISDN modemle konuşan 2G bağlantıları durumunda etkinleştirilmesi gerekir
Başlık sıkıştırma (Header compression)	Yavaş seri bağlantılar üzerinden TCP/IP performansını artırabilecek 3GPP başlık sıkıştırmasını etkinleştirir veya devre dışı bırakır. Sağlayıcınız tarafından desteklenmesi gerekir.
Veri sıkıştırma (Data compression)	Verimi artırmak için paketlerin boyutunu küçülten 3GPP veri sıkıştırmasını etkinleştirir veya devre dışı bırakır. Sağlayıcınız tarafından desteklenmesi gerekir.
İstemci adresi (Client address)	Sağlayıcı tarafından atanmışsa sabit bir istemci IP adresi belirtir
MTU	Bu arayüz için Maksimum İletim Birimi (Maximum Transmission Unit)

6.3.4. WLAN

Yapılandırma

Yönlendiriciniz bir WLAN (veya Wi-Fi) modülüne sahip ise, onu istemci (“client”), erişim noktası (“access point”), ağ noktası (“mesh point”) veya belirli ikili modlar (“dual modes”) olarak çalıştırabilirsiniz. İstemci olarak, örneğin yedek bağlantı olarak kullanılabilen ek bir WAN bağlantısı oluşturabilir. Erişim noktası olarak, Ethernet tabanlı bir LAN arayüzüne köprülenebilen veya yönlendirme için kullanılabilen ve bir Ethernet LAN arayüzünün yaptığı gibi hizmetler (DHCP/DNS/NTP gibi) sağlamak için kullanılabilen bağımsız bir IP arayüzü oluşturabilen başka bir LAN arayüzü oluşturabilir. Ağ noktası olarak, dinamik yol seçimiyle bir geri yol bağlantısı sağlamak için kablosuz bir ağ ağı oluşturabilir. İkili mod olarak, aynı radyo modülünde erişim noktası ve istemci veya ağ noktası ve erişim noktası işlevselliğini çalıştırmak mümkündür.



Ekran 6.17.: WLAN Yönetimi

Yönetim durumu devre dışı (“disabled”) olarak ayarlanırsa, genel güç tüketimini azaltmak için modül kapatılır. Antenlerle ilgili olarak, daha iyi kapsama ve verim için genellikle iki anten kullanmanızı öneririz. 802.11n'de olduğu gibi daha yüksek verim oranlarına ulaşmak istiyorsanız ikinci bir anten kesinlikle zorunludur.

Bir WLAN istemcisi (“client”) ve bir ağ noktası (“mesh point”) otomatik olarak bir WAN bağlantısı haline gelir ve 6.3.1. bölümde açıklandığı gibi yönetilebilir.

Erişim noktası, istemci modu, ağ noktası ve herhangi bir ikili mod için yapılandırılabilir parametreler:

Parametre	WLAN Yönetimi
Düzenleyici etki alanı (Regulatory Domain)	Yönlendiricinin çalıştığı ülkeyi seçin
Anten sayısı (Number of antennas)	Bağlı anten sayısını ayarlayın
Anten kazancı (Antenna gain)	Bağlı antenler için anten kazanımını belirtin. Doğru kazanım değeri için lütfen anten veri sayfasına bakın.
Tx gücü (Tx power)	dBm cinsinden kullanılan azami iletim gücünü belirtir.
Düşük veri hızlarını devre dışı bırak (Disable low data rates)	Düşük veri hızlarını devre dışı bırakarak ağa düşük hızla bağlanan istemcilerden kaçının.

**Dikkat:**

- Uygunsuz parametrelerin uygunluk düzenlemelerinin ihlaline yol açabileceğini lütfen unutmayın.

Erişim noktası veya ikili mod olarak çalıştırırken, aşağıdaki ayarları daha ayrıntılı olarak yapılandırabilirsiniz:

Parametre	WLAN Yönetimi
İşlem türü (Operation type)	İstenen IEEE 802.11 çalışma modunu belirtir
Radyo bantı (Radio band)	Bağlantılar için kullanılacak radyo bandını seçer, modülünüze bağlı olarak 2,4 veya 5 GHz olabilir
Dış mekan (Outdoor)	5 GHz dış mekan kanallarını gösterir
Bant genişliği (Bandwidth)	Kanal bant genişliği çalışma modunu belirtin
Kanal (Channel)	Kullanılacak kanalı belirtir
istemci takibini etkinleştir (enable client tracking)	İlişkili olmayan istemcilerin izlenmesini sağlar
Kısa Koruma Aralığı (Short Guard Interval)	Kısa Koruma Aralığını (SGI, Short Guard Interval) etkinleştirir

İstemci (client) olarak çalıştırdığınızda, aşağıdaki ayarları daha ayrıntılı olarak yapılandırabilirsiniz:

Parametre	WLAN Yönetimi
Kanalları tara (Scan channels)	Desteklenen tüm kanalların mı yoksa yalnızca kullanıcı tanımlı kanalların mı taranacağını seçin
2.4 GHz	2,4 GHz'de taranması gereken kanalları ayarlayın
5 GHz	5 GHz'de taranması gereken kanalları ayarlayın



Mevcut çalışma modları şunlardır:

Standart	Frekanslar	Bant Genişliği	Veri Hızı
802.11a	5 GHz	20 MHz	54 Mbit/s
802.11b	2.4 GHz	20 MHz	11 Mbit/s
802.11g	2.4 GHz	20 MHz	54 Mbit/s
802.11n	2.4/5 GHz	20/40 MHz	300 Mbit/s
802.11ac	5 GHz	20/40/80 MHz	866.7 Mbit/s

Tablo 6.25.: IEEE 802.11 Ağ Standartları

Mesh noktası olarak çalıştırdığınızda, aşağıdaki ayarları daha ayrıntılı olarak yapılandırabilirsiniz:

Parametre	WLAN Ağ-Noktası Yönetimi
Radyo bantı (Radio band)	Bağlantılar için kullanılacak radyo bandını seçer, modülünüze bağlı olarak 2,4 veya 5 GHz olabilir
Kanal (Channel)	Kullanılacak kanalı belirtir

Not: 802.11n ve 802.11ac destekli NetModule Yönlendiriciler 2x2 MIMO'yu destekler

Bir erişim noktası kurmadan önce, komşu WLAN ağlarının bir listesini almak için bir ağ taraması çalıştırmak ve ardından daha az karışan kanalı seçmek her zaman iyi bir fikirdir. Lütfen 802.11n ve 40 MHz bant genişliği ile iyi verimler elde etmek için iki yeterli kanalın gerekli olduğunu unutmayın.

WLAN Yapılandırması

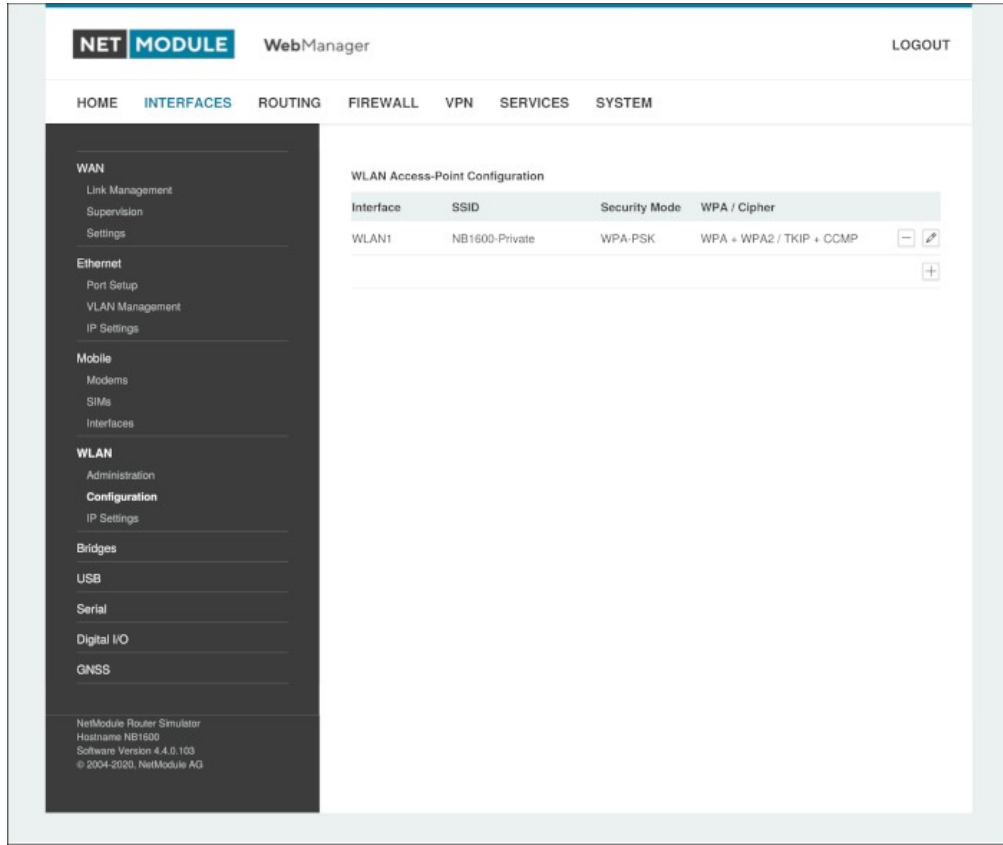
İstemci modunda çalışırken, bir veya daha fazla uzak erişim noktasına bağlanmak mümkündür. Sistem, bir tanesi kapanırsa listedeki bir sonraki ağa geçecek ve geri döndüğünde en yüksek öncelikli ağa geri dönecektir. Bir WLAN ağ taraması gerçekleştirebilir ve keşfedilen bilgilerden ayarları doğrudan seçebilirsiniz. Kimlik doğrulama bilgileri, uzak erişim noktasının operatörü tarafından alınmalıdır.

Parametre	WLAN İstemci Yapılandırması
SSID	Kablosuz ağın adı (SSID olarak adlandırılır)
Güvenlik Modu (Security mode)	İstenen güvenlik modu
WPA modu (WPA mode)	İstenilen şifreleme yöntemi. WPA3, WPA2 ve WPA1'e tercih edilmelidir.
WPA şifresi (WPA cipher)	Kullanılacak WPA şifresi, varsayılan olarak her ikisini de (TKIP ve CCMP) çalıştırmaktır
Kimlik (Identity)	WPA-RADIUS ve WPA-EAP-TLS için kullanılan kimlik
Parola (Passphrase)	WPA-Personal ile kimlik doğrulama için kullanılan parola ifadesi, aksi takdirde WPA-EAP-TLS için anahtar parola ifadesi
Gerekli sinyal gücü (Required signal strength)	Bağlantıyı kurmak için gereken sinyal gücü

İstemci (client), bir ESS içinde dolaşma amacıyla arka plan taramaları gerçekleştiriyor. Arka plan taramaları, geçerli sinyal gücüne dayanmaktadır.

Parametre	WLAN İstemcisi Arka Plan Tarama Ayarları
Eşik (Threshold)	Uzun veya kısa zaman aralığının oluşması gereken dBm cinsinden sinyal gücü eşiği
Uzun aralık (Long interval)	Eşik değeri belirtilen eşik değerinin üzerindeyse arka plan taramasının yapılması gereken saniye cinsinden süre
Kısa aralık (Short interval)	Eşik değeri belirtilen eşik değerinin altındaysa arka plan taramasının yapılması gereken saniye cinsinden süre

Erişim noktası (access-point) modunda çalışırken, her biri kendi ağ yapılandırmasını çalıştıran 8 adede kadar SSID oluşturabilirsiniz. Ağlar, bir LAN arayüzüne ayrı ayrı köprülenebilir veya yönlendirme modunda özel arayüz olarak çalışabilir.



Ekran 6.18.: WLAN Yapılandırma



Bu bölüm güvenlikle ilgili ayarları yapılandırmak için kullanılabilir.

Parametre	WLAN Erişim Noktası Ayarları
SSID	Kablosuz ağ adı
Güvenlik modu (Security mode)	İstenen güvenlik modu
WPA modu (WPA mode)	WPA1 yerine WPA2 tercih edilmelidir, WPA/WPA2 karma modunu çalıştırmak her ikisini de sunar.
WPA şifresi (WPA cipher)	Kullanılacak WPA şifresi, varsayılan olarak her ikisini de (TKIP ve CCMP) çalıştırmaktır
Parola (Passphrase)	WPA-Personal ile kimlik doğrulaması için kullanılan parola.
Zorunlu PMF (Force PMF)	Korunan Yönetim Çerçevesini (Protected Management Frames) etkinleştirir
SSID sakla (Hide SSID)	SSID'yi sakla
İstemciler izole edilsin (Isolate clients)	İstemciden istemciye iletişimi devre dışı bırak
Bant yönlendirme (Band steering master)	İstemcinin yönlendirilmesi gereken WLAN arayüzü
Fırsatçı Kablosuz Şifreleme geçişi (Opportunistic Wireless Encryption transition)	AÇIK WLAN'dan OWE şifreli WLAN arayüzüne sorunsuz geçiş için WLAN arayüzü
Hesap yönetimi (Accounting)	Hesap profilini ayarlar

Aşağıdaki güvenlik modları yapılandırılabilir:

Parametre	WLAN Güvenlik Modları
Kapalı (Off)	SSID devre dışı bırakıldı
Hiçbiri (None)	Kimlik doğrulaması yok, açık bir ağ sağlıyor
WEP	WEP (günümüzde önerilmemektedir)
WPA-Personal	WPA-Kişisel (TKIP, CCMP), parola tabanlı kimlik doğrulaması sağlar
WPA-Enterprise	Erişim noktası (Access-Point, AP) modunda WPA-Enterprise, 6.8.2 bölümünde yapılandırılabilen uzak bir RADIUS sunucusuna karşı kimlik doğrulaması yapmak için kullanılabilir
WPA-RADIUS	İstemci modunda EAP-PEAP/MSCHAPv2, 6.8.2 bölümünde yapılandırılabilen uzak bir RADIUS sunucusuna karşı kimlik doğrulaması yapmak için kullanılabilir
WPA-TLS	İstemci modunda EAP-TLS, 6.8.8 bölümünde yapılandırılabilen sertifikaları kullanarak kimlik doğrulaması gerçekleştirir
OWE	Fırsatçı Kablosuz Şifreleme diğer adıyla Geliştirilmiş AÇIK, herhangi bir kimlik doğrulaması olmadan WLAN şifrelemesi sağlar



Ağ noktası (mesh-point) modunda çalışırken, aynı anda mesh ağı içindeki bir veya daha fazla mesh noktasına bağlanmak mümkündür. Sistem otomatik olarak kablosuz ağı katılacak, aynı ID ve güvenlik kimlik bilgilerine sahip diğer mesh ortaklarına bağlanacaktır. Kimlik doğrulama kimlik bilgileri mesh ağının operatörü tarafından alınmalıdır.

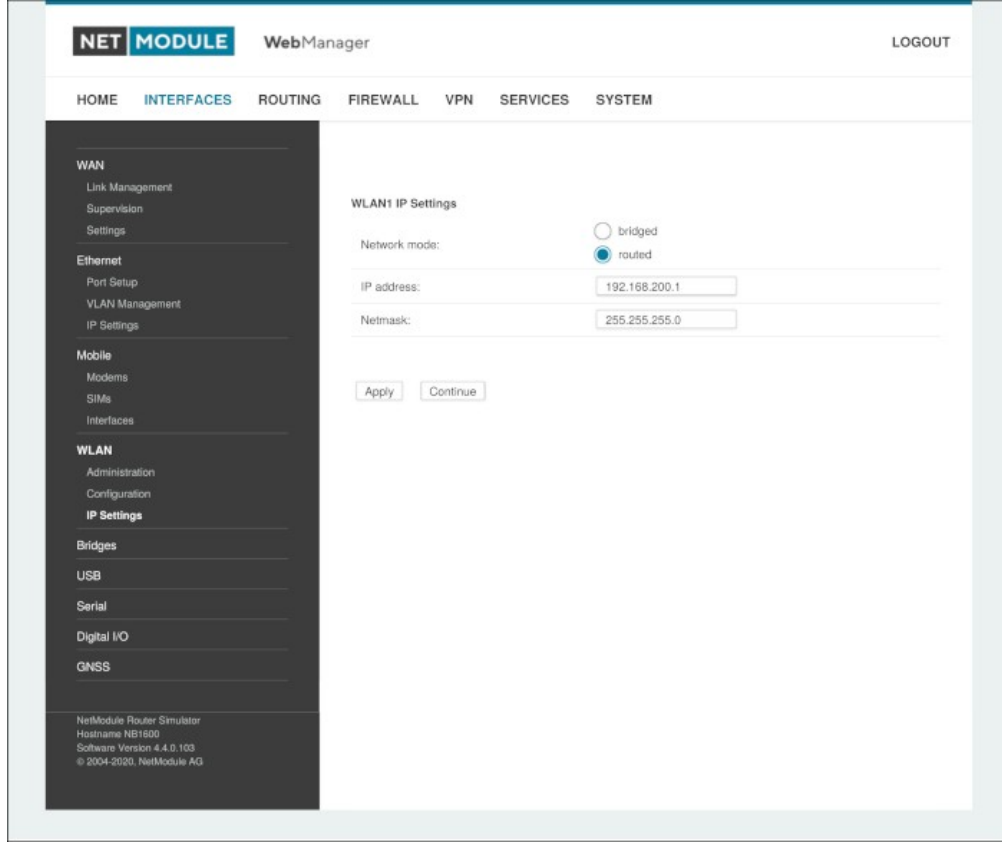
Parametre	WLAN Ağ Noktası (mesh-point) Ayarları
MESHID	Ağ adı (MESHID olarak adlandırılır)
Güvenlik modu (Security mode)	İstenilen güvenlik modu
Geçit duyurularını etkinleştir (enable gate announcements)	Örgü (mesh) ağı için geçit duyurularını etkinleştirmek için

Aşağıdaki güvenlik modları yapılandırılabilir:

Parametre	WLAN Ağ Noktası (mesh-point) Güvenlik Ayarları
Kapalı (Off)	MESHID devre dışı bırakıldı
Hiçbiri (None)	Kimlik doğrulaması yok, açık bir ağ sağlıyor
SAE	SAE (Simultaneous Authentication of Equals, Eşitlerin Eş Zamanlı Kimlik Doğrulaması), güvenli bir parola tabanlı kimlik doğrulama ve anahtar oluşturma protokolüdür

WLAN IP Ayarları

Bu bölüm WLAN ağınızın TCP/IP ayarlarını yapılandırmanızı sağlar. Bir istemci (client) ve ağ noktası (mesh point) arayüzü DHCP üzerinden veya statik olarak yapılandırılmış bir adres ve varsayılan ağ geçidiyle çalıştırılabilir.



Ekran 6.19.: WLAN IP Yapılandırma

Erişim noktası ağları, WLAN istemcilerinin ve Ethernet ana bilgisayarlarının aynı alt ağda çalışmasına izin vermek için herhangi bir LAN arabirimine köprülenebilir. Ancak, birden fazla SSID için, arabirimler arasında istenmeyen erişimi ve trafiği önlemek amacıyla yönlendirme modunda ayrı arabirimler kurmanızı şiddetle öneririz. Her ağ için karşılık gelen DHCP sunucusu, 6.7.2. bölümde açıklandığı gibi daha sonra yapılandırılabilir.

Parametre	WLAN IP Ayarları
Ağ modu (Network mode)	Arayüzün köprülenmiş mi yoksa yönlendirme modunda mı çalıştırılacağını seçin
Köprü arayüzü (Bridge interface)	Köprülenmişse, WLAN ağının köprülenmesi gereken LAN arabirimi
IP adresi / ağ maskesi (IP address / netmask)	Yönlendirme modunda, bu WLAN ağının IP adresi ve ağ maskesi



WLAN arayüzü köprülenirse aşağıdaki özellik yapılandırılabilir.

Parametre	WLAN Köprüleme Özellikleri
4addr frame	4 adresli çerçeve biçimini etkinleştirir (köprü bağlantıları için gereklidir)
IAPP	Inter-Erişim Noktası (Inter-Access Point) Protokolü özelliğini etkinleştirir
Pre-auth	Gezgin istemciler için ön kimlik doğrulama mekanizmasını etkinleştirir (istemci tarafından destekleniyorsa). Ön kimlik doğrulama yalnızca CCMP'li WPA2-Enterprise ile desteklenir
Hızlı geçiş (Fast transition)	Gezici istemci için hızlı geçiş (FT) yeteneklerini etkinleştirin (istemci tarafından destekleniyorsa)

Aşağıdaki hızlı geçiş parametreleri yapılandırılabilir

Parametre	WLAN Köprüleme Özellikleri
Hareketlilik alanı (Mobility domain)	FT ağının hareketlilik alanı
Önceden Paylaşılan Anahtar (Preshared key)	FT ağı için PSK
Yalnızca hızlı geçiş müşterileri (Fast transition clients only)	Etkinleştirilirse, AP yalnızca FT'yi destekleyen istemcileri kabul eder



6.3.5. Yazılım Köprüleri (Software Bridges)

Yazılım köprüleri, fiziksel bir LAN arayüzüne ihtiyaç duymadan OpenVPN TAP, GRE veya WLAN arayüzleri gibi katman-2 aygıtlarını köprülemek için kullanılabilir.

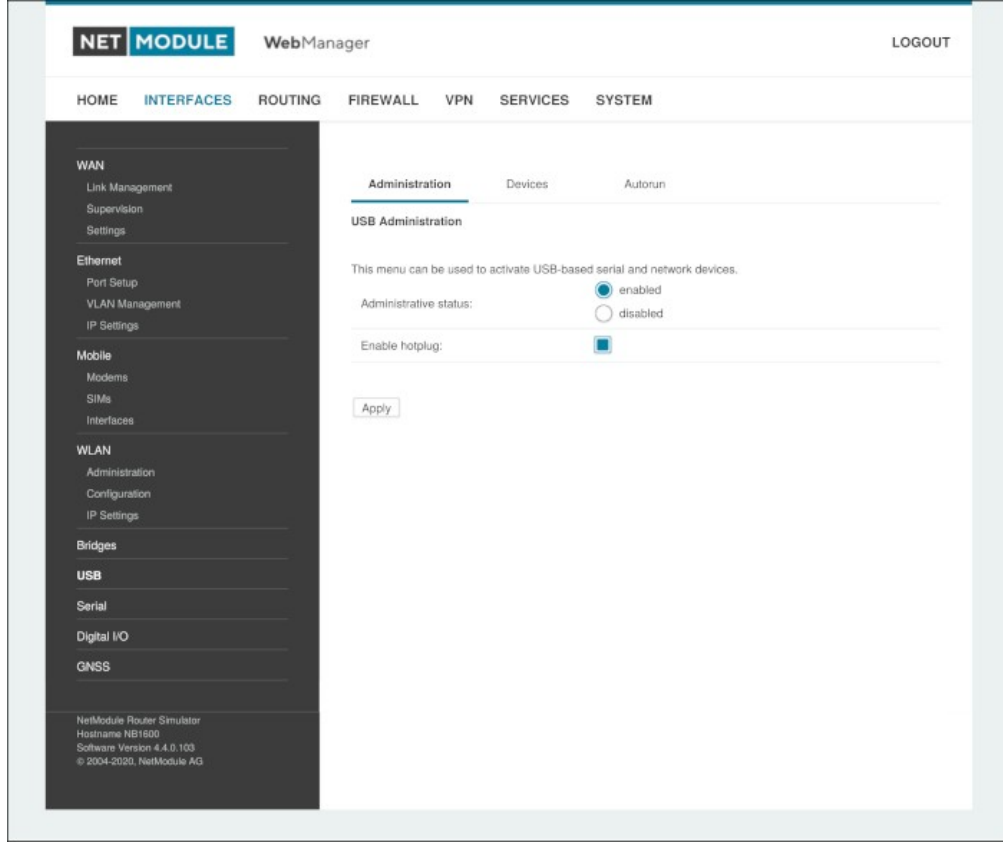
Köprü Ayarları

Bu sayfa yazılım köprülerini etkinleştirmek/devre dışı bırakmak için kullanılabilir. Aşağıdaki gibi yapılandırılabilir:

Parametre	Köprü Ayarları
Yönetimsel durum (Administrative status)	Köprü arayüzünü etkinleştirir veya devre dışı bırakır. Yerel sisteme bir arayüze ihtiyacınız varsa yerel cihaz için bir IP adresi tanımlamanız gerekir.
IP Address (IP Adresi)	Yerel arayüzün IP adresi (yalnızca "Yerel arayüzle etkinleştirildi" seçiliyse kullanılabilir)
Ağ maskesi (Netmask)	Yerel arayüzün ağ maskesi (yalnızca "Yerel arayüzle etkinleştirildi" seçiliyse kullanılabilir)
MTU	Yerel arayüz için isteğe bağlı MTU boyutu (yalnızca "Yerel arayüzle etkinleştirildi" seçiliyse kullanılabilir)

6.3.6. USB

NetModule AG yönlendiricileri, bir depolama, ağ veya seri USB aygıtı bağlamak için kullanılabilen standart bir USB ana bilgisayar bağlantı noktasıyla birlikte gelir. Desteklenen aygıtların bir listesini almak için lütfen destek ekibimize iletişime geçin.



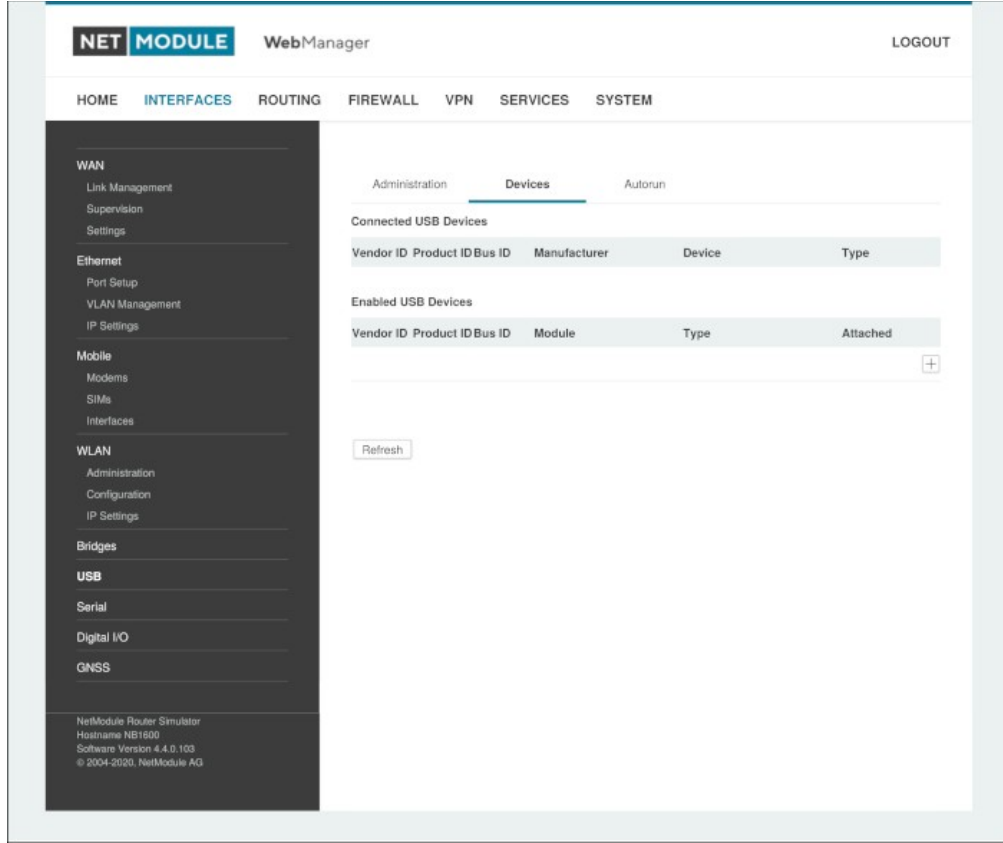
Ekran 6.20.: USB Yönetimi

USB Yönetimi

Parametre	USB Yönetimi
Yönetimsel durum (Administrative status)	Cihazların tanınıp tanınmayacağını belirtir
Hotplug'ı etkinleştir (Enable hotplug)	Aygıtın çalışma zamanı sırasında mı yoksa yalnızca önyükleme sırasında mı takıldığında tanınacağını belirtir

USB Aygıtlar

Bu sayfa şu anda bağlı olan cihazları gösterir ve Satıcı ve Ürün Kimliğine göre belirli bir cihazı etkinleştirmek için kullanılabilir. Yalnızca etkinleştirilen cihazlar sistem tarafından tanınacak ve ek portlar ve arayüzler oluşturulacaktır.



Ekran 6.21.: USB Aygıt Yönetimi

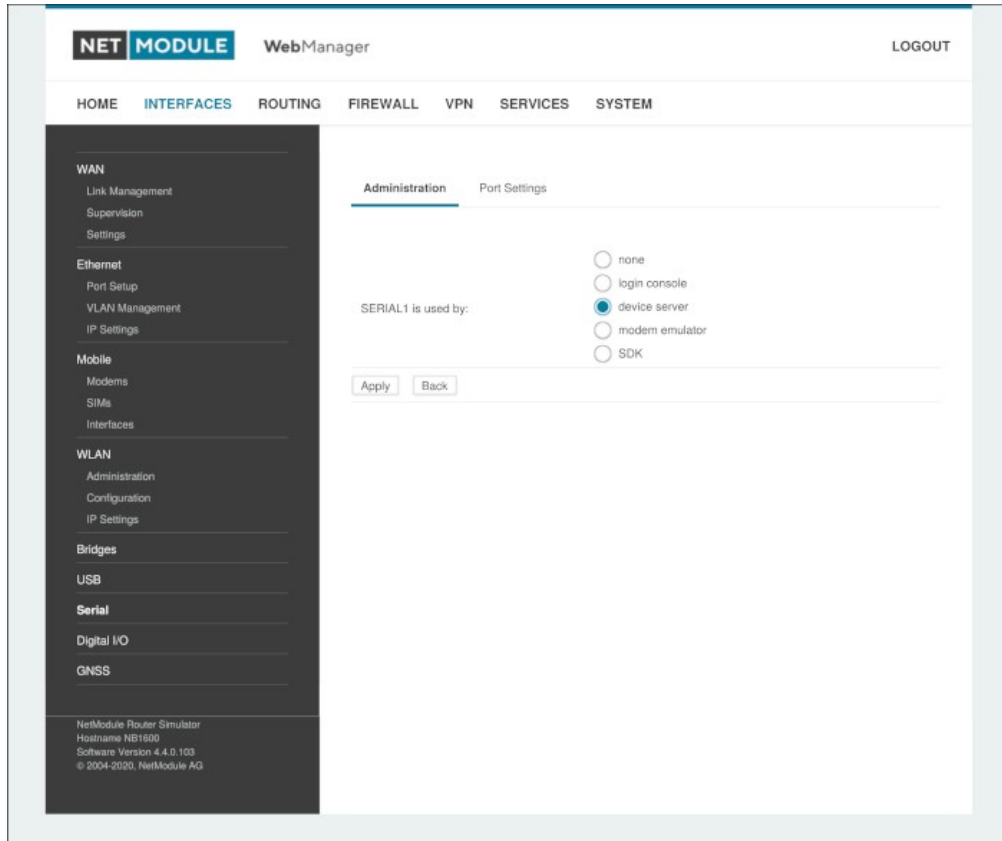
Parametre	USB Aygıtlar
Üretici kimliği (Vendor ID)	Aygıtın USB üretici kimliği
Ürün kimliği (Product ID)	Aygıtın USB ürün kimliği
Modül (Module)	Bu cihaz için uygulanacak USB modülü ve sürücü türü

Herhangi bir kimlik onaltılık gösterimde belirtilmelidir, joker karakterler desteklenir (örn. AB[0-1][2-3] veya AB*) Bir USB ağ aygıtı LAN10 olarak referans alınacaktır.

6.3.7. Seri Haberleşme

Bu sayfa seri portlarımızı yönetmek için kullanılabilir. Bir seri port şunlar tarafından kullanılabilir:

Parametre	Seri Port Kullanımı
Hiçbiri (none)	Seri port kullanılmıyor
Oturum açma konsolu (login console)	Seri port, seri terminal istemcisiyle erişilebilen bir konsolu açmak için kullanılır. Yararlı cihaz başlatma ve çekirdek mesajlarının görüntülenmesini sağlar ve kullanıcıların sisteme giriş yapabilmesi için bir oturum açma kabuğu oluşturur. Birden fazla seri arayüz mevcutsa, bir seri arayüz aynı anda 'oturum açma konsolu' olarak yapılandırılabilir.
Aygıt sunucu (device server)	Seri port bir TCP/IP portu üzerinden açığa çıkarılarak bir Seri/IP ağ geçidini uygulamak için kullanılabilir.
Modem köprüsü (modem bridge)	Entegre WWAN modeminin TTY'sine seri arayüzü köprüler.
Modem emülatörü (modem emulator)	Seri arayüzde klasik bir AT komut odaklı modemi taklit eder. Ayrıntılı bilgi için http://wiki.netmodule.com/app-notes/hayes-modem-at-simulator adresine bakın.
SDK	Seri bağlantı noktası SDK komut dosyaları için ayrılacaktır.



Ekran 6.22.: Seri Port Yönetimi

Bir aygıt sunucusu olarak çalıştırıldığında aşağıdaki ayarlar uygulanabilir:

NET MODULE WebManager LOGOUT

HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM

WAN
Link Management
Supervision
Settings

Ethernet
Port Setup
VLAN Management
IP Settings

Mobile
Modems
SIMs
Interfaces

WLAN
Administration
Configuration
IP Settings

Bridges

USB

Serial

Digital I/O

GNSS

Administration Port Settings

SERIAL1 Port Settings

Physical protocol: RS232

Baud rate: 115200

Data bits: 8 data bits

Parity: None

Stop bits: 1 stop bit

Software flow control: None

Hardware flow control: None

Server Configuration

Protocol on IP port: Telnet

Port: 2000

Timeout: endless numbered 600

Allow remote control (RFC 2217):

Show banner:

Allow clients from: everywhere specify

Apply

NetModule Router Simulator
Hostname: NB1500
Software Version: 4.4.0.103
© 2004-2020, NetModule AG

Ekran 6.23.: Seri Port Ayarları

Parametre	Seri Port Ayarları
Fiziksel protokol (Physical protocol)	Seri portta istenilen fiziksel protokolü seçer
Bağlantı hızı (Baud rate)	Seri portta çalıştırılan bağlantı hızını belirtir
Veri bitleri (Data bits)	Her çerçevede bulunan veri bitlerinin sayısını belirtir
Parite (Parity)	İletilen veya alınan her çerçeve için kullanılan pariteyi belirtir
Durdurma bitleri (Stop bits)	Bir çerçevenin sonunu belirtmek için kullanılan durdurma bitlerinin sayısını belirtir
Yazılım akış kontrolü (Software flow control)	Seri port için yazılım akış kontrolünü tanımlar, XOFF bir durdurma karakteri, XON ise gelen herhangi bir verinin hızını kontrol etmek için diğer uca bir başlatma karakteri gönderecektir.
Donanım akış kontrolü (Hardware flow control)	RTS/CTS donanım akış denetimini etkinleştirebilirsiniz, böylece RTS ve CTS hatları veri akışını denetlemek için kullanılır
TCP/IP'deki protokol (Protocol on TCP/IP)	Cihaz sunucusu için Telnet veya TCP ham IP protokollerini seçebilirsiniz
Port	Aygıt sunucusu için TCP bağlantı noktası
Zaman aşımı (Timeout)	Bir istemcinin bağlantısı kesilene kadar geçen zaman aşımı



Parametre	Sunucu Ayarları
IP portundaki protokol (Protocol on IP port)	İstenilen IP protokolünü (TCP veya Telnet) seçer
Port	Sunucunun kullanılabilir olacağı TCP portunu belirtir
Zaman aşımı (timeout)	Port üzerinde herhangi bir etkinlik yoksa, portun bağlantısının kesilmesinden önceki saniye cinsinden süre. Sıfır değeri bu işlevi devre dışı bırakır.
Uzaktan kontrole izin ver (Allow remote control)	Seri portun uzaktan kontrolüne izin ver (RFC 2217'ye göre)
Afişi göster (Show banner)	İstemciler bağlandığında bir afiş göster
Durdurma bitleri (Stop bits)	Bir çerçevenin sonunu belirtmek için kullanılan durdurma bitlerinin sayısını belirtir
İstemcilere izin ver (Allow clients from)	Sunucuya hangi istemcilerin bağlanmasına izin verildiğini belirtir

Lütfen cihaz sunucusunun kimlik doğrulama veya şifreleme sağlamadığını ve istemcilerin her yerden bağlanabileceğini unutmayın. Lütfen sınırlı bir ağ/ana bilgisayara erişimi kısıtlamayı veya güvenlik duvarını kullanarak paketleri engellemeyi düşünün.

Seri portu AT modem emülatörü olarak çalıştırırken aşağıdaki ayarlar uygulanabilir:

Parametre	Seri Port Ayarları
Fiziksel protokol (Physical protocol)	Seri portta istenilen fiziksel protokolü seçer
Bağlantı hızı (Baud rate)	Seri portta çalıştırılan bağlantı hızını belirtir
Donanım akış kontrolü (Hardware flow control)	RTS/CTS donanım akış denetimini etkinleştirebilirsiniz, böylece RTS ve CTS hatları veri akışını denetlemek için kullanılır

Parametre	Telnet Üzerinden Gelen Bağlantılar
Port	Aygıt sunucusunun TCP portu

Parametre	Telefon Rehberi Girişleri
Numara (Number)	Takma ad alacak telefon numarası
IP adresi (IP address)	Numaranın alacağı IP adresi
Port	IP adresinin portu

6.3.8. Ses (Audio)

Ses Yönetimi

Bu sayfa ses modülünü önceden yapılandırmak için kullanılabilir. Daha sonra ses ağ geçidi için kullanılabilir. Aşağıdaki şekilde yapılandırılabilir:

Parametre	Ses Ayarları
Ses seviyesi (Volume level)	Hat çıkışı için varsayılan ses seviyesi

Ses Testi

Bu sayfa bir ses örneğini oynatmak veya kaydetmek için kullanılabilir. Oynatma testi için 2 kanallı, 44100 hz, 16 bit wav dosyası yüklenebilir.

6.3.9. GNSS

Yapılandırma

GNSS sayfası, sistemde bulunan GNSS modüllerini etkinleştirmenize veya devre dışı bırakmanıza olanak tanır ve alıcılara erişimi çekişme veya veri kaybı olmadan paylaşmak ve GNSS cihazı tarafından doğrudan yayılan NMEA 0183'ten önemli ölçüde daha kolay ayrıştırılabilen bir formatla sorgulara yanıt vermek için kullanılabilen daemon'u yapılandırmak için kullanılabilir. Şu anda yeni JSON formatını destekleyen Berlios GPS daemon'unu (sürüm 3.15) çalıştırıyoruz. Herhangi bir istemciyi daemon'a uzaktan nasıl bağlayacağınız hakkında daha fazla bilgi edinmek için lütfen <http://www.catb.org/gpsd/> adresine gidin. Konum değerleri ayrıca CLI tarafından sorgulanabilir ve SDK betiklerinde kullanılabilir.

Parametre	GNSS Modül Yapılandırma
Yönetimsel durum (Administrative status)	GNSS modülünü etkinleştirin veya devre dışı bırakın
Çalıştırma modu (Operation mode)	Çalışma şekli, bağımsız veya destekli (A-GPS için)
Anten tipi (Antenna type)	Bağlı GPS antenin türü, pasif veya aktif 3 Volt güçle çalışan
Doğruluk (Accuracy)	GNSS alıcısı, uydu bilgilerine dayalı hesaplanan konum doğruluğunu karşılaştırır ve bunu metre cinsinden bu doğruluk eşiğiyle karşılaştırır. Hesaplanan konum doğruluğu doğruluk eşiğinden daha iyiyse, konum bildirilir. GNSS alıcısı bir konum düzeltmesi bildirmezse veya bir düzeltmeyi hesaplamak uzun zaman alırsa, bu parametreyi daha yüksek bir eşiğe ayarlayın. Bu, GNSS antenin net bir gökyüzü görünümü olmadığı, yani tünellerde, yüksek binaların, ağaçların yanında vb. meydana gelebilir.
Sabitleme çerçeve aralığı (Fix frame interval)	Sabitleme girişimleri arasındaki beklenmesi gereken süre

GNSS modülü AssistNow'ı destekliyorsa ve çalışma modu destekliyse aşağıdaki yapılandırma yapılabilir:

Parametre	GNSS Destekli GPS Yapılandırması
Birincil URL (Primary URL)	Birincil AssistNow URL'si
İkincil URL (Secondary URL)	İkincil AssistNow URL'si



AssistNow hakkında bilgi:

- AssistNow hizmetini kullanan çok sayıda cihazınız varsa, lütfen <http://www.u-blox.com> adresinden kendi AssistNow token'inizi oluşturmayı düşünün. Zaman başına çok fazla istek varsa, hizmet beklendiği gibi çalışmayabilir. Başka sorularınız varsa lütfen destek ekibimize iletişime geçin.

Parametre	GNSS Sunucu Yapılandırması
Sunucu portu (Server port)	Daemon'un gelen bağlantıları dinlediği TCP portu
İzinli istemciler (Allow clients from)	İstemcilerin nereden bağlanabileceğini belirtir, her yerden veya belirli bir ağdan olabilir
İstemci başlama modu (Clients start mode)	Bir istemci bağlandığında veri aktarımının nasıl gerçekleştirileceğini belirtir. Genellikle bir R gönderilmesini gerektiren isteği belirtebilirsiniz. Veriler, NMEA çerçeveleri sağlayacak ham mod veya GPS alıcısının orijinal verilerini içeren süper ham mod durumunda anında gönderilecektir. İstemci JSON formatını destekliyorsa (yani daha yeni libgps kullanılıyorsa) json modu belirtilebilir.

Lütfen özel bir istemci ağı belirleyerek veya bir güvenlik duvarı kuralı kullanarak sunucu portuna erişimi kısıtlamayı düşünün.

**Dead Reckoning hakkında bilgi:**

- Dead Reckoning'i destekleyen bir cihazınız varsa, daha fazla bilgi için lütfen GNSS Dead Reckoning kurulum kılavuzuna bakın veya destek ekibimize iletişime geçin.

Konum

Bu sayfa, görüntüdeki uydular ve bunlardan elde edilen değerler hakkında daha fazla bilgi sağlar:

Parametre	GNSS Bilgisi
Enlem (Latitude)	Kuzey-güney konumunu belirten coğrafi koordinat
Boylam (Longitude)	Doğu-batı konumunu belirten coğrafi koordinat
Yükseklik (Altitude)	Mevcut konumun deniz seviyesinden yüksekliği
Görüntülenen uydular (Satellites in view)	GPGSV çerçevelerinde belirtildiği gibi görüntüdeki uydu sayısı
Hız (Speed)	GPRMC çerçevelerinde belirtildiği gibi yatay ve dikey hız, saniye başına metre cinsinden
Kullanılan uydular (Satellites used)	GPGGA çerçevelerinde belirtildiği gibi konumu hesaplamak için kullanılan uydu sayısı
Keskinliğin seyreltilmesi (Dilution of precision)	GPGSA çerçevelerinde belirtilen hassasiyetin seyreltilmesi



Ayrıca her uydunun şu detayları da bulunuyor:

Parametre	GNSS Uydu Bilgisi
PRN	GPGGA çerçevelerinde belirtilen uydunun PRN kodu (uydu kimliği olarak da bilinir)
Yükseklik (Elevation)	GPGSV çerçevelerinde belirtildiği gibi yükseklik (çanak işaret yönü arasındaki yukarı-aşağı açısı) derece cinsinden
Azimuth	GPGSV çerçevelerinde belirtildiği gibi derece cinsinden azimut (dikey eksen etrafındaki dönüş)
SNR	SNR (Sinyal Gürültü Oranı), genellikle sinyal gücü olarak adlandırılır

Denetim

Parametre	GNSS Denetim
Yönetimsel durum (Administrative status)	GNSS denetimini etkinleştirin veya devre dışı bırakın
Mod (Mode)	NMEA akışının mı yoksa GPS düzeltmelerinin mi izleneceğini belirtir
Azami kesinti süresi (Max. downtime)	Acil bir eylemin gerçekleştirileceği geçerli NMEA akışı veya GPS tespiti olmadan geçen zaman dilimi
Acil eylem (Emergency action)	İlgili acil durum eylemi. Sunucuyu yeniden başlatmaya izin verebilirsiniz, bu da modüldeki GPS işlevini yeniden başlatacaktır, veya ciddi durumlarda modülü sıfırlayabilirsiniz. Lütfen bunun çalışan herhangi bir WWAN/SMS hizmeti üzerinde etkileri olabileceğini unutmayın.

6.4. YÖNLENDİRME (ROUTING)

6.4.1. Statik Rotalar

Bu menü sistemin tüm yönlendirme girişlerini gösterir. Bunlar genellikle bir paketin hedefini belirten bir adres/ağ maskesi çifti (IPv4 noktalı ondalık gösteriminde gösterilir) tarafından oluşturulur. Paketler bir ağ geçidine veya bir arayüze veya her ikisine birden yönlendirilebilir. Arayüz HERHANGİ BİRİ (ANY) olarak ayarlanırsa, sistem bir arayüz için yapılandırılmış en iyi eşleşen ağa bağlı olarak rota arayüzünü otomatik olarak seçer.

NET MODULE WebManager LOGOUT

HOME INTERFACES **ROUTING** FIREWALL VPN SERVICES SYSTEM

Static Routes

Extended Routes

Multipath Routes

Multicast

IGMP Proxy

Static Routes

BGP

OSPF

Mobile IP

Administration

QoS

Administration

Classification

NetModule Router Simulator
Hostname NB1600
Software Version 4.4.0.103
© 2004-2020, NetModule AG

Static Routes

This menu shows all routing entries of the system, they can consist of active and configured ones. The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route (Netmasks can be specified in CIDR notation)

Destination	Netmask	Gateway	Interface	Metric	Flags
192.168.1.0	255.255.255.0	0.0.0.0	LAN1	0	AN
192.168.101.0	255.255.255.0	0.0.0.0	LAN1-1	0	AN
192.168.102.0	255.255.255.0	0.0.0.0	LAN1-2	0	AN
192.168.200.0	255.255.255.0	0.0.0.0	WLAN1	0	AN

Route lookup

Ekran 6.24.: Statik Yönlendirme

Genel olarak, ana bilgisayar rotaları ağ rotalarından önce gelir ve ağ rotaları varsayılan rotalardan önce gelir. Ek olarak, bir rotanın önceliğini belirlemek için bir ölçüm kullanılabilir, bir paket, bir hedef birden fazla rotayla eşleşirse en düşük ölçüme sahip yöne gider.

Ağ maskeleri CIDR gösteriminde belirtilebilir (yani /24, 255.255.255.0'a genişler).

Parametre	Statik Rota Yapılandırma
Variş noktası (Destination)	Bir paketin hedef adresi
Ağ maskesi (Netmask)	Hedefle birlikte adreslenecek ağı oluşturan alt ağ maskesi. Tek bir ana bilgisayar 255.255.255.255 ağ maskesiyle belirtilebilir, varsayılan rota 0.0.0.0'a karşılık gelir
Ağ geçidi (Gateway)	Bu ağ için ağ geçidi olarak çalışan bir sonraki atlama (eşler arası bağlantılarda atlanabilir)
Arayüz (Interface)	Bir paketin arkasındaki ağ geçidine veya ağa ulaşabilmesi için iletileceği ağ arabirimi
Metrik (Metric)	Arayüzün yönlendirme metriği (varsayılan 0), daha yüksek metrikler bir rotayı daha az elverişli hale getirme etkisine sahiptir
Bayraklar (Flags)	A: Aktif, P: Kalıcı, H: Ana bilgisayar, N: Ağ rotası, D: Varsayılan

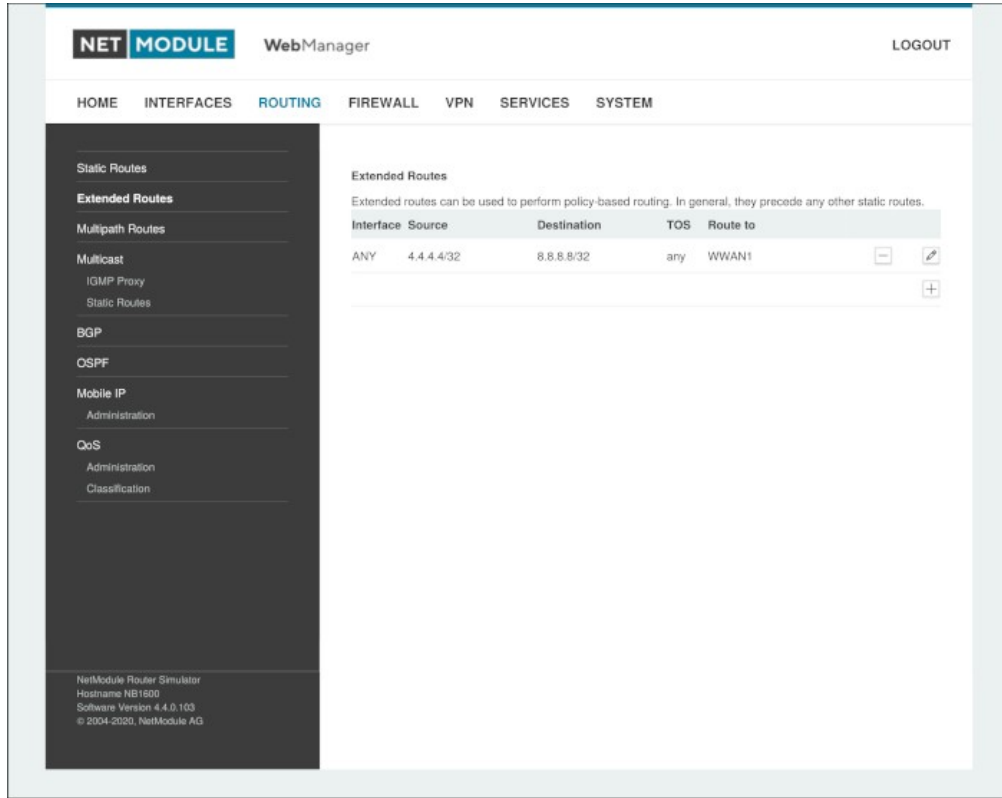
Bayraklar şu anlamları taşır:

Bayrak	Açıklama
A	Rota aktif olarak kabul edilir, bu rota için arayüz henüz hazır değilse pasif olabilir.
P	Rota kalıcıdır, yani yapılandırılmış bir rotadır, aksi takdirde bir arayüz rotasına karşılık gelir.
H	Rota bir ana bilgisayar rotasıdır, genellikle ağ maskesi 255.255.255.255 olarak ayarlanır.
N	Rota, adreslenecek alt ağı oluşturan bir adres ve ağ maskesinden oluşan bir ağ rotasıdır.
D	Rota varsayılan, adres ve ağ maskesi 0.0.0.0 olarak ayarlanmıştır, herhangi bir paketle eşleşir.

Tablo 6.53.: Statik Rota Bayrakları

6.4.2. Genişletilmiş Yönlendirme

Genişletilmiş rotalar, politika tabanlı yönlendirme gerçekleştirmek için kullanılabilir ve genellikle statik rotalardan önce gelir.



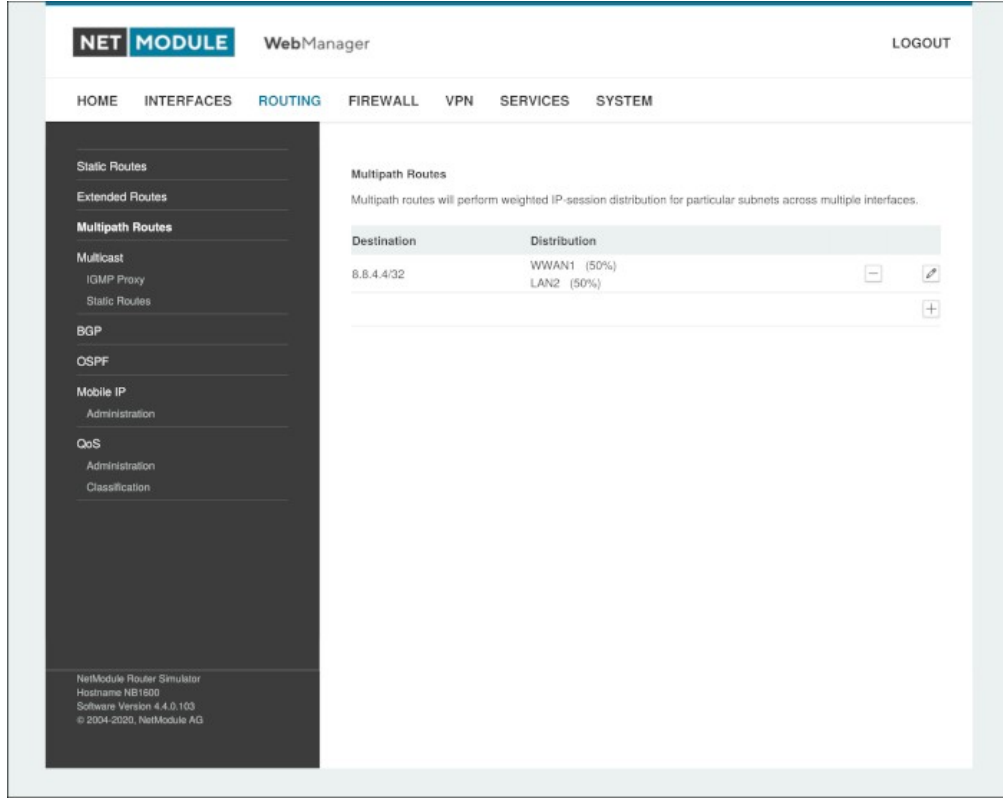
Ekran 6.25.: Genişletilmiş Yönlendirme

Statik rotaların aksine, genişletilmiş rotalar yalnızca bir hedef adres/ağ maskesinden değil, aynı zamanda bir kaynak adres/ağ maskesinden, gelen arayüzden ve paketlerin hizmet türünden (Type Of Service, TOS) oluşabilir.

Parametre	Genişletilmiş Rota Yapılandırması
Kaynak adresi (Source address)	Bir paketin kaynak adresi
Kaynak ağ maskesi (Source netmask)	Bir paketin kaynak adresi
Hedef adres (Destination address)	Bir paketin hedef adresi
Hedef ağ maskesi (Destination netmask)	Bir paketin hedef adresi
Gelen arayüz (Incoming interface)	Paketin sisteme girdiği arayüz
Servis tipi (Type of service)	Paket başlığındaki TOS değeri
Rotaya (Route to)	Paketin yönlendirileceği hedef arayüzü veya ağ geçidini belirtir
Bağlantı yoksa kes (discard if down)	Belirtilen arayüz kapalıysa paketleri atın

6.4.3. Çoklu Yol Rotaları (Multipath Routes)

Çoklu yol rotaları, birden fazla arayüzdeki belirli alt ağlar için ağırlıklı IP oturumu dağıtımını gerçekleştirir.



Ekran 6.26.: Çoklu Yol Rotaları

Çoklu yol yönlendirmesini kurmak için en az iki arayüz tanımlanmalıdır. Artı işaretine basılarak ek arayüzler eklenebilir.

Parametre	Çoklu Yol Rotası Ekle
Hedef ağ/ağ maskesi (Target network/netmask)	Çoklu yol yönlendirmesinin uygulanacağı hedef ağ tanımlar
Arayüz (Interface)	Bir yol için arayüzü seçer
Ağırlık (Weight)	Arayüzün diğerlerine göre ağırlığı
NextHop	Bu arayüzün varsayılan ağ geçidini geçersiz kılar

6.4.4. Multicast

Çoklu yayın, IP paketlerini abonelere bire-çok ilişkisinde dağıtır. Aboneler, bir MCR grubuna abone olmak ve verileri çoklu yayın paketleri biçiminde almak için çoklu yayın mesajlarını kullanır. Bu nedenle mesajlar paket alıcısı tarafından paket kaynağına gönderilir. Çoklu yayın yönlendirmesi (MultiCast Routing, MCR), çoklu yayın verilerini bir ağdan diğerine iletmek için kullanılır.

**Dikkat:**

- Çoklu yayın, aynı ağdaki birden fazla hedefe veri göndermek için kullanıldığından, paketlerin diğer ağlara yayılmasını önlemek için çoklu yayın paketlerinin TTL'sini 1 olarak ayarlamak test uygulamaları için oldukça yaygındır. Çoklu yayın paketlerini yönlendirmek istiyorsanız (bu yüzden buna MCR denir), verilerinizi TTL > 1 ile gönderdiğinizden emin olmalısınız.

Multicast yönlendirme bir arka plan programı (daemon) tarafından yapılandırılabilir ve yönetilebilir. Aynı anda yalnızca bir MCR arka plan programı kullanılabilir. NetModule AG yönlendiricileri, gereksinimlerinize bağlı olarak seçilebilecek iki farklı MCR arka plan programı ile birlikte gelir:

Parametre	Yönetimsel Durum
IGMP vekil (proxy)	Belirli bir arayüzde dinamik olarak algılanan çoklu yayın mesajlarının başka bir arayüze iletilmesi
Statik rotalar (static routes)	Belirli bir arayüzden diğerine özel kaynak ve grubun mesajlarını iletmek için MCR kurallarının listesi
Devre dışı bırakıldı (disabled)	Çoklu yayın iletilerinin yönlendirilmesini devre dışı bırak

IGMP vekil (proxy)

Belirli bir arayüzde çoklu yayın gruplarını sürdürebilen ve gelen çoklu yayın paketlerini, ana bilgisayarların gruplara katıldığı alt akış arayüzlerine dağıtabilen IGMP vekili.

Parametre	Çoklu Yayın Yönlendirme Ayarları
Gelen arayüz (Incoming interface)	Çoklu yayın gruplarının katıldığı ve çoklu yayın paketlerinin geldiği yukarı akış arabirimi
Gönderen ağ (Sender network)	Çoklu yayın kaynak ağ adresi
Gönderen ağ maskesi (Sender netmask)	Çoklu yayın kaynak ağ maskesi
Şuna dağıt (Distribute to)	Çoklu yayın paketlerinin iletileceği alt akış arayüzlerini belirtir

Statik Rotalar (Static Routes)

Belirli bir MCR kuralları kümesine göre, çoklu yayın paketlerini kökenlerine ve gruplarına bağlı olarak farklı yönlere yönlendirir:

Parametre	Çoklu Yayın Yönlendirme Ayarları
Grup (Group)	MCR grubunun IP adresi
Kaynak (Source)	Paketlerin kaynak IP'si
Gelen arayüz (Incoming interface)	Paket kaynağına arayüz
Giden arayüz (Outgoing interface)	Paketleri iletmek için arayüz



6.4.5. BGP

BGP sekmesi, NetModule AG yönlendiricisinin diğer Sınır Ağ Geçidi Protokolü etkin yönlendiricilerle eşleştirilmesini ayarlamaya olanak tanır.

Parametre	BGP Genel Ayarları
Yönetimsel durum (Administrative status)	BGP yönlendirme protokolünün etkin olup olmadığını belirtir
Yönlendirici kimliği (Router ID)	İsteğe bağlı olarak yönlendirici kimliği, 1.2.3.4 gibi noktalı bir IPv4 gösterimi biçiminde tanımlanabilir. Kimlik atlanırsa, BGP daemon geçerli bir değer belirlemeye çalışacak veya 0.0.0.0'a geri dönecektir.
AS numarası (AS number)	NetModule AG yönlendiricisinin ait olduğu otonom sistemin numarası (1-4294967295)
Bağlı rotaları yeniden dağıt (Redistribute connected routes)	NetModule AG yönlendiricisine doğrudan bağlı olan ağlara rotaları yeniden dağıtın
Yerel rotaları yeniden dağıtın (Redistribute local routes)	NetModule AG yönlendiricisinin kendi yönlendirme tablosundan rotaları yeniden dağıtın
OSPF rotalarını yeniden dağıtın (Redistribute OSPF routes)	OSPF yönlendirme protokolü aracılığıyla öğrenilen rotaları yeniden dağıtın
Yedeklilik sırasında devre dışı bırak (Disable when redundancy backup)	Yönlendirici VRRP yedeklilik protokolü tarafından köle (slave) moduna ayarlandığında BGP protokolünü devre dışı bırakır
Canlı tutma zamanlayıcısı (Keepalive timer)	Keepalive mesajının gönderilmesinin saniye cinsinden aralığı
Bekleme zamanlayıcısı (Holddown timer)	Yönlendiricinin komşunun öldüğünü varsayana kadar gelen BGP mesajlarını bekleyeceği saniye cinsinden süre

Komşular sekmesi, eşleşilecek tüm BGP yönlendiricilerini yapılandırmak için kullanılır.

Parametre	BGP Komşuları
IP adres (IP address)	Eş yönlendiricinin IP adresi
AS sayısı (AS number)	Eş yönlendiricinin otonom sistem numarası (1-4294967295)
Şifre (Password)	Eş yönlendiriciyle kimlik doğrulama için parola. Boş bırakılırsa kimlik doğrulama devre dışı bırakılır.
Multihop	Eşin doğrudan bağlı olmasını gerektirmek yerine, bu yönlendirici ile eş yönlendirici arasında birden fazla atlamaya izin verir.
Adres Ailesi (Address Family)	ipv4-unicast veya l2vpn-evpn adres ailesinin etkinleştirilip etkinleştirilmeyeceğini seçin
Ağırlık (Weight)	Bu parametre komşu rota için varsayılan ağırlığı belirtir

Ağlar sekmesi, genel sekmesinde tanımlandığı gibi diğer kaynaklardan yeniden dağıtılan ağlara ek olarak BGP üzerinden dağıtılacak IP ağ öneklerinin eklenmesine olanak tanır.

Parametre	BGP Ağları
Önek (Prefix)	Dağıtılacak ağın öneki
Önek uzunluğu (Prefix length)	Dağıtılacak önek uzunluğu

6.4.6. OSPF

OSPF menüsü, NetModule AG yönlendiricisinin bir OSPF yönlendiricileri ağına eklenmesine olanak tanır.

Parametre	OSPF Genel Ayarları
Yönetimsel durum (Administrative status)	BGP yönlendirme protokolünün etkin olup olmadığını belirtir
Yönlendirici kimliği (Router ID)	Router-id, NetModule AG yönlendiricisine özgü bir kimliktir. Router-id belirtilmezse, sistem otomatik olarak en yüksek IP adresini router-id olarak seçecektir.
Bağlı rotaları yeniden dağıt (Redistribute connected routes)	NetModule AG yönlendiricisine doğrudan bağlı olan ağlara rotaları yeniden dağıtın
Yerel rotaları yeniden dağıt (Redistribute local routes)	NetModule AG yönlendiricisinin kendi yönlendirme tablosundan rotaları yeniden dağıtın
BGP rotalarını yeniden dağıt (Redistribute BGP routes)	BGP yönlendirme protokolü aracılığıyla öğrenilen rotaları yeniden dağıtın
Varsayılan rotayı yeniden dağıt (Redistribute default route)	Yönlendiricilerin varsayılan rotasını yeniden dağıtın
Yedeklilik sırasında devre dışı bırak (Disable when redundancy backup)	Yönlendirici VRRP yedeklilik protokolü tarafından köle moduna ayarlandığında OSPF protokolünü devre dışı bırakır

Arayüzler sekmesi, yönlendiricinin IP arayüzleri için OSPF'ye özgü ayarları tanımlamak için kullanılır. Belirli bir arayüz için hiçbir ayar tanımlanmamışsa, varsayılan ayarlar kullanılacaktır.

Parametre	OSPF Arayüzleri
Arayüz (Interface)	Ayarların tanımlanacağı arayüzün adı
Kimlik doğrulama (Authentication)	OSPF paketlerini doğrulamak için arayüzde kullanılacak kimlik doğrulama protokolü
Anahtar (Key)	Kimlik doğrulama için kullanılacak anahtar
Anahtar kimliği (Key ID)	Kimlik doğrulama için kullanılacak anahtarın kimliği (1-255)
Maliyet (Cost)	Bu arayüz üzerinden paket göndermenin maliyeti. Belirtilmezse veya 0 olarak ayarlanmaz ise OSPF varsayılanları kullanılır.
Pasif (Passive)	Bu arayüzde OSPF paketleri göndermeyin

Ağlar sekmesi, OSPF'de işlenecek IP ağlarını ve bunların hangi yönlendirme alanına ait olduğunu tanımlar.

Parametre	OSPF Ağları
Önek (Prefix)	Dağıtılacak ağın öneki
Önek uzunluğu (Prefix length)	Dağıtılacak önek uzunluğu
Alan (Area)	Bu arayüzün ait olduğu yönlendirme alanı (0-65535, 0 omurga anlamına gelir)

6.4.7. Mobile IP

Mobile IP (MIP), farklı WAN bağlantıları (örneğin hücresel ağ - WWAN veya kablosuz ağ - WLAN) arasında kesintisiz geçiş yapılmasını sağlar. Bu sayede, mobil cihaz (mobil düğüm, mobile node), hangi bağlantı üzerinden internete bağlı olursa olsun, her zaman aynı IP adresi (ev adresi, home address) üzerinden erişilebilir olur. WAN bağlantısı değiştiğinde, bu geçiş sırasında sadece çok kısa süreli kesintiler yaşanır ve mevcut IP bağlantıları kopmadan çalışmaya devam eder.

NetModule AG yönlendiricileri, aynı zamanda NAT (ağ adresi çevirisi) arkasındaki mobil cihazlar için NAT-T (NAT-Traversal) desteği sunar. Bu sayede, güvenlik duvarı arkasında kalan mobil cihazlara da merkez ofisten ev adresi üzerinden erişmek mümkün olur. Böylece karmaşık VPN kurulumlarına gerek kalmaz.

Bu sistem, ev ajanı (home agent) adı verilen bir yapı sayesinde çalışır. Ev ajanı, mobil cihazla (mobile node) arasında VPN benzeri bir tünel bağlantısı kurar. Mobil cihazın bağlantı (care-of) adresi değiştiğinde, bu bilgi ev ajanına iletilir. Ev ajanı da mobil cihazın ev adresine gönderilen verileri, güncel bağlantı adresine yönlendirerek iletir.

Güvenlik duvarı ve özel IP adresleme sorunlarını önlemek için, MIP her zaman ters tünelleme (reverse tunneling) yöntemini kullanır. Yani, mobil cihazdan giden tüm trafik önce ev ajanına yönlendirilir, oradan asıl hedefe iletilir. Bu sayede MIP, hafif bir VPN alternatifi gibi çalışabilir (ancak şifreleme sağlamaz).

MIP uygulaması şu standartları destekler: RFC 3344, 5177, 3024 ve 3519. Çok sayıda mobil cihazın kullanıldığı uygulamalarda, Cisco 2900 serisi yönlendiricilerle uyumluluğu test edilmiştir. Ancak, NetModule AG yönlendiricileri hem mobil cihaz hem de ev ajanı işlevini desteklediği için, ek donanım gerekmeden 10 adede kadar mobil cihaz içeren bir MIP ağı kurulabilir.

Parametre	Mobil IP Ayarları
Birincil ev ajanı adresi (Primary home agent address)	Birincil ev ajanının adresi
İkincil ev ajanı adresi (Secondary home agent address)	İkincil ana ajanın adresi. Mobil düğüm, birincil ana ajana ulaşamıyorsa bu ana ajana kaydolmaya çalışacaktır.
Ev adresi (Home address)	Mobil yönlendiriciye her an ulaşılabilmesini sağlayan mobil düğümün kalıcı ev adresi.
SPI	Mobil düğüm ile ana aracı arasındaki mobil IP tüneli için güvenlik bağlamını tanımlayan Güvenlik Parametresi Endeksi (SPI). Bu, mobil düğümleri birbirinden ayırt etmek için kullanılır. Bu nedenle her mobil düğüme benzersiz bir SPI atanması gerekir. Bu, 32 bitlik onaltılık bir değerdir.
Kimlik doğrulama tipi (Authentication type)	Kullanılan kimlik doğrulama algoritması. Bu prefix-suffix-md5 (MIP için varsayılan) veya hmac-md5 olabilir.
Paylaşılan sır (Shared secret)	Mobil düğümün ev aracısında kimlik doğrulaması için kullanılan paylaşılan sır. Bu, 128 bitlik bir onaltılık değer veya rastgele uzunlukta bir ASCII dizesi olabilir.
Yaşam süresi (Life time)	Güvenlik ilişkilerinin ömrü saniyeler mertebesinde.
MTU	Bayt cinsinden maksimum iletim birimi, varsayılan değer 1468'dir.
UDP kapsülleme (UDP encapsulation)	UDP kapsüllemesinin kullanılıp kullanılmayacağını belirtir. NAT geçişine izin vermek için UDP kapsüllemesi etkinleştirilmelidir.
Mobil ağ adresi (Mobile network)	İsteğe bağlı olarak mobil düğüme yönlendirilmesi gereken bir alt ağ

address)	belirtir. Bu bilgi, Ağ Hareketliliği (NEMO) uzantıları aracılığıyla ana aracıya iletilir. Ana aracı daha sonra mobil düğüm aracılığıyla alt ağa otomatik olarak IP rotaları ekleyebilir. Bu özelliğin tüm üçüncü taraf ana aracı uygulamaları tarafından desteklenmediğini unutmayın.
Mobil ağ maskesi (Mobile network mask)	İsteğe bağlı yönlendirilen ağ için ağ maskesi.

MIP bir ana ajan olarak çalıştırılırsa, öncelikle ana ajan için bir ana adres ve ağ maskesi ayarlamamız gerekecektir. Daha sonra aşağıdaki ayarlardan oluşan tüm mobil düğümler için yapılandırmayı eklemeniz gerekecektir:

Ekran 6.27.: Mobile IP

Parametre	Yapılandırma ana aracı
Ev ağı adresi (Home network address)	Ev ağı adresi
Ev ağı maskesi (Home network mask)	Ev ağı maskesi

6.4.8. Quality Of Service (Servis Kalitesi)

NetModule AG yönlendiricileri belirli IP trafiği türlerini önceliklendirebilir ve şekillendirebilir. Bu şu anda çıkışla sınırlıdır, yani yalnızca giden trafik belirlenebilir. Mevcut QoS çözümü, Stokastik Adalet Kuyruğu (SFQ) sınıflarını Hiyerarşi Token Kovası (HTB) qdiscs ile birlikte kullanır. Çalışma prensibi, bağlantı başına maksimum verimi sınırlamak ve trafiği belirtilen kuyruk önceliklerini yansıtarak şekillendirmek olarak özetlenebilir. Genel olarak, bir kuyruğun en düşük öncelik numarası mevcut bant genişliğinden en iyi şekilde yararlanır. Diğer sınıf veya qdisc algoritmalarına yönelik talepler olması durumunda, uygulamanız için en iyi yaklaşımı değerlendirmek üzere lütfen destek ekibimize iletişime geçin.

QoS Yönetimi

Yönetim sayfası QoS'u etkinleştirmek ve devre dışı bırakmak için kullanılabilir.

QoS Sınıflandırması

Sınıflandırma bölümü QoS'un etkin olması gereken WAN arayüzlerini tanımlamak için kullanılabilir.

Parametre	QoS Arayüz Ayarları
Arayüz (Interface)	QoS'un etkin olması gereken WAN arayüzü
Bant genişliği tıkanıklığı (Bandwidth congestion)	Bant genişliği tıkanıklığı yöntemi. Otomatik olması durumunda sistem sınırları en iyi şekilde uygulamaya çalışacaktır. Ancak, QoS davranışını ayarlamamanın bir yolunu sundukları için sabit bant genişliği sınırları belirlemek önerilir.
İndirme bant genişliği (Downstream bandwidth)	Gelen trafik için kullanılabilir bant genişliği
Yükleme bant genişliği (Upstream bandwidth)	Giden trafik için kullanılabilir bant genişliği
IP'den ping'e -birincil (IP to ping -primary)	Bağlantının bant genişliğini belirlemek için ICMP yankı isteklerine yanıt veren bir IP
IP'den ping'e -ikincil (IP to ping -secondary)	Bağlantının bant genişliğini belirlemek için ICMP yankı isteklerine yanıt veren bir IP

Sınırları tanımlarken, en azından mümkün olan bant genişliği sınırlarını göz önünde bulundurmalısınız çünkü belirtilen sınırlara ulaşılamazsa çoğu şekillendirme ve kuyruk algoritması doğru şekilde çalışmayacaktır. Özellikle, mobil bir ortamda çalışan herhangi bir WWAN arayüzü değişken bant genişliklerinden muzdariptir, bu nedenle daha düşük değerler kullanılmalıdır.

Bir arayüz aktif hale getirildiğinde sistem otomatik olarak aşağıdaki kuyrukları oluşturacaktır:

Parametre	QoS Varsayılan Kuyrukları
Yüksek (high)	Herhangi bir gecikme açısından kritik hizmeti (VoIP gibi) barındırabilen yüksek öncelikli bir kuyruk
Varsayılan (default)	Diğer tüm hizmetleri işleyecek varsayılan bir kuyruk
Düşük (low)	Şekillendirmenin amaçlandığı daha az kritik hizmetleri barındırabilen düşük öncelikli bir kuyruk



Her kuyruk aşağıdaki şekilde yapılandırılabilir:

Parametre	QoS Kuyruk Parametreleri
Ad (Name)	QoS kuyruğunun adı
Öncelik (Priority)	Sıra için sayısal bir öncelik, daha düşük değerler daha yüksek öncelikleri gösterir
Bant genişliği (Bandwidth)	Tüm kuyrukların toplam bant genişliği "QoS Arayüz Parametreleri"nin ayarlanmış yukarı akış bant genişliğini aşarsa bu kuyruk için mümkün olan maksimum bant genişliği
TOS'u belirle (Set TOS)	Eşleşen paketlerde ayarlanacak TOS/DiffServ değeri

Artık her kuyruğa herhangi bir hizmeti yapılandırabilir ve atayabilirsiniz. Aşağıdaki parametreler geçerlidir:

Parametre	QoS Servis Parametreleri
Arayüz (Interface)	Kuyruğun QoS arayüzü
Kuyruk (Queue)	Bu hizmetin atanacağı QoS kuyruğu
Kaynak (Source)	Paketlerin kaynak adresiyle eşleşmek için kullanılan bir ağ adresi ve ağ maskesini belirtir
Hedef (Destination)	Paketlerin hedef (hedef) adresini eşleştirmek için kullanılan bir ağ adresi ve ağ maskesi belirtir
Protokol (Protocol)	Paketlerin eşleştirileceği protokolü belirtir
Kaynak port (Destination Port)	Paketlerin eşleştirileceği kaynak portunu belirtir
Hedef port (Destination Port)	Paketlerin eşleştirileceği kaynak bağlantı noktasını belirtir
Servis tipi (Type of Service)	Eşleştirilecek paketler için TOS/DiffServ'i belirtir

6.5. GÜVENLİK DUVARI (FIREWALL)

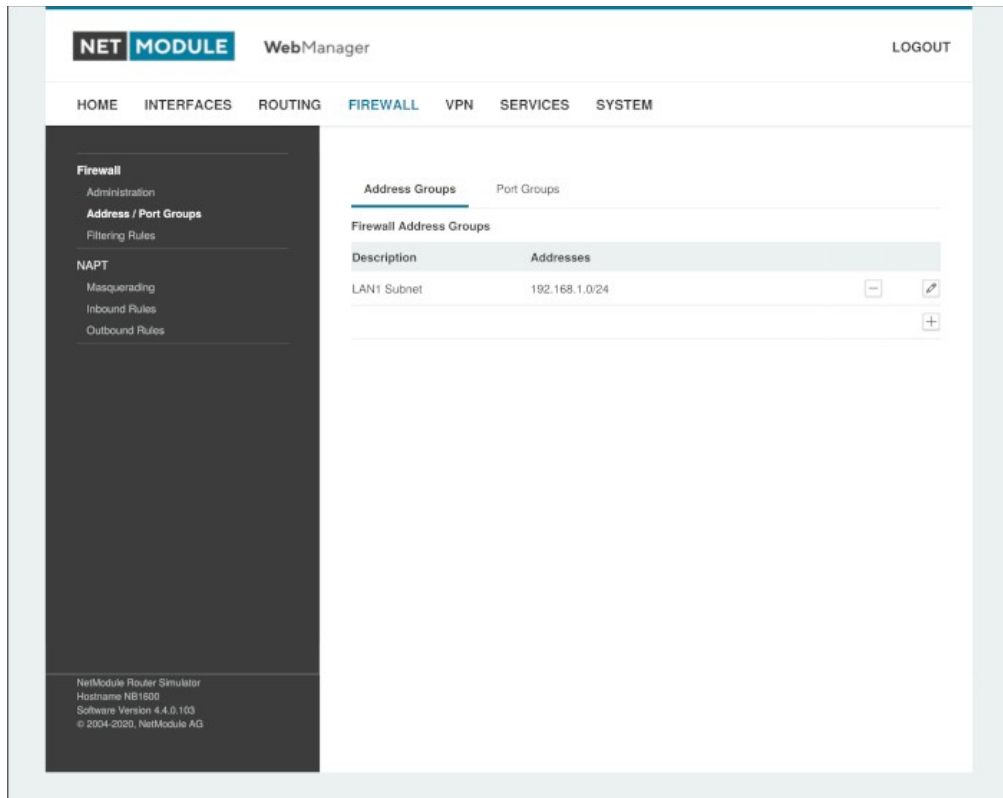
6.5.1. Yönetim

NetModule AG yönlendiricileri, durum denetimini destekleyen Linux'un netfilter/iptables güvenlik duvarı çerçevesini kullanır (daha fazla bilgi için <http://www.netfilter.org> adresine bakın) yani bir IP oturumu içindeki devralınan bağlantılar için aynı izinleri verir (örneğin, bir kontrol ve veri bağlantısı oluşturan FTP).

Yönetim sayfası güvenlik duvarını etkinleştirmek ve devre dışı bırakmak için kullanılabilir. Açıldığında, varsayılan olarak yönetime (HTTP, HTTPS, SSH veya TELNET üzerinden) izin veren ancak WAN arayüzünden gelen diğer paketleri engelleyen önceden tanımlanmış bir kural kümesi oluşturmak için bir kısayol kullanılabilir.

6.5.2. Adres/Port Grupları

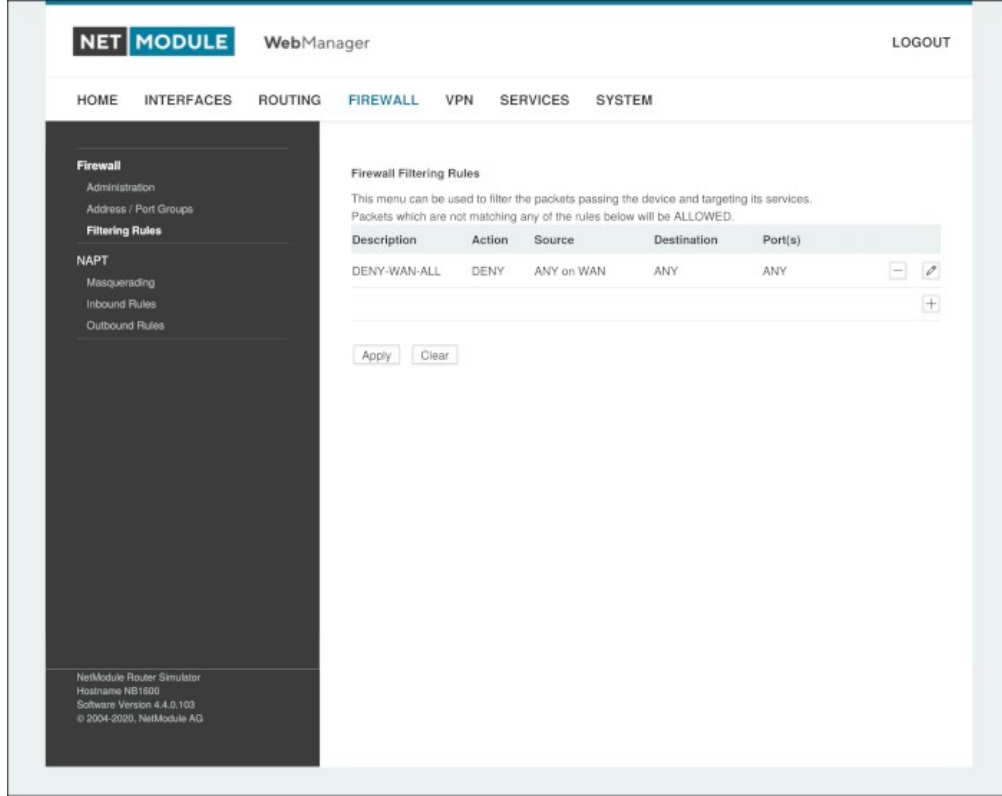
Bu menü, kural sayısını azaltmak için daha sonra güvenlik duvarı kuralları için kullanılacak adres veya bağlantı noktası grupları oluşturmak için kullanılabilir. Adres veya bağlantı noktası gruplarına başvurulduysa, yapılandırılmış varlıklardan biri pakete uygulanırsa paketler eşleşecektir.



Ekran 6.28.: Güvenlik Duvarı Grupları

6.5.3. Kurallar

Genel olarak, güvenlik duvarı her paketin yönlendiriciyi geçme iznini kontrol eden bir dizi kuraldan oluşur. Lütfen kuralların sırayla işlendiğini unutmayın, yani eşleşen bir kural bulunana kadar listenin en üstten en alta doğru taranması anlamına gelir. Yapılandırılan kurallardan hiçbirine uymayan paketlere İZİN VERİLECEKTİR.



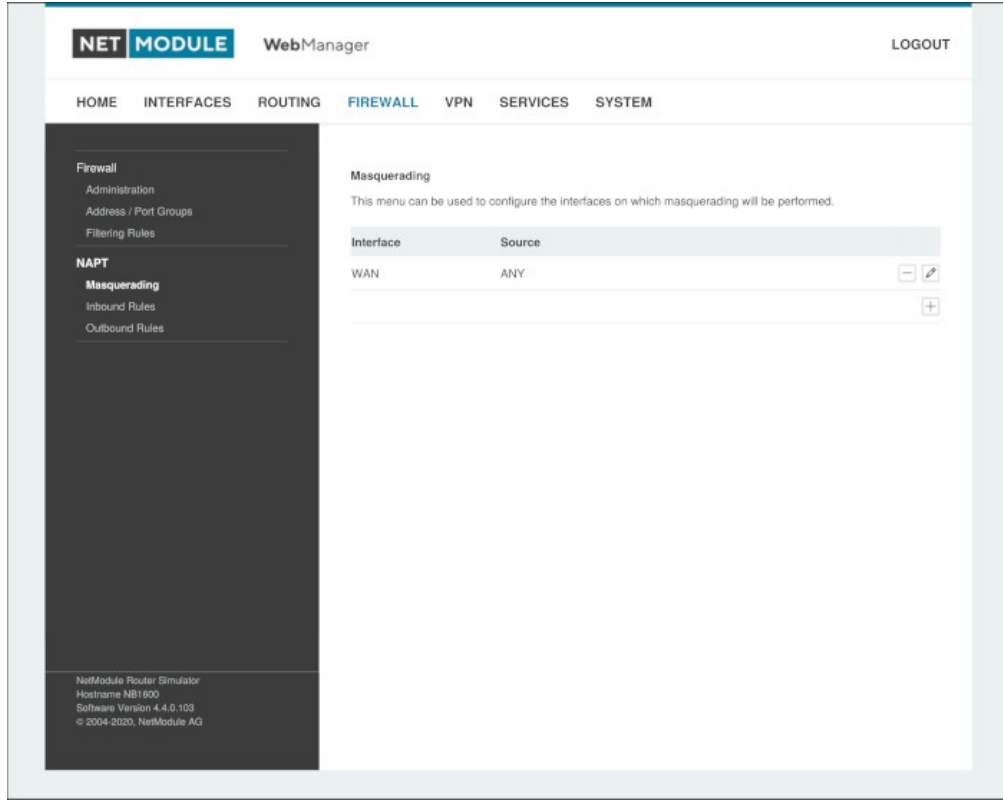
Ekran 6.29.: Güvenlik Duvarı Kuralları

Parametre	Güvenlik Duvarı Kuralı
Açıklama (Description)	Bu kuralın amacı hakkında anlamlı bir açıklama
Eylem (Action)	Bu kuralın paketlerine izin verilip verilmeyeceğini belirtir
Kayıt eşlemeleri (log matches)	Kural eşleşirse bir syslog mesajı gönder
Kaynak (Source)	Eşleşen paketlerin kaynak adresi herhangi biri olabilir veya adres/ağ tarafından belirtilebilir. Kaynak MAC adresinden seçim de mümkündür.
Hedef (Destination)	Eşleşen paketlerin hedef adresi herhangi bir yerel (sistemin kendisine adreslenmiş) veya adres/ağ tarafından belirtilmiş olabilir
Gelen arayüz (Incoming interface)	Eşleşen paketlerin alındığı arayüz
Giden arayüz (Outgoing interface)	Eşleşen paketlerin gönderildiği arayüz
Protokol (Protocol)	Eşleşen paketlerin kullanılan IP protokolü (UDP, TCP, ICMP, ESP, GRE veya OSPF)

İstatistik sayfası, kuralların herhangi bir paketle eşleşip eşleşmediğini anlamak için kullanılabilir ve güvenlik duvarı kurulumunuzda hata ayıklamak için kullanışlı bir yol sağlar.

6.5.4. NAPT

Bu sayfa, sistemi geçen paketler için Ağ Adresi ve Bağlantı Noktası Çevirisi'ni (NAPT) yapılandırmak için kullanılabilir. NAPT, eşleşen IP paketlerindeki IP adreslerini veya/veya TCP/UDP bağlantı noktalarını değiştirir. Bu bağlantıları izleyerek, bir IP oturumunun geri dönen paketlerini de otomatik olarak ayarlayacaktır.



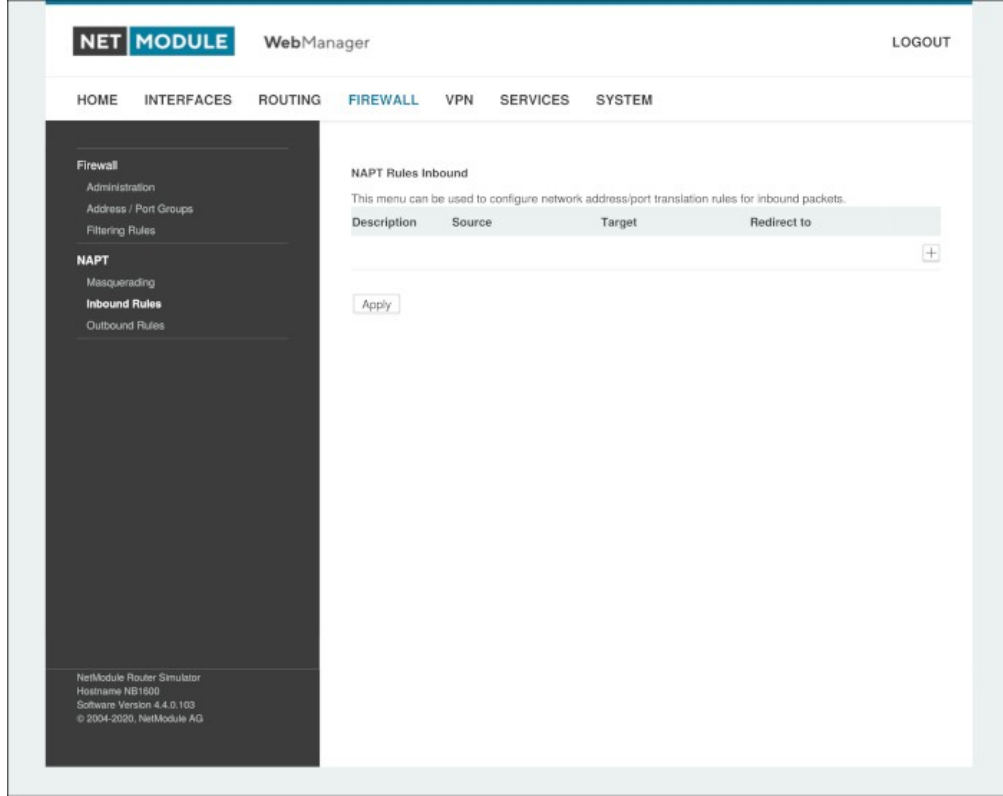
Ekran 6.30.: Maskeleye (Masquerading)

Yönetim sayfası, maskeleyenin gerçekleştirileceği arayüzleri belirtmenize olanak tanır. NAT, burada seçilen arayüzün adresini kullanacak ve giden bağlantılar için rastgele bir kaynak portu seçecek ve böylece özel bir yerel alan ağından genel ağdaki ana bilgisayarlara doğru ana bilgisayarlar arasında iletişimi etkinleştirecektir.

Parametre	Maskeleye Kuralları
Arayüz (Interface)	Bağlantıların maskeleneceği giden arayüz
Kaynak adresi (Source address)	Eşleşen paketlerin maskelendiği kaynak adresi veya ağ
Kaynak ağ maskesi (Source netmask)	Eşleşen paketlerin maskelendiği ağın kaynak ağ maskesi

NAPT Gelen Kuralları

Gelen kurallar, IP paketlerinin hedef bölümünü değiştirmek ve örneğin bir hizmeti veya portu dahili bir ana bilgisayara iletmek için kullanılabilir. Bunu yaparak, bu hizmeti açığa çıkarabilir ve İnternet'ten kullanılabilir hale getirebilirsiniz. Ayrıca, ek giden kurallar kullanarak tek bir ana bilgisayar için 1:1 NAT eşlemesi de oluşturabilirsiniz.



Ekran 6.31.: Gelen NAPT

Belirtilen kuralların sırayla işlendiğini, yani eşleşen bir kural bulunana kadar listenin en üstten en alta doğru ilerlediğini lütfen unutmayın. Eşleşen bir kural bulunmazsa, paket olduğu gibi geçecektir.

Parametre	Gelen NAPT Kuralları
Açıklama (Description)	Bu kuralın anlamlı bir açıklaması
Harita (Map)	Bağlam: Ana Bilgisayar, Ağ veya Bağlantı Noktası Aralığı - aşağıdaki tabloya bakın
Gelen arayüz (Incoming interface)	Eşleşen paketlerin alındığı arayüz
Kaynak (Source)	Eşleşen paketlerin alındığı kaynak adresi veya ağ
Hedef adresi (Target address)	Eşleşen paketlerin hedef adresi (isteğe bağlı)
Protokol (Protocol)	Eşleşen paketlerin kullanılan protokolü
Portlar (Ports)	Eşleşen paketlerin kullandığı UDP/TCP portu
Şuraya yönlendir (Redirect to)	Eşleşen paketlerin yönlendirileceği adres
Şu porta yönlendir (Redirect port)	Eşleşen paketlerin yönlendirileceği port



İhtiyaçlarınıza göre eşleme bağlamını seçin:

Parametre	Bağlamı Eşleme
Ana bilgisayar (host)	Belirli bir ana bilgisayar için hedef adresi ve bağlantı noktasını yeniden yazın (yani 10.0.0.1:8080 → 192.168.1.100:80)
Ağ (network)	Tam bir ağ için hedef adresini yeniden yazın (yani 192.168.1.0/24)
Port aralığı (port range)	Hedef adresi ve portu gelen porta göre yeniden yazın (yani 10.0.0.1:22000-22255 → 192.168.1.0/24:22). Giden kurallarda port aralığı çevirisi için karşılık gelen bir kural yoktur. Orada ağ tabanlı eşleme kullanın.

NAPT Giden Kuralları

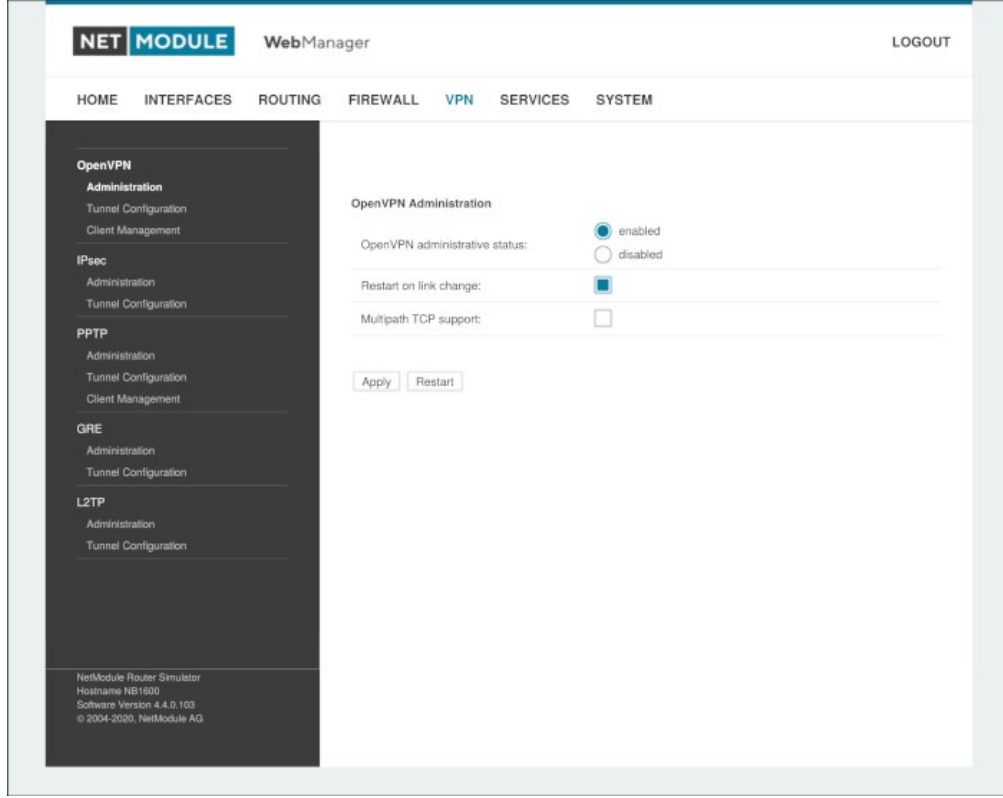
Giden kurallar, IP paketlerinin kaynak bölümünü değiştirecek ve 1:1 NAT eşlemeleri oluşturmak için kullanılabilir gibi paketleri belirli bir hizmete yönlendirmek için de kullanılabilir.

Parametre	Giden NAPT Kuralları
Açıklama (Description)	Bu kuralın anlamlı bir açıklaması
Giden arayüz (Outgoing interface)	Eşleşen paketlerin yönlendiriciden ayrıldığı giden arayüz
Hedef adresi (Target address)	Eşleşen paketlerin hedef adresi (isteğe bağlı)
Kaynak (Source)	Eşleşen paketlerin alındığı kaynak adresi veya ağ
Protokol (Protocol)	Eşleşen paketlerin kullanılan protokolü
Portlar (Ports)	Eşleşen paketlerin kullandığı UDP/TCP portu
Şuraya yönlendir (Redirect to)	Eşleşen paketlerin kaynak adresinin yeniden yazılacağı adres
Şu porta yönlendir (Redirect port)	Eşleşen paketlerin kaynak portunun yeniden yazılacağı port

6.6. VPN

6.6.1. OpenVPN

OpenVPN Yönetimi

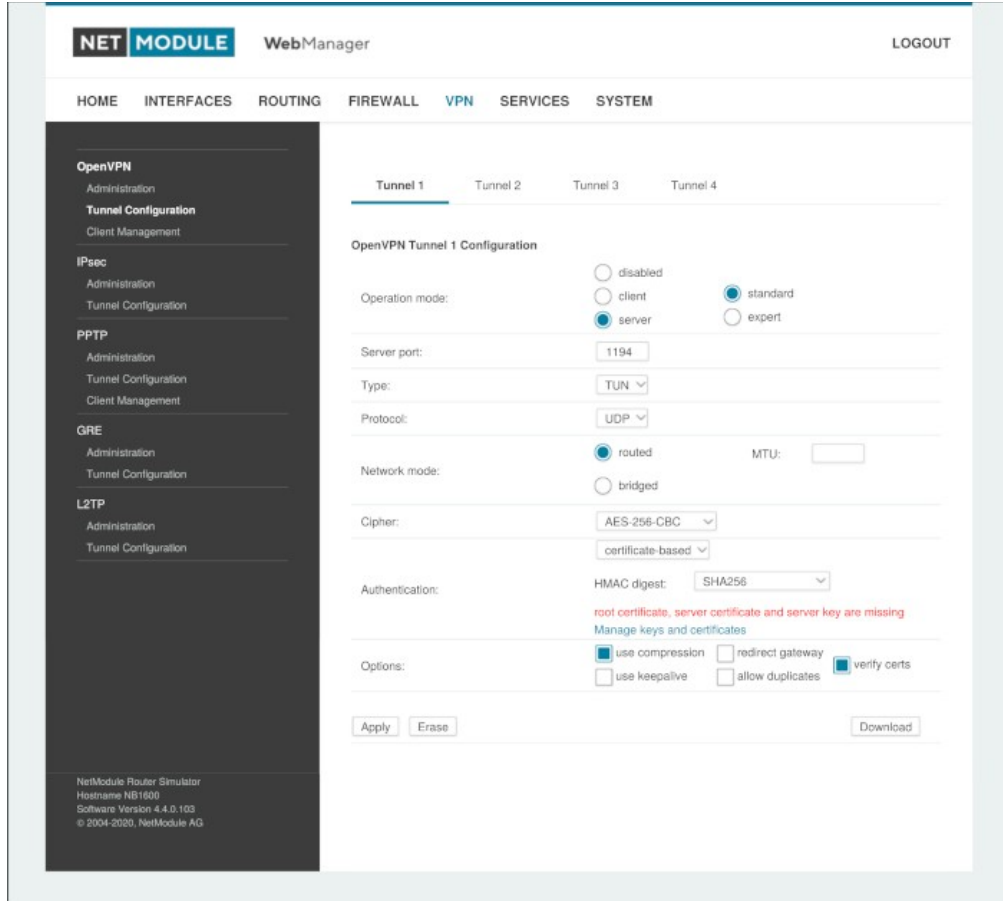


Ekran 6.32.: OpenVPN Yönetimi

Parametre	OpenVPN Yönetimi
Yönetim durumu (Administrative status)	OpenVPN'in etkin olup olmadığını belirtir
Bağlantı değişiminde yeniden başlatma (Restart on link change)	WAN bağlantısında değişiklik olursa OpenVPN sürecini yeniden başlatır

Tünel Yapılandırması

NetModule AG yönlendiricileri, bir adet sunucu tüneli ve dört adet istemci tünelini destekler. Tünel parametreleri, standart yapılandırma modunda manuel olarak girilebilir ya da önceden oluşturulmuş uzman mod dosyası yüklenebilir. Daha fazla bilgi için bölüm 6.6.1'e bakınız.



Ekran 6.33.: OpenVPN Yapılandırma

Parametre	OpenVPN Yapılandırma
Çalıştırma modu (Operation mode)	Bu tünel için istemci veya sunucu modunun kullanılıp kullanılmayacağını belirtir, ayrıca tünelin standart bir şekilde yapılandırılıp yapılandırılmayacağını veya uzman modu dosyasının kullanılıp kullanılmayacağını belirtir.



Tünel istemci modunda çalıştırılıyorsa, aşağıdaki ayarlar uygulanabilir:

Parametre	OpenVPN İstemci Yapılandırma
Eş seçimi (Peer selection)	Uzaktaki eşin nasıl seçileceğini belirtir, tek bir sunucunun yanı sıra, arızalar durumunda sırayla (yani devralma) veya rastgele (yani yük dengeleme) seçilebilen birden fazla sunucu yapılandırabilirsiniz.
Sunucu (Server)	Uzak sunucunun adresi veya ana bilgisayar adı
Bağlantı noktası (Port)	Uzak sunucunun bağlantı noktası (varsayılan olarak 1194)

Bir tüneli (istemci ve sunucu modu) yapılandırmak için aşağıdaki ayarlar kullanılabilir:

Parametre	OpenVPN Yapılandırma
Arayüz tipi (Interface type)	Bu tünel için cihaz türü TUN (genellikle yönlendirilmiş bağlantılar için kullanılır) veya TAP (köprülenmiş ağlar için gereklidir) olabilir
Protokol (Protocol)	Taşıma bağlantısı için kullanılacak tünel protokolü
Ağ modu (Network mode)	Paketlerin nasıl iletileceğini tanımlar, bu da belirli bir LAN arayüzünden/aracılığına yönlendirilebilir veya köprülenebilir. Gerekirse, tünel arayüzü için maksimum aktarım birimini de belirtebilirsiniz.
MTU	Tünel arayüzünün Maksimum İletim Birimi (Maximum Transmission Unit, MTU)
Şifreleme (Encryption)	Şifreleme için kullanılan gerekli şifreleme mekanizması
Özet (Digest)	Kimlik doğrulama için kullanılan özet algoritması

Kimlik doğrulama aşağıdaki yollarla yapılabilir:

Parametre	OpenVPN Yetkinlendirme
Sertifika tabanlı (certificate-based)	Tüneli doğrulamak için sertifikalar ve anahtarlar. Lütfen uygun anahtarların/sertifikaların yüklendiğinden veya oluşturulduğundan emin olun (bkz. 6.8.8).
Kimlik bilgisi tabanlı (credential-based)	Kimlik doğrulama için kullanıcı adı ve şifre kullanılmaktadır.
Her ikisi (both)	Tünel doğrulaması sertifikaları ve kimlik bilgilerini kullanır.
Hiçbiri (none)	Tünel doğrulanmadı (önerilmez)



Aşağıdaki ek seçenekler uygulanabilir:

Parametre	OpenVPN Seçenekleri
Sıkıştırma kullan (use compression)	LZO paket sıkıştırmasını etkinleştirin veya devre dışı bırakın
Hayatta tutmayı kullan (use keepalive)	Etkin olmama durumuna rağmen tünelin açık kalmasını sağlamak için periyodik bir canlı tutma paketi göndermek için kullanılabilir
Ağ geçidini yönlendir (redirect gateway)	Ağ geçidini yeniden yönlendirerek tüm paketler VPN tüneline yönlendirilecektir. Lütfen tünelin arkasındaki ağda temel hizmetlerin (DNS veya NTP sunucuları gibi) erişilebilir olduğundan emin olun. Şüphe durumunda, doğru arayüzü işaret eden ekstra bir statik rota oluşturun.
Kopyalara izin ver (allow duplicates)	Aynı ortak ada sahip birden fazla istemcinin aynı anda bağlanmasına izin verin. (sadece sunucu modu)
Sertifika doğrula (verify certs)	Eş sertifikayı yerel CRL ile karşılaştırın. (sadece sunucu modu)
DNS ile uzlaş (negotiate DNS)	Etkinleştirildiğinde sistem tünel üzerinden müzakere edilen isim sunucularını kullanacaktır.

OpenVPN Uzman Yapılandırması (İstemci)

Uzman yapılandırma modu, gerekli yapılandırmayı ve isteğe bağlı olarak anahtar/sertifika dosyalarını veya ayrıca bir OpenVPN dosya biçimini (*.ovpn) içeren bir zip paketini (*.zip) yükleyerek bir tüneli yapılandırmanın basit bir yolunu sunar. Bir istemci tüneli genellikle aşağıdaki dosyalardan oluşur:

Parametre	İstemci Uzman Dosyaları
client.conf	OpenVPN yapılandırma dosyası (mevcut seçenekler için http://www.openvpn.net adresine bakın)
ca.crt	Kök sertifika yetkilisi dosyası
client.crt	Sertifika dosyası
client.key	Özel anahtar dosyası
client.p12	PKCS#12 dosyası
ta.key	TLS kimlik doğrulama anahtar dosyası

Lütfen istediğiniz dosya adlarını belirtebileceğinizi unutmayın; ancak yapılandırma dosyası son eki .conf olmalı ve yapılandırma dosyasında belirtilen tüm dosyalar görelî yol adlarına karşılık gelmelidir.



OpenVPN Uzman Yapılandırması (Server)

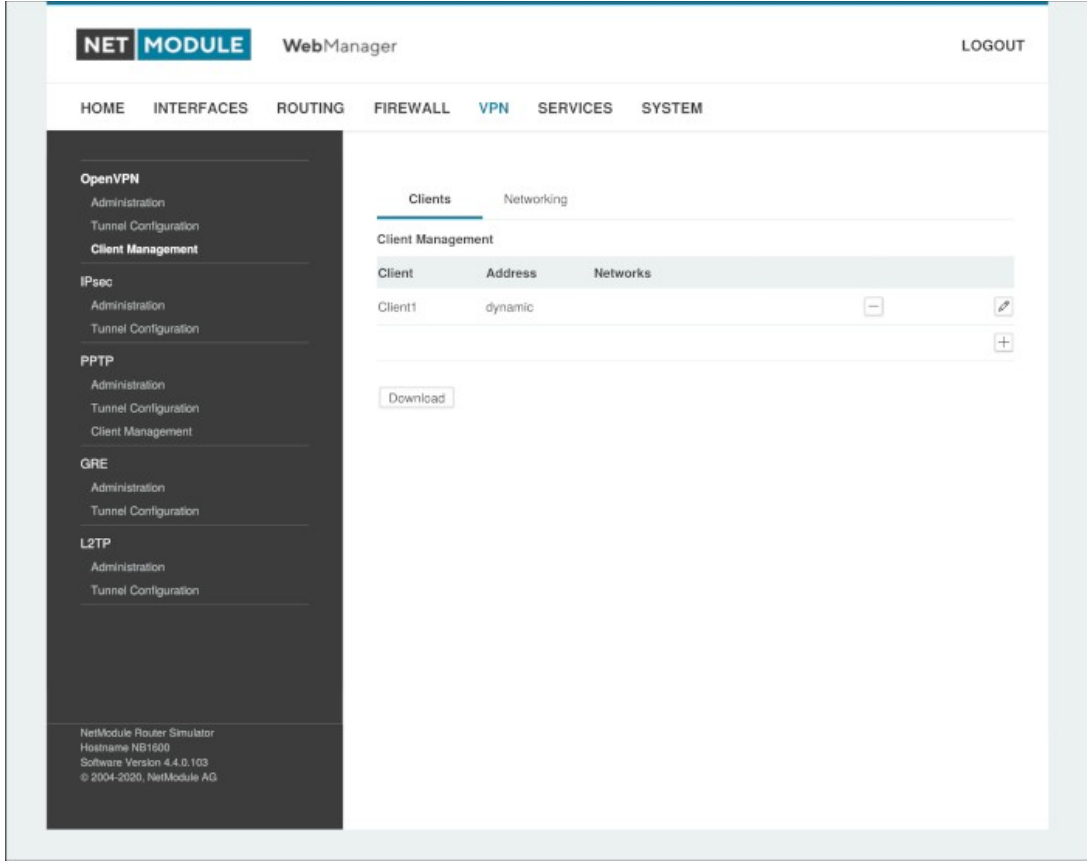
Bir sunucu tüneli genellikle aşağıdaki dosyaları gerektirir:

Parametre	Sunucu Uzman Dosyaları
server.conf	OpenVPN yapılandırma dosyası
ca.crt	Kök sertifika yetkilisi dosyası
server.crt	Sertifika dosyası
server.key	Özel anahtar dosyası
dh1024.pem	Diffie-Hellman parametre dosyası
ccd	İstemciye özgü yapılandırma dosyalarını içeren bir dizin

Bir sertifikanın geçerlilik süresi dolduğunda geçerli hale geldiğini unutmayın, bu nedenle sertifikalar oluşturulmadan ve tünel bağlantısı kurulmadan önce doğru bir sistem saati ayarlanmalıdır. Lütfen tüm NTP sunucularının erişilebilir olduğundan emin olun. Ana bilgisayar adlarını kullanmak için çalışan bir DNS sunucusu da gereklidir.

İstemci Yönetimi

OpenVPN sunucu tüneline başarıyla kurduğunuzda, hizmetinize bağlanan istemcileri yönetebilir ve etkinleştirebilirsiniz. Şu anda bağlı istemciler, bağlantı zamanı ve IP adresi dahil olmak üzere bu sayfada görülebilir. Bağlı istemcileri devre dışı bırakarak atabilirsiniz.



Ekran 6.34.: OpenVPN İstemci Yönetimi

Ağ bölümünde her istemci için sabit bir tünel uç noktası adresi belirtebilirsiniz. Belirli bir istemci için sabit bir adres kullanmayı düşünüyorsanız, diğerlerine de sabit adresler uygulamanız gerekeceğini lütfen unutmayın.

İstemcilerin arkasındaki ağı ve her istemciye gönderilecek rotaları belirtebilirsiniz. Bu, yönlendirme amaçları için yararlı olabilir, örneğin belirli ağlar için trafiği sunucuya yönlendirmek istemeniz durumunda.

İstemciler arasında yönlendirme genellikle izin verilmez ancak isterseniz etkinleştirebilirsiniz.

Son olarak, etkinleştirilmiş istemciler için tüm uzman modu dosyalarını oluşturabilir ve indirebilirsiniz; bunlar her istemciyi kolayca doldurmak için kullanılabilir.

Sertifikalarla sunucu modunda çalışırken, muhtemelen çalınmış bir istemci sertifikasını iptal ederek belirli bir istemciyi engellemek mümkündür (bkz. 6.8.8).

6.6.2. IPSec

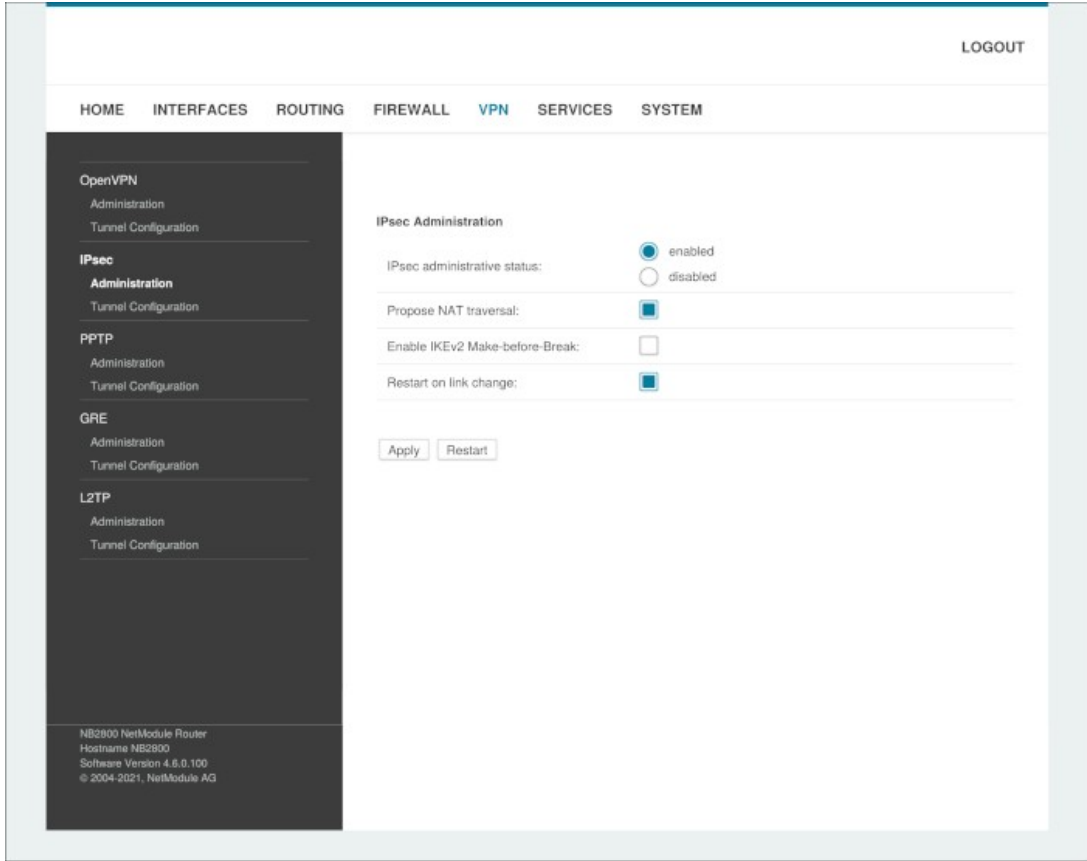
IPsec, bir iletişim oturumunun her paketini doğrulayıp şifreleyerek ve böylece güvenli bir sanal özel ağ kurarak IP iletişimlerini güvence altına alan bir protokol paketidir.

IPsec, anahtar değişimi ve veri şifrelemesi için çeşitli kriptografik protokoller ve şifreler içerir ve güvenlik açısından en güçlü VPN teknolojilerinden biri olarak görülebilir. Aşağıdaki mekanizmaları kullanır:

Mekanizma	Açıklama
AH	Kimlik Doğrulama Başlıkları (Authentication Headers, AH), IP datagramları için bağlantısız bütünlük ve veri kaynağı kimlik doğrulaması sağlar ve tekrar saldırılarına karşı koruma sağlar.
ESP	Kapsüllenmiş Güvenlik Yüğü (Encapsulating Security Payloads, ESP), gizlilik, veri kaynağı kimlik doğrulaması, bağlantısız bütünlük, tekrar oynatma önleme hizmeti ve sınırlı trafik akışı gizliliği sağlar.
SA	Güvenlik Birlikleri (Security Associations, SA), AH ve/veya ESP işlemlerini çalıştırmak için gerekli parametreleri sağlayan güvenli bir kanal ve bir algoritma paketi sağlar. İnternet Güvenlik Birliği Anahtar Yönetim Protokolü (Internet Security Association Key Management Protocol, ISAKMP), kimliği doğrulanmış anahtar değişimi için bir çerçeve sağlar.

Şifreleme ve kimlik doğrulama için anahtarların pazarlığı genellikle iki aşamadan oluşan İnternet Anahtar Değişim Protokolü (Internet Key Exchange, IKE) tarafından yapılır:

Faz	Açıklama
IKE faz 1 (IKE phase 1)	IKE, bu aşamada ISAKMP güvenli ilişkisini kurmak için eşi doğrular. Bu, ana (main) veya agresif (aggressive) mod kullanılarak gerçekleştirilebilir. Ana mod yaklaşımı, Diffie-Hellman anahtar değişimini kullanır ve kimlik doğrulama her zaman müzakere edilen anahtarla şifrelenir. Saldırgan mod, önceden paylaşılan anahtarın karmalarını kullanır ve bu nedenle sözlük saldırılarına eğilimli olduğu için genellikle kaçınılması gereken daha az güvenli bir mekanizmayı temsil eder.
IKE faz 2 (IKE phase 2)	IKE son olarak IPsec SA parametrelerini ve anahtarlarını müzakere eder ve daha sonra AH/ESP için gerekli olacak olan eşlerde eşleşen IPsec SA'ları kurar.

Yönetim (Administration)

Ekran 6.35.: IPsec Yönetimi

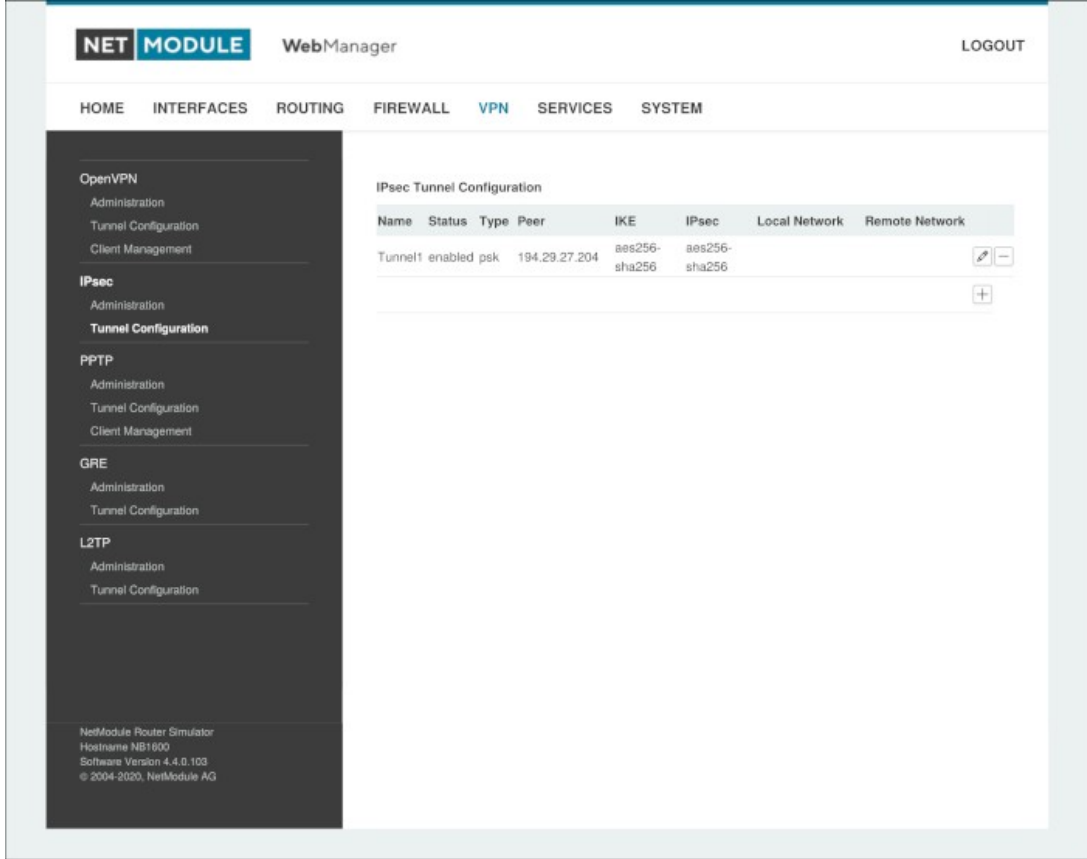
Bu sayfa IPsec'i etkinleştirmek/devre dışı bırakmak için kullanılabilir, ayrıca NAT-Traversal ve IKEv2 Make-before-break'in kullanılıp kullanılmayacağını da belirtebilirsiniz.

NAT-Traversal, esas olarak bir yönlendiricinin paketlerin IP adresini/portunu değiştirdiği bir yolu geçen bağlantılar için kullanılır. Paketleri UDP'de kapsüller ve bu nedenle küçük boyutlu MTU arayüzleri üzerinden çalıştırıldığında hesaba katılması gereken küçük bir ek yük gerektirir.

NAT-Traversal'ı çalıştırmanın IKE'nin güvenlik duvarı kurallarını ayarlarken hesaba katılması gereken 500 yerine 4500 numaralı UDP portunu kullanmasını sağladığını lütfen unutmayın.

Make-before-break, şu anda kullanılan SA'yı (=break) silmeden önce çakışan bir SA (=make) oluşturarak gerekli düzenli yeniden kimlik doğrulamasını optimize etmek için kullanılan bir IKEv2 seçeneğidir. Bu şekilde, veri akışının kesintiye uğraması en aza indirilir. Bu seçeneği kullanmak için her iki eşin de çakışan SA'ları işleyebilmesi gerekir.

Yapılandırma (Configuration)



Ekran 6.36.: IPsec Yapılandırma

Genel (General)

Tünel kurulumu için öncelikle aşağıdaki parametreleri yapılandırmanız gerekecektir:

Parametre	IPsec Genel Ayarlar
Yerel IP adresi (Local IPaddress)	Yerel arayüzün IP'si. Herhangi bir IP adresine izin vermek için 0.0.0.0 belirtebilirsiniz.
Uzak eş adresi (Remote peer address)	Uzak IPsec eşinin IP adresi veya ana bilgisayar adı. Roadwarrior istemcileri için yanıtlayıcı olarak hareket etmek üzere 0.0.0.0 belirtebilirsiniz.
Ölü eş algılama durumu (Dead Peer Detection Status)	Ölü Eş Algılama'nın (Dead Peer Detection, DPD) (RFC 3706'ya bakın) kullanılıp kullanılmayacağını belirtir. DPD, özellikle ISAKMP tüneli olmak üzere, herhangi bir kopuk IPsec bağlantısını algılayacak ve tünelin daha hızlı yeniden kurulması için ilgili SA'ları (Güvenlik İlişkileri, Security Associations) ve SPI'ları (Güvenlik Yük Tanımlayıcısı, Security Payload Identifier) yenileyecektir.
Algılama döngüsü (Detection cycle)	Bu bağlantı için gönderilen DPD keepalive'ları arasındaki gecikme (saniye cinsinden) (varsayılan 30 saniye)



Parametre	IPsec Genel Ayarlar
Başarısızlık eşiği (Failure threshold)	IPsec eşi ölü olarak kabul edilene kadar yanıtlanmamış DPD isteklerinin sayısı (yönlendirici daha sonra ölü bir bağlantıyı otomatik olarak yeniden kurmaya çalışacaktır)
Eylem (Action)	Bir eşin bağlantısı kesilirse gerçekleştirilecek eylem. Açılır menüden kullanılabilen seçenekler eşi temizlemek, tutmak veya yeniden başlatmaktır.

IKE Kimlik Doğrulaması (IKE Authentication)

NetModule AG yönlendiricileri, önceden paylaşılan anahtarlar (PSK) veya genel anahtar altyapısı içindeki sertifikalar aracılığıyla IKE kimlik doğrulamasını destekler. Genişletilmiş Kimlik Doğrulama (XAUTH), RADIUS benzeri kimlik doğrulamasını kullanır ve IPsec üzerinden kullanıcı düzeyinde erişim denetimi uygulamak için kullanılabilir. PSK kullanımını aşağıdaki ayarları gerektirir:

Parametre	PSK ile IPsec IKE Kimlik Doğrulama Ayarları
PSK	Eşler arasında kimlik doğrulaması yapmak için kullanılan önceden paylaşılan anahtar
Yerel ID tipi (Local ID Type)	Yerel kimlik için FQDN, username@FQDN veya IP adresi olabilen kimlik türü
Yerel ID (Local ID)	Yerel ID değeri
Uzak ID tipi (Remote ID type)	Uzak kimlik için kimlik türü
Uzak ID (Remote ID)	Uzak ID değeri

Sertifikaları kullanırken çalışma modunu belirtmeniz gerekir. PKI istemcisi (başlatıcı) olarak çalıştırdığınızda, sertifikalar bölümünde Sertifika Yetkilinize gönderilmesi ve sonrasında yönlendiriciye aktarılması gereken bir Sertifika İmzalama Talebi (CSR) oluşturabilirsiniz. PKI sunucu modunda (yoğunlaştırıcı), yönlendirici Sertifika Yetkilisini temsil eder ve uzak eşler için sertifikaları verir. Bunlar iptal edilebilir. Genişletilmiş Kimlik Doğrulama (XAUTH) kullanılarak aşağıdaki ayarlar yapılabilir:

Parametre	IPsec XAUTH Ayarları
Kullanıcı adı (User name)	XAUTH kullanıcısının adı
Kullanıcı şifresi (User password)	XAUTH kullanıcısının şifresi
Grup adı (Group name)	Grup ID
Grup şifresi (Group password)	Grup şifresi



IKE Teklifi (IKE Proposal)

Bu bölüm, 1. aşama ayarlarını yapılandırmak için kullanılabilir:

Parametre	IPsec IKE Teklif Ayarları
Müzakere modu (Negotiation mode)	İstenilen müzakere modunu seçin. Tercihen ana (main) mod kullanılmalıdır ancak dinamik uç nokta adresleriyle uğraşırken agresif (aggressive) mod uygulanabilir.
Şifreleme algoritması (Encryption algorithm)	İstenilen IKE şifreleme yöntemi (AES256'yı öneririz)
Kimlik doğrulama algoritması (Authentication algorithm)	İstenilen IKE kimlik doğrulama yöntemi (SHA2, SHA256, SHA384, SHA512 öneririz)
IKE Diffie-Hellman Group	IKE Diffie-Hellman Grup
SA yaşam süresi (SA life time)	SA yaşam süresi
Yalancı rastgele fonksiyon (Pseudo-random function)	İsteğe bağlı olarak kullanılabilen PRF (Pseudo-random function) algoritmaları.

IPSec Teklifi (IPsec Proposal)

Bu bölüm, 2. aşama ayarlarını yapılandırmak için kullanılabilir:

Parametre	IPsec Teklif Ayarları
Kapsülleme modu (Encapsulation mode)	İstenilen kapsülleme modu (Tünel veya Taşıma)
IPsec protokol (IPsec protocol)	İstenilen IPsec protokolü (AH veya ESP)
Şifreleme algoritması (Encryption algorithm)	İstenilen IKE şifreleme yöntemi (AES256'yı öneririz)
Kimlik doğrulama algoritması (Authentication algorithm)	İstenilen IKE kimlik doğrulama yöntemi (SHA2, SHA256, SHA384, SHA512 öneririz)
SA hayat süresi	SA (Security Associations) etkin kalma süresi
Mükemmel ileri gizlilik (Perfect forward secrecy, PFS)	Perfect Forward Secrecy (PFS) kullanılıp kullanılmayacağını belirtir. Bu özellik, PFS'nin anahtar değişim protokolünün ihlal edilmesini önlemesi ve önceki anahtarların tehlikeye atılmasını engellemesi nedeniyle güvenliği artırır.
Kapsüllemeyi zorla (Force encapsulation)	NAT durumu algılanmasa bile ESP paketleri için UDP kapsüllemesini zorla.

Ağlar (Networks)

Güvenlik ilişkileri oluştururken, IPsec tünel içindeki yönlendirilen ağları izleyecektir. Paketler yalnızca eşleşen kaynak ve hedef ağa sahip geçerli bir SA mevcut olduğunda iletilecektir. Bu nedenle, aşağıdaki ayarları uygulayarak uç noktaların sağındaki ve solundaki ağları belirtmeniz gerekebilir:

Parametre	IPsec Ağ Ayarları
Yerel ağ (Local network)	Yerel alan ağınızın adresi
Yerel ağ maskesi (Local netmask)	Yerel alan ağınızın ağ maskesi
Eş ağı (Peer network)	Eşin arkasındaki uzak ağın adresi
Eş ağ maskesi (Peer netmask)	Eşin arkasındaki uzak ağın ağ maskesi



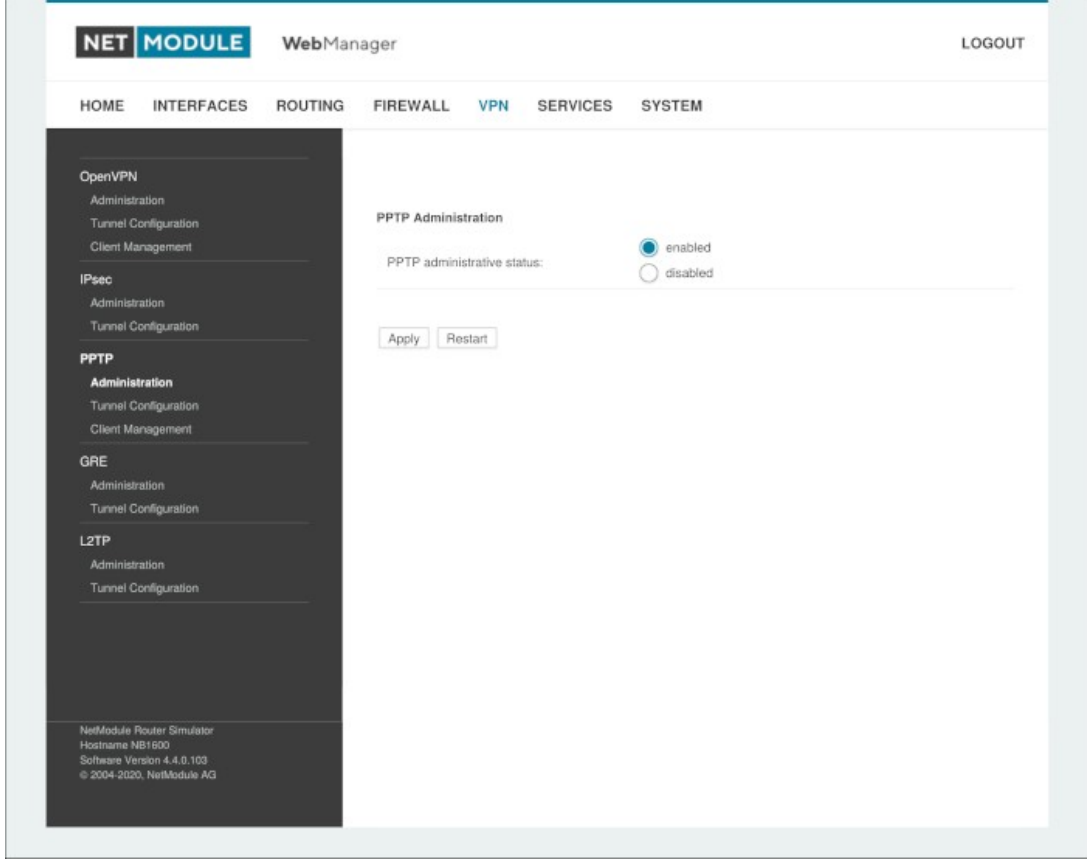
Parametre	IPsec Ağ Ayarları
NAT adresi (NAT address)	İsteğe bağlı olarak, farklı bir yerel ağdan gelen paketler için NAT (maskeleyme) uygulayabilirsiniz. NAT adresi, daha önce yerel ağ olarak belirtilen ağda bulunmalıdır. NAT adresi etkinleştirilmişse ancak değer boşsa yönlendirici geçerli bir NAT adresi tahmin etmeye çalışacaktır (önerilmez).

İstemci Yönetimi (Client Management)

Bir IPsec tüneli başarıyla kurduğunuzda, hizmetinize bağlanan istemcileri yönetebilir ve etkinleştirebilirsiniz. Etkinleştirilmiş istemciler için uzman modu dosyaları oluşturmak ve indirmek mümkündür; bu dosyalar her istemciyi kolayca doldurmak için kullanılabilir.

6.6.3. PPTP

Noktadan Noktaya Tünelleme Protokolü (Point-to-Point Tunneling Protocol, PPTP), iki ana bilgisayar arasında sanal özel ağlar uygulamak için bir yöntemdir. PPTP, yapılandırması kolaydır ve Microsoft Çevirmeli ağ sunucuları arasında yaygın olarak dağıtılır. Ancak, zayıf şifreleme algoritmaları nedeniyle, günümüzde güvensiz olarak kabul edilir, ancak yine de tüneller kurmak için basit bir yol sağlar.

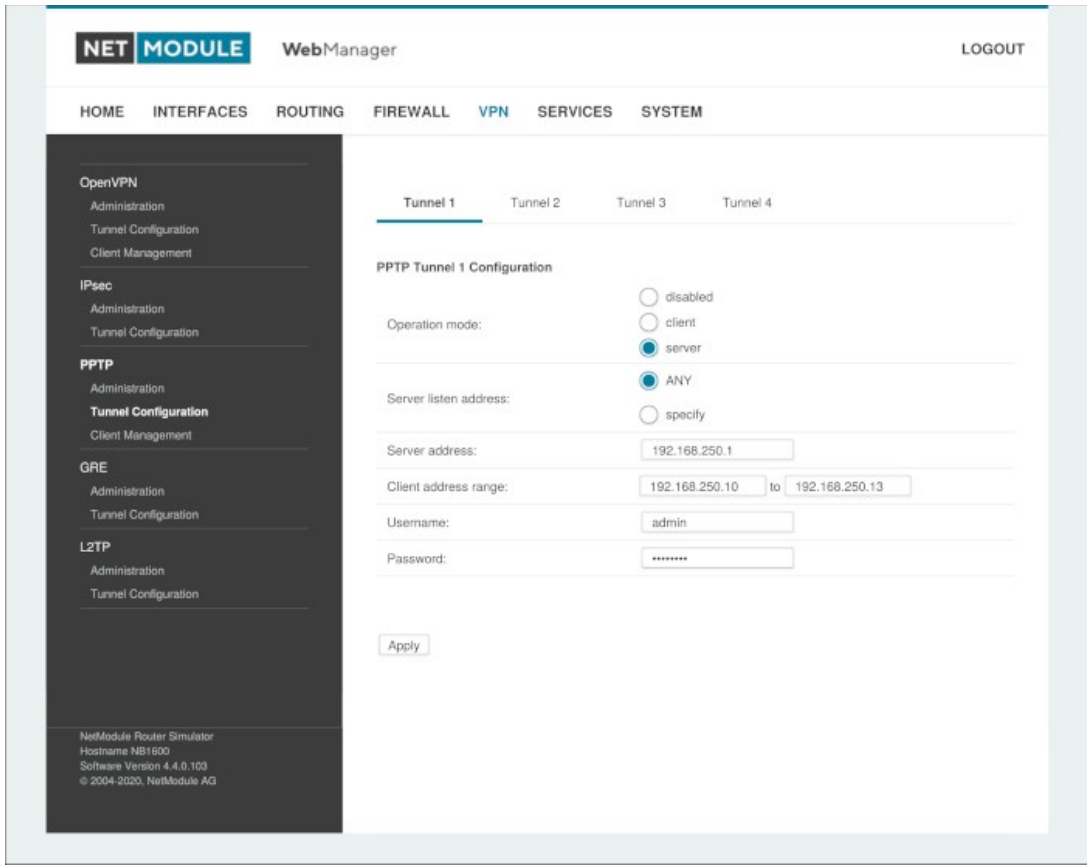


Ekran 6.37.: PPTP Yönetimi

Bir PPTP tüneli kurarken, sunucu veya istemci arasında seçim yapmanız gerekir. Bir istemci tüneli için aşağıdaki parametrelerin ayarlanması gerekir:

Parametre	PPTP İstemci Ayarları
Sunucu adresi (Server address)	Uzak sunucunun IP adresi
Kullanıcı adı (Username)	Kimlik doğrulama için gerekli kullanıcı adı
Şifre (Password)	Kimlik doğrulama için gerekli şifre

Sabit adresli istemcilerin kurulumunda kullanıcı adı ve şifre kullanılmadığını lütfen unutmayın.



Ekran 6.38.: PPTP Tünel Yapılandırması

Bir sunucu kurmak için aşağıdaki ayarların yapılması gerekir:

Parametre	PPTP Sunucu Ayarları
Dinleme adresi (Listen address)	Gelen istemci bağlantıları için hangi IP adresinin dinleneceğini belirtir
Sunucu adresi (Server address)	Tünel içindeki sunucu adresi
İstemci adres aralığı (Client address range)	Her istemciye atanan IP adreslerinin aralığını belirtir



PPTP İstemci Yönetimi (PPTP Client Management)

Bir sunucu tüneli için PPTP istemcilerinin burada yapılandırılması gerekir. Bunlar kullanıcı adı ve paroladan oluşur. Bunlara, herhangi bir rotayı özel bir tünele yönlendirmek için kullanılabilen sabit bir IP adresi atanabilir.

The screenshot displays the NET MODULE WebManager interface. The top navigation bar includes 'NET MODULE', 'WebManager', and 'LOGOUT'. Below this, a menu bar lists 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. The 'VPN' section is expanded, showing a sidebar with categories: 'OpenVPN', 'IPsec', 'PPTP', 'GRE', and 'L2TP'. Under 'PPTP', 'Client Management' is selected. The main content area is titled 'PPTP Clients' and features a table with columns 'Username' and 'Address'. A '+' button is visible in the bottom right corner of the table area. At the bottom left, system information is displayed: 'NetModule Router Simulator', 'Hostname NB1800', 'Software Version 4.4.0.103', and '© 2004-2020, NetModule AG'.

Ekran 6.39.: PPTP İstemci Yönetimi

6.6.4. GRE

Genel Yönlendirme Kapsüllemesi (GRE), IP üzerinden sanal noktadan noktaya bağlantılar içinde çok çeşitli ağ katmanı protokollerini kapsülleyebilen bir tünelleme protokolüdür. GRE, RFC 1701, 1702 ve 2784'te tanımlanmıştır. Şifreleme veya yetkilendirme sağlamaz ancak tünelleme amaçları için diğer VPN tekniklerinin (IPsec gibi) üstünde adres bazında kullanılabilir. Bir tünel kurmak için aşağıdaki parametreler gereklidir:

Parametre	GRE Ayarları
Yerel adres (Local address)	GRE paketlerinin gönderici adresi olarak kullanılan IP adresi (isteğe bağlı)
Eş adresi (Peer address)	Uzaktaki eşin IP adresi
Arayüz (Interface)	Bu tünel için cihaz türü
Yerel tünel adresi (Local tunnel address)	Tünelin yerel IP adresi
Yerel tünel ağ maskesi (Local tunnel netmask)	Tünelin yerel ağ maskesi
Uzak ağ (Remote network)	Tünel uzak ağ adresi
Uzak ağ maskesi (Remote netmask)	Tünel uzak ağ maskesi
Tünel anahtarı (Tunnel key)	GRE tünel anahtarı, uzak sunucunun farklı iletişim ortaklarından gelen GRE paketlerini ayırt etmesine olanak tanır

Genel olarak, yerel tünel adresi/ağ maskesi diğer arayüz adresleriyle çakışmamalıdır. Uzak ağ/ağ maskesi, hangi paketlerin kapsülünüp tünel üzerinden aktarılacağını kontrol etmek için ek bir rota girişiyle sonuçlanacaktır.

6.6.5. L2TP

Katman 2 Tünelleme Protokolü, herhangi bir şifreleme veya gizliliği desteklemeyen bir tünelleme protokolüdür. Gizlilik sağlamak için tünel içinde geçtiği bir şifreleme protokolüne güvenir. Bir tünel kurmak için aşağıdaki parametreler gereklidir:

Parametre	L2TP Ayarları
Taşıma protokolü (Transport protocol)	Kullanılacak taşıma protokolü
Yerel IP (Local IP)	Tünelin yerel IP adresi
Uzak IP (Remote IP)	Tünelin uzak IP adresi
Yerel port (Local port)	Tünelin yerel port adresi
Uzak port (Remote Port)	Tünel uzak bağlantı noktası adresi
Yerel tünel ID (Local tunnel ID)	Yerel tünel kimliği, oturumun oluşturulacağı tüneli tanımlar
Uzak tünel (Remote tunnel ID)	Uzak tünel kimliği, eş tarafından atanan tüneli tanımlar
Yerel oturum ID (Local Session ID)	Yerel oturum kimliği, oluşturulan oturumu tanımlar
Uzak oturum ID (Remote Session ID)	Uzak oturum kimliği, eş tarafından atanan oturumu tanımlar
Yerel çerez (Local Cookie)	Yerel çerez, oturuma atanacak isteğe bağlı bir çerez değeri ayarlar
Uzak çerez (Remote Cookie)	Uzak çerez, oturuma atanacak isteğe bağlı bir eş çerez değeri ayarlar
MTU	Tünel arayüzünün Maksimum İletim Birimi (Maximum Transmission Unit)
Köprü arayüzü (Bridge Interface)	Misafir arayüzünün bağlanacağı arayüz

6.6.6. Dial-In

Bu sayfada GSM aramaları üzerinden veri bağlantısı kurmak için Dial-In sunucusunu yapılandırabilirsiniz. Bu nedenle, genellikle yalnızca 2G'lik gerekli bir servis türü uygulanır, böylece modem yalnızca GSM'e kaydolar. Doğal olarak, giden WWAN arayüzlerinin ve Dial-In bağlantısının eş zamanlı kullanımı mümkün değildir.

The screenshot displays the 'Dial-in Server Configuration' page in the NET MODULE WebManager. The interface includes a top navigation bar with 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. A left sidebar menu lists various services: OpenVPN, IPsec, PPTP, GRE, L2TP, and Dial-in Server. The main configuration area for the Dial-in Server includes the following fields: Administrative status (radio buttons for 'enabled' and 'disabled', with 'disabled' selected), Modem (dropdown menu set to 'Mobile1'), Username (text input), Password (text input), Address range start (text input set to '192.168.254.1'), and Address range size (text input set to '3'). An 'Apply' button is located below the configuration fields. Below the configuration fields, the 'Dial-in Server Status' section shows the Operational status as 'disabled'. At the bottom of the sidebar, there is a footer with the text: 'NetModule Router Simulator, Hostname NB1600, Software Version 4.4.0.103, © 2004-2020, NetModule AG'.

Ekran 6.40.: Dial-in Sunucu Ayarları

Aşağıdaki ayarlar yapılabilir:

Parametre	Çevirmeli Sunucu Yapılandırması
Yönetimsel durum (Administrative status)	Gelen çağrılarının cevaplanıp cevaplanmayacağını belirtir
Modem	Aramaların gelebileceği modemi belirtir
Kullanıcı (User)	Gelen PPP bağlantısı için kullanıcı adını belirtir
Şifre (Password)	Gelen PPP bağlantısı için parolayı belirtir
Adres aralığı başlangıcı (Address range start)	Gelen istemcilere atanan IP adresi aralığının başlangıcı
Adres aralığı boyutu (Address range size)	İstemci IP adresi aralığı için adres sayısı

Lütfen Dial-In bağlantılarının genellikle önerilmediğini unutmayın. GSM sesli aramaları olarak uygulandıkları için güvenilirlik ve zayıf bant genişliği sorunları yaşarlar.

6.7. Servisler (Services)

6.7.1. SDK

NetModule AG yönlendiricileri, müşteriye özel işlev ve uygulamaları basit ve hızlı bir şekilde hayata geçirme olanağı sunan bir Yazılım Geliştirme Kiti (Software Development Kit, SDK) ile birlikte gönderiliyor. Şunlardan oluşur:

1. Çalışma zamanı ortamını tanımlayan bir SDK ana bilgisayarı (sözde bir sanal alan), yani sistem kaynaklarına (bellek, depolama ve CPU gibi) erişimi kontrol eder ve bunu yaparak doğru ölçeklenebilirliği sağlar
2. ANSI-C'ye benzer bir sözdizimi kullanan ancak bunun üzerine istisnalar, otomatik bellek yönetimi ve çalışma zamanı polimorfizmi desteği ekleyen, gömülü sistemler için optimize edilmiş hafif bir betik dili olan `arena` adlı bir yorumlayıcı dil
3. Donanım arayüzlerine (ör. dijital G/Ç bağlantı noktaları, GPS, harici depolama ortamı, seri bağlantı noktaları) erişmek için kapsamlı bir işlev setiyle birlikte gelen ancak aynı zamanda sistem durum parametrelerini almak, E-posta veya SMS mesajları göndermek veya yalnızca yönlendiriciyi yapılandırmak için bir NetModule AG'ye özgü Uygulama Programlama Arayüzü (API)

C dilinde makul derecede deneyimli olan herkes, kolayca çalışabilecek bir ortam bulacaktır. Ancak lütfen support@netmodule.com adresi üzerinden bizimle iletişime geçmekten çekinmeyin, özel sorununuza uygun bir programlama çözümü bulmanızda size memnuniyetle destek olacağız.

Dil

Arena betik dili, geniş bir POSIX işlevi yelpazesi (`printf` veya `open` gibi) sunar ve özel yapım API işlevleriyle birlikte, favori cihazınızı veya hizmetinizi yönlendiriciyle birbirine bağlamak için her türlü uygulamayı uygulamak için basit bir platform sağlar.

İşte kısa bir örnek:

```
/* We are going to eavesdrop on the first serial port
 * and turn on lights via a digital I / O output port ,
 * otherwise we 'd have to send a short message .
 */
for ( attempts = 0; attempts < 3; attempts ++ ) {
  if ( nb_serial_read ( " serial0 " ) == " Knock Knock ! " ) {
    nb_serial_write ( " serial0 " , " Who 's there ? " ) ;
    if ( nb_serial_read ( " serial0 " ) == " Santa " ) {
      printf ( " Hurray !\n " ) ;
      nb_dio_set ( " out1 " , 1 ) ;
    }
  }
}
nb_sms_send ( " +123456789 " , " No presents this year :( " )
```

Örnek betikler doğrudan yönlendiriciden indirilebilir, bunların bir listesini ekte bulabilirsiniz. NetModule AG destek web sayfasından (<https://support.netmodule.com>) edinilebilen kılavuz, tüm kullanılabilir işlevlerin bir açıklaması da dahil olmak üzere dilin ayrıntılı bir tanıtımını verir.

SDK API İşlevleri

Mevcut API işlevleri aralığı aşağıdaki özellikleri uygulamak için kullanılabilir:

1. SMS Gönder/Al
2. E-posta Gönder
3. Seri cihazdan/cihaza Oku/Yaz
4. Dijital giriş/çıkış portlarını kontrol edin
5. TCP/UDP sunucularını çalıştırın



6. IP/TCP/UDP istemcilerini çalıştırın
7. Takılı medya dosyalarına erişin (ör. bir USB bellek)
8. Sistemden durum bilgilerini alın
9. Yapılandırma parametrelerini alın veya ayarlayın
10. Syslog'a yazın
11. HTTP/FTP üzerinden dosyaları aktarın
12. Yapılandırma/yazılım güncellemelerini gerçekleştirin
13. LED'leri kontrol edin
14. Sistem olaylarını alın, hizmetleri yeniden başlatın veya sistemi yeniden başlatın
15. Kapsama alanındaki ağları tarayın
16. Kendi web sayfalarınızı oluşturun
17. Sesle kontrol işlevleri
18. SNMP işlevleri
19. CAN soket işlevleri
20. Çeşitli ağla ilgili işlevler
21. Diğer sistemle ilgili işlevler

SDK API kılavuzu (yönlendiriciden indirilebilir) bir genel bakış sunar ancak aynı zamanda tüm işlevleri ayrıntılı olarak açıklar. Lütfen bazı işlevlerin SDK'da kullanılmadan önce ilgili hizmetlerin (örn. E-posta, SMS) veya yapılandırılmış arayüzlerin (örn. CAN) düzgün şekilde yapılandırılmasını gerektirdiğini unutmayın.

Şimdi çok güçlü API fonksiyonu `nb_status`'a biraz dikkat edelim. Yönlendiricinin durum değerlerini CLI ile gösterilebildiği şekilde sorgulamak için kullanılabilir. Belirli bir bölüm için değişkenlerin bir yapısını döndürür (mevcut bölümlerin bir listesi `cli status -h` çalıştırılarak elde edilebilir). `Dump` fonksiyonunu kullanarak döndürülen yapının içeriğini anlayabilirsiniz:

```
/* dump current location */  
dump(nb_status("location"));
```

Komut dosyası daha sonra şuna benzer satırlar üretecektir:

```
struct(8): {  
  .LOCATION_STREET = string[11]: "Bahnhofquai"  
  .LOCATION_CITY = string[10]: "Zurich"  
  .LOCATION_COUNTRY_CODE = string[2]: "ch"  
  .LOCATION_COUNTRY = string[11]: "Switzerland"  
  .LOCATION_POSTCODE = string[4]: "8001"  
  .LOCATION_STATE = string[6]: "Zurich"  
  .LOCATION_LATITUDE = string[9]: "47.3778058"  
  .LOCATION_LONGITUDE = string[8]: "8.5412757"  
}
```

`nb_config_set` işleviyle birlikte, durum değişiklikleri üzerine sistemin herhangi bir parçasının yeniden yapılandırılmasını başlatmak mümkündür. Olası bölümleri ve parametreleri CLI ile tekrar sorgulayabilirsiniz:

```
~ $ cli get -c wanlink.0  
cli get -c wanlink.0  
Showing configuration entities (matching 'wanlink.0'):  
wanlink.0.mode           wanlink.0.multipath      wanlink.0.name  
wanlink.0.options        wanlink.0.passthru       wanlink.0.prio  
wanlink.0.suspend        wanlink.0.switchback     wanlink.0.weight
```

CLI'yi etkileşimli moda çalıştırdığınızda, TAB tuşu yardımıyla olası yapılandırma parametreleri arasında adım adım gezinebilirsiniz.

İşte bu fonksiyonların adapte edilmesine dair bir örnek:

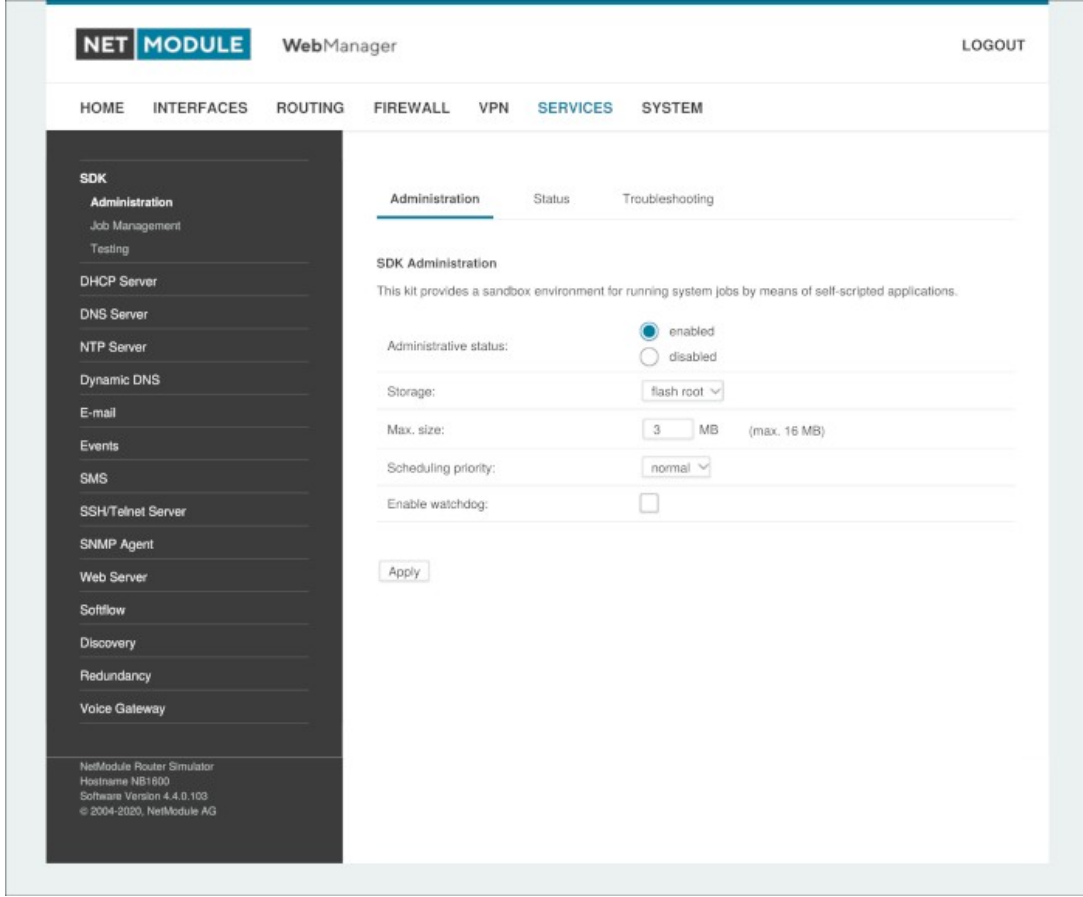
```
/* check current city and enable the second WAN link */  
location = nb_status("location");  
if (location) {  
    city = struct_get(location, "LOCATION_CITY");  
  
    if (city == "Wonderland" ) {  
        for (led = 0; led < 5; led ++ ) {  
            nb_led_set(led, LED_BLINK_FAST | LED_COLOR_RED);  
        }  
    } else {  
        printf("You'll never walk alone in %s ...\n", city);  
        nb_config_set("wanlink .1. mode =1");  
    }  
}
```

SDK'yi Çalıştırmak

SDK'da, işleri oluşturan betikler (`scripts`) ve tetikleyicilerden (`triggers`) bahsediyoruz. Herhangi bir `arena` betiği yönlendiriciye yüklenebilir veya özel kullanıcı yapılandırma paketleri kullanılarak içe aktarılabilir. Ayrıca betiği doğrudan Web Yöneticisi'nde düzenleyebilir veya örneklerimizden birini seçebilirsiniz. Yönlendiricide sözdiziminizi kontrol etmek veya test çalıştırmaları yapmak için kullanılacak bir test bölümünüz daha olacak.

Yükledikten sonra, bir tetikleyici belirtmeniz, yani yönlendiriciye betiğin ne zaman yürütüleceğini söylemeniz gerekecektir. Bu, zaman tabanlı (örneğin her Pazartesi) veya Olaylar bölüm 6.7.7'de açıklandığı gibi önceden tanımlanmış sistem olaylarından biri (örneğin `wan-up`) tarafından tetiklenebilir. Hem betik hem de tetikleyici ile artık sonunda bir SDK işi ayarlayabilirsiniz. `test` olayı genellikle işinizin iyi gidip gitmediğini kontrol etmek için iyi bir olanak görevi görür. Yönetici bölümü ayrıca herhangi bir sorunu gidermek ve çalışan işleri kontrol etmek için olanaklar sunar.

SDK ana bilgisayarını (`sdhost`), betikleri ve işlemlerini yöneten ve böylece sisteme herhangi bir zarar gelmesini önleyen `daemon`'a karşılık gelir. Kaynaklar açısından, betikleri çalıştırmak için CPU ve belleği sınırlayacak ve ayrıca depolama aygıtının kullanılabilir alanının önceden tanımlanmış bir bölümünü sağlayacaktır. Ancak, bunu harici USB depolama veya (modelinize bağlı olarak) genişletilmiş flash depolama ile genişletebilirsiniz. `/tmp`'ye yazılan dosyalar bellekte tutulacak ve betik yeniden başlatıldığında temizlenecektir. Betikleriniz sanal alanda çalıştığından, sistemdeki araçlara (`ifconfig` gibi) erişiminiz olmayacaktır.

Yönetim (Administration)

Ekran 6.41.: SDK Yönetimi

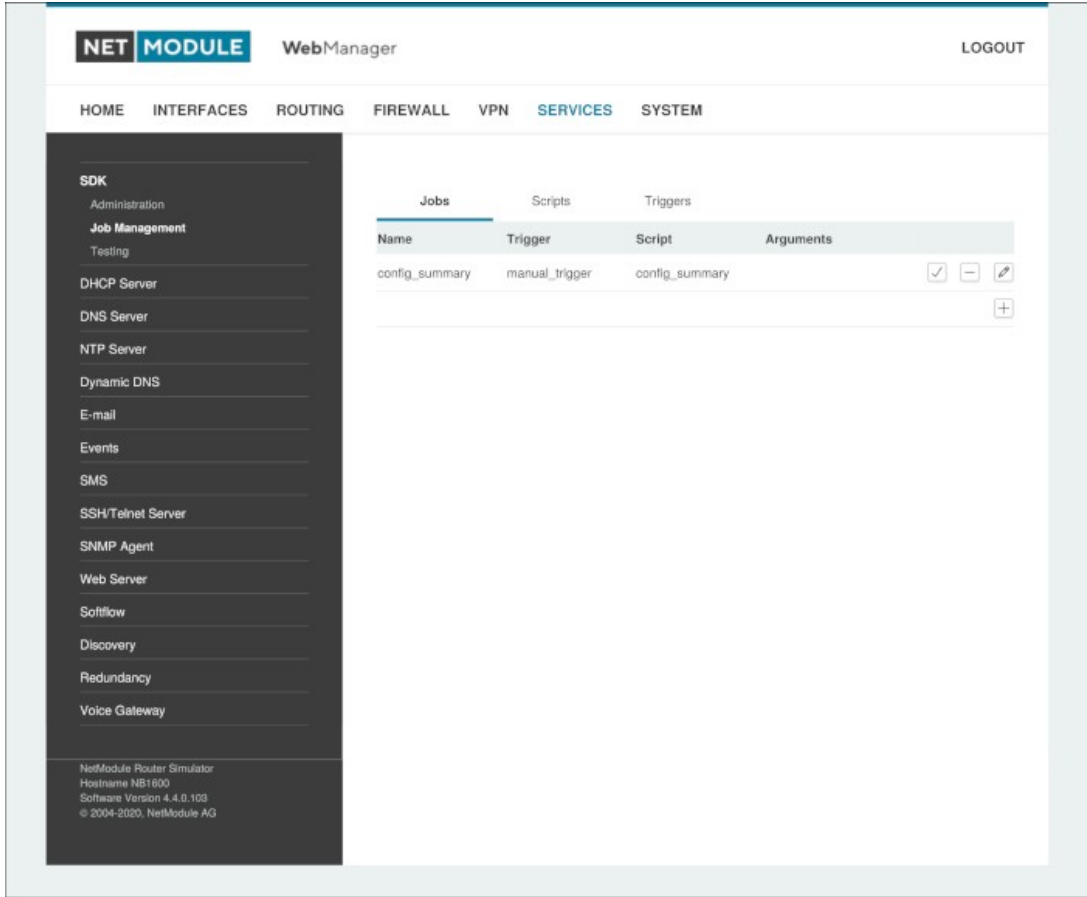
Bu sayfa SDK ana bilgisayarını kontrol etmek ve aşağıdaki ayarları uygulamak için kullanılabilir:

Parametre	SDK Yönetimi Ayarları
Yönetimsel durum (Administrative status)	SDK betiklerinin çalıştırılıp çalıştırılmayacağını belirtir
Depolama (Storage)	Sandbox'ın depolanacağı depolama aygıtı (bkz. bölüm 6.8.1)
Azami büyüklük (Max. size)	Komut dosyalarının depolama aygıtında tüketebileceği maksimum MB miktarı
Planlama önceliği (Scheduling priority)	sdkhost'un işlem önceliğini belirtir, daha yüksek öncelikler betiklerinizin planlanmasını hızlandırır, daha düşük öncelikler ise ana bilgisayar sistemine daha az etki eder
Bekçiyi etkinleştir (Enable watchdog)	Bu seçenek, her bir betik için betik yanıt vermezse veya sıfırdan farklı bir çıkış koduyla durursa sistemin yeniden başlatılmasına yol açan betik denetimini etkinleştirir.

Durum sayfası sizi SDK'nin geçerli durumu hakkında bilgilendirir. Tamamlanmış işler hakkında genel bir bakış sağlar, ayrıca çalışan bir işi orada durdurabilir ve kılavuzları ve örnekleri indirmek için bağlantılar da bulacağınız sorun giderme bölümünde komut dosyası çıktısını görüntüleyebilirsiniz.



İş Yönetimi (Job Management)



Ekran 6.42.: SDK İşleri

Parametre	SDK Tetikleyici Ayarları
Ad (Name)	Tetiği tanımlayan anlamlı bir isim
Tip (Type)	Tetikleyicinin türü, zamana dayalı veya olaya dayalı
Koşul (Condition)	Zaman tabanlı tetikleyiciler için zaman koşulunu belirtir (örneğin saatlik)
Zaman belirteci (Timespec)	Tetiğin çekilmesi gereken zamanı/zamanları belirten koşulla birlikte zaman belirtimi
Olay (Event)	Tetiğin çekilmesi gereken sistem olayı

Artık aşağıdaki parametreleri uygulayarak kişisel betiğinizi sisteme ekleyebilirsiniz:

Parametre	SDK Betik Ayarları
Ad (Name)	Tetiği tanımlayan anlamlı bir isim
Açıklama (Description)	Komut dosyasının isteğe bağlı açıklaması



Parametre	SDK Betik Ayarları
Argümanlar (Arguments)	Komut dosyasına geçirilen isteğe bağlı bir argüman kümesi (tırnak işaretini destekler)
Eylem (Action)	Bir betiği düzenleyebilir, sisteme yükleyebilir veya örnek betiklerden birini veya önceden yüklenmiş bir betiği seçebilirsiniz

Daha sonra bir iş kurmaya hazırsınız, aşağıdaki parametreleri kullanarak bu işi oluşturabilirsiniz:

Parametre	SDK İş Ayarları
Ad (Name)	Mesleği tanımlayan anlamlı bir isim
Tetikleyici (Trigger)	İşin başlatılması gereken tetikleyiciyi belirtir
Betik (Script)	Çalıştırılacak betiği belirtir
Argümanlar (Arguments)	Komut dosyasına geçirilebilecek argümanları tanımlar (tırnak işaretini destekler), bunlar komut dosyasına daha önce atamış olabileceğiniz argümanlardan önce gelir

Yapılandırdığınız her iş doğrudan tetikleyebilirsiniz; bu, test amaçları açısından faydalı olabilir.

Sayfalar

Programlanmış herhangi bir SDK sayfası burada gösterilecektir.

Test

Test sayfası, komut dosyanızın test çalışmalarını gerçekleştirmek veya ayrılmış bölümlerini test etmek veya tüm bir dosyayı yüklemek için kullanılabilir isteğe bağlı argümanlar için bir düzenleyici ve bir giriş alanı sunar. Aksi takdirde boşluklarla ayrılacakları için argümanları tırnak işaretine almanız gerekebileceğini lütfen unutmayın.

```
/* arguments : 'schnick schnack " s c h n u c k "'
for (i = 0; i < argc; i ++ ) {
    printf("argv%d: %s\n", i, argv[i]);
}
/* generates :
*     argv0 : scriptname
*     argv1 : schnick
*     argv2 : schnack
*     argv3 : s c h n u c k
*/
```

Sözdizimi hataları durumunda, **arena** genellikle hata mesajlarını aşağıdaki gibi yazdırır (ayırıştırma hatasının olduğu satırı ve konumu belirtir):

```
/scripts/testrun:2:10:FATAL: parse error, unexpected $, expecting ';''
```



SDK Örnek Uygulama

Giriş olarak, kısa mesajlar üzerinde uzaktan kontrol uygulayan ve sistemin durumunu göndericiye geri göndermek için kullanılabilen SMS kontrol betiği adlı örnek bir uygulamayı inceleyebilirsiniz. Kaynak kodu ekte listelenmiştir. Etkinleştirildiğinde, bir SIM/modemle ilişkili telefon numarasına bir mesaj gönderebilirsiniz. Genellikle ilk satırda bir parola ve ikinci satırda bir komut verilmesi gerekir, örneğin:

```
admin01  
status
```

İstenmeyen erişimi önlemek için kimlik doğrulamayı kullanmanızı şiddetle öneririz, ancak devre dışı bırakmak için noauth'u argüman olarak geçirebilirsiniz. Daha sonra parolayı içeren ilk satırı atlayabilirsiniz. Betiğe daha yakından baktığınızda, izin verilen göndericilerin listesini de kısıtlayabileceğinizi göreceksiniz. Herhangi bir sorun olup olmadığını görmek için lütfen sistem günlüğünü inceleyin.

Aşağıdaki komutlar desteklenmektedir:

Parametre	Eylem
Durum (status)	Kısa bir sistem özeti içeren bir mesajı göndericiye yanıt olarak gönderecektir
Bağlan (connect)	Sistemde yapılandırılan ilk WAN bağlantısını etkinleştirecektir
Bağlantıyı kes (disconnect)	Sistemde yapılandırılan ilk WAN bağlantısını devre dışı bırakacaktır
Yeniden başlat (reboot)	Sistemin yeniden başlatılmasını başlatır
Çıkış 1 açık (output 1 on)	İlk dijital çıkış portunu açar
Çıkış 1 kapalı (output 1 off)	İlk dijital çıkış portunu kapatır
Çıkış 2 açık (output 2 on)	İkinci dijital çıkış portunu açar
Çıkış 2 kapalı (output 2 off)	İkinci dijital çıkış portunu kapatır

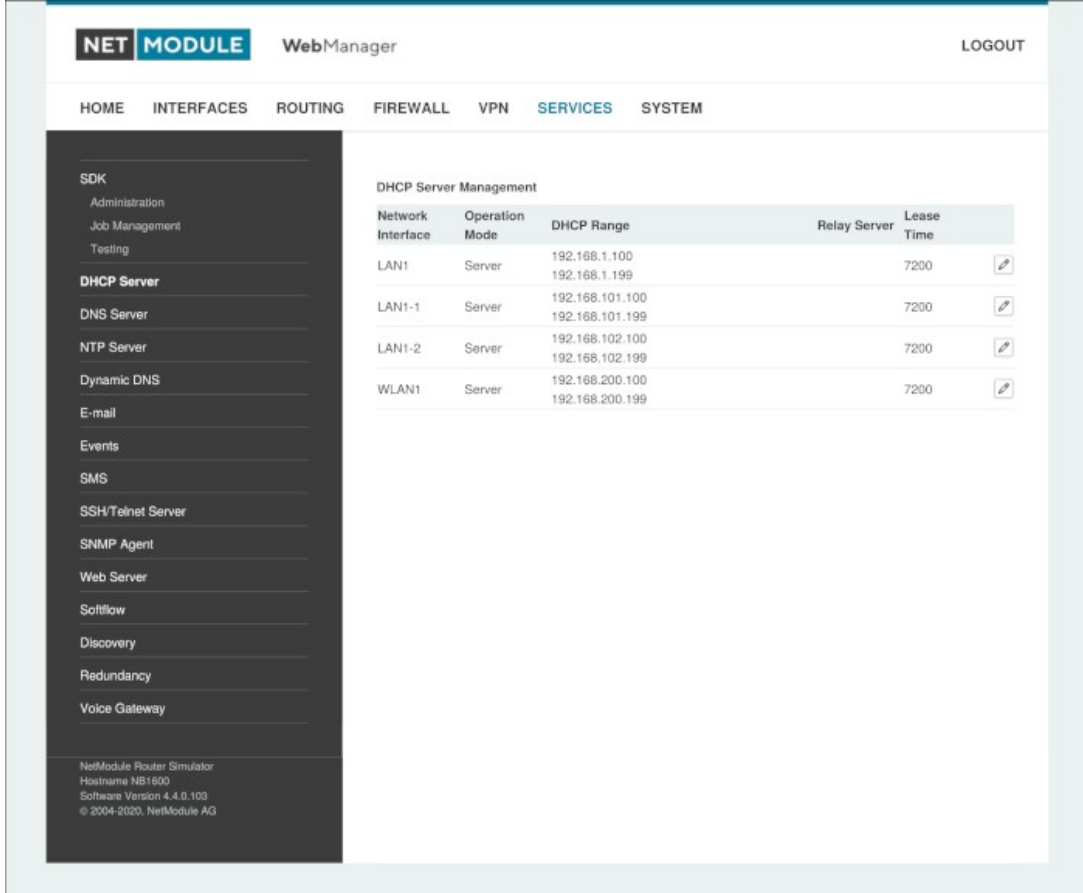
Tablo 6.101.: SMS Kontrol Komutları

Durum komutuna verilen yanıt genellikle şöyle görünür:

```
System: NB2700 hostname (00:11:22:AA:BB:CC)  
WAN1: WWAN1 is up (10.0.0.1, Mobile1, UMTS, -83 dBm, LAI 12345)  
GPS: lat 47.377894, lon 8.540055, alt 282.200  
OVPN: client on tun0 is up (10.0.8.4)  
DIO: IN1=off, IN2=off, OUT1=on, OUT2=off
```

6.7.2. DHCP Sunucu

Bu bölüm, yerel ağdaki ana bilgisayarlara dinamik IP adresleri sunacak her LAN arabirimi için Dinamik Ana Bilgisayar Yapılandırma Protokolü (Dynamic Host Configuration Protocol, DHCP) hizmetini ayrı ayrı yapılandırmak için kullanılabilir. Ayrıca, müzakere edilen istemci adresleri hakkında bir genel bakış bulabileceğiniz durum sayfasına da bakabilirsiniz. Lütfen, bir erişim noktası yapılandırdıysanız WLAN arabirimlerinin (her SSID için) burada da açılacağını unutmayın.



Ekran 6.43.: DHCP Sunucu

Daha sonra her arayüz için aşağıdaki ayarlar uygulanabilir:

Parametre	DHCP Yönetim Ayarları
Çalıştırma modu (Operation mode)	DHCP modunun sunucu, röle veya devre dışı olup olmadığını belirtir

Parametre	DHCP Sunucu Ayarları
İlk kiralık adres (First lease address)	Ana bilgisayarlara verilen IP adresleri aralığındaki ilk adres
Son kiralık adres (Last lease address)	Bu aralığın dışındaki son adres
Kira süresi (Lease duration)	Verilen bir kiralamanın tekrar talep edilmesi gerekene kadar geçerli olacağı saniye sayısı



Parametre	DHCP Sunucu Ayarları
Kalıcı kiralamalar (Persistent leases)	Bu seçeneğin açılmasıyla yönlendirici, yeniden başlatmadan sonra bile verilen kiralamaları hatırlayacaktır. Bu, aynı IP adresinin belirli bir ana bilgisayara atanmasını sağlamak için kullanılabilir.
DHCP seçenekleri (DHCP options)	Varsayılan olarak DHCP, arayüz adresini varsayılan ağ geçidi olarak ve başka türlü yapılandırılmamışsa geçerli DNS sunucu adreslerini dağıtacaktır. Burada sabit adresler belirtebilirsiniz.
Yalnızca statik bilgisayarlara izin ver (Only allow static hosts)	Statik olmayan sunuculardan gelen istekler göz ardı edilecektir.

Parametre	DHCP Seçenekleri
Ağ geçidi adresi (Gateway address)	Varsayılan ağ geçidi adresi
Birincil DNS (Primary DNS)	Birincil ad sunucusu
İkincil DNS (Secondary DNS)	İkincil ad sunucusu
Birincil WINS (Primary WINS)	Birincil WINS sunucusu
İkincil WINS (Secondary WINS)	İkincil WINS sunucusu
Agent ID	Aktarma aracı kimliği (DHCP seçeneği 82)

Parametre	DHCP Röle Ayarları
Birincil röle sunucu (Primary relay server)	Birincil DHCP röle sunucusu
İkincil röle sunucu (Secondary relay server)	İkincil DHCP röle sunucusu

Belirli istemciler için özel kiralama adresleri yapılandırmak da mümkündür.

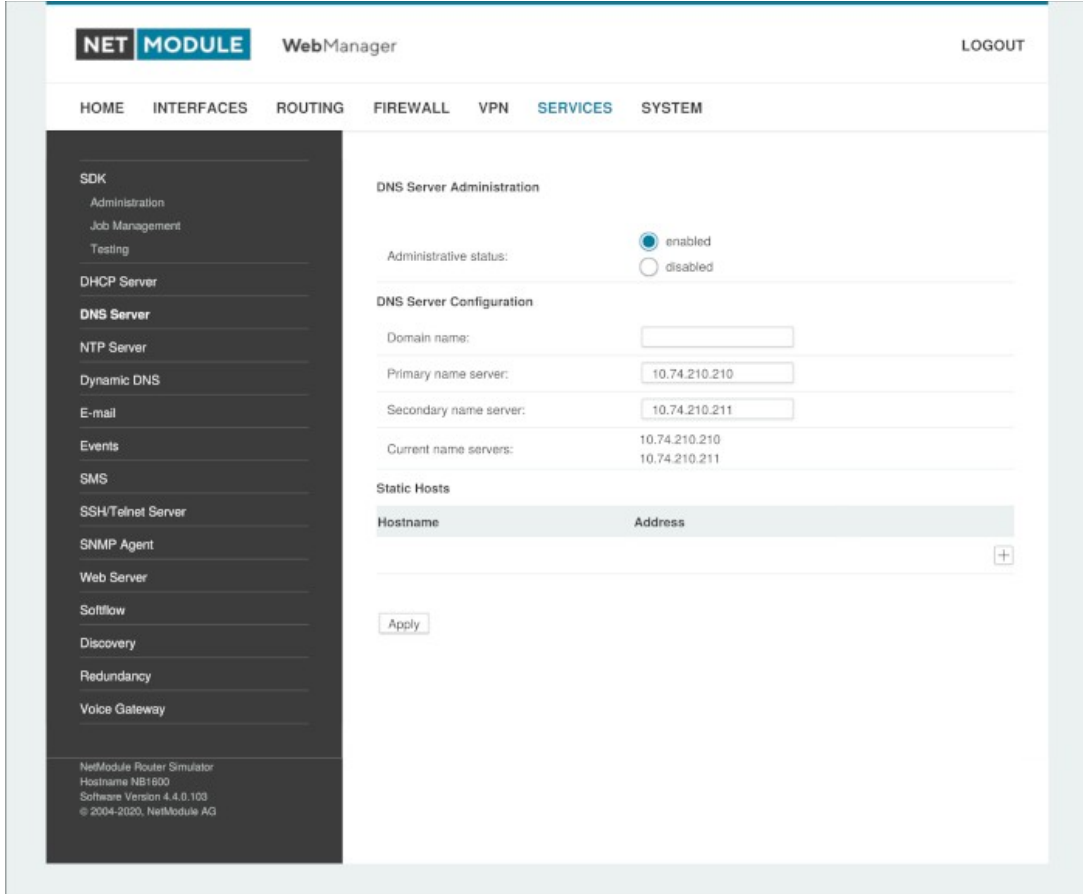
Parametre	DHCP Statik Ana Bilgisayar Ayarları
IP adresi (IP address)	Kiralamanın IP adresi
Tarafından tanımlandı (Identified by)	Müşterinin hangi kriterlere göre tanımlanacağını belirtir
MAC adresi (MAC address)	İstemcinin MAC adresi
Ana bilgisayar adı (hostname)	İstemci tanımlayıcısı (DHCP seçeneği 61)
Port	DHCP isteğinin alındığı Ethernet portu

Özel DHCP seçenekleri aracılığıyla ek DHCP seçenekleri belirtilebilir.

Parametre	DHCP Statik Ana Bilgisayar Ayarları
Anahtar (Key)	Seçenek, ondalık sayı veya "option:<seçenek-adı>" (RFC 2132) olarak gönderilecek
Değer (Value)	Dize olarak gönderilecek ek DHCP seçeneğinin değeri

6.7.3. DNS Sunucu

DNS sunucusu, örneğin WAN bağlantı müzakeresi sırasında müzakere edilmiş olan ağdaki sunuculara DNS isteklerini proxy etmek için kullanılabilir. DNS isteklerini yönlendiriciye yönlendirerek, önceden çözülmüş adları önbelleğe aldığı için giden DNS trafiğini azaltabilir, ancak belirli ana bilgisayar adları için sabit adresler sunmak için de kullanılabilir.



Ekran 6.44.: DNS Sunucu

Aşağıdaki ayarlar uygulanabilir:

Parametre	DNS Sunucu Ayarları
Yönetimsel durum (Administrative status)	DNS sunucusunu etkinleştirir veya devre dışı bırakır
Etki alanı adı (Domain name)	Kısa ad aramaları için kullanılan etki alanı adı
Birincil ad sunucu (Primary name server)	Anlaşmalı ad sunucuları yerine kullanılacak birincil varsayılan ad sunucusu
İkincil ad sunucu (Secondary name server)	Anlaşmalı ad sunucuları yerine kullanılacak ikincil varsayılan ad sunucusu

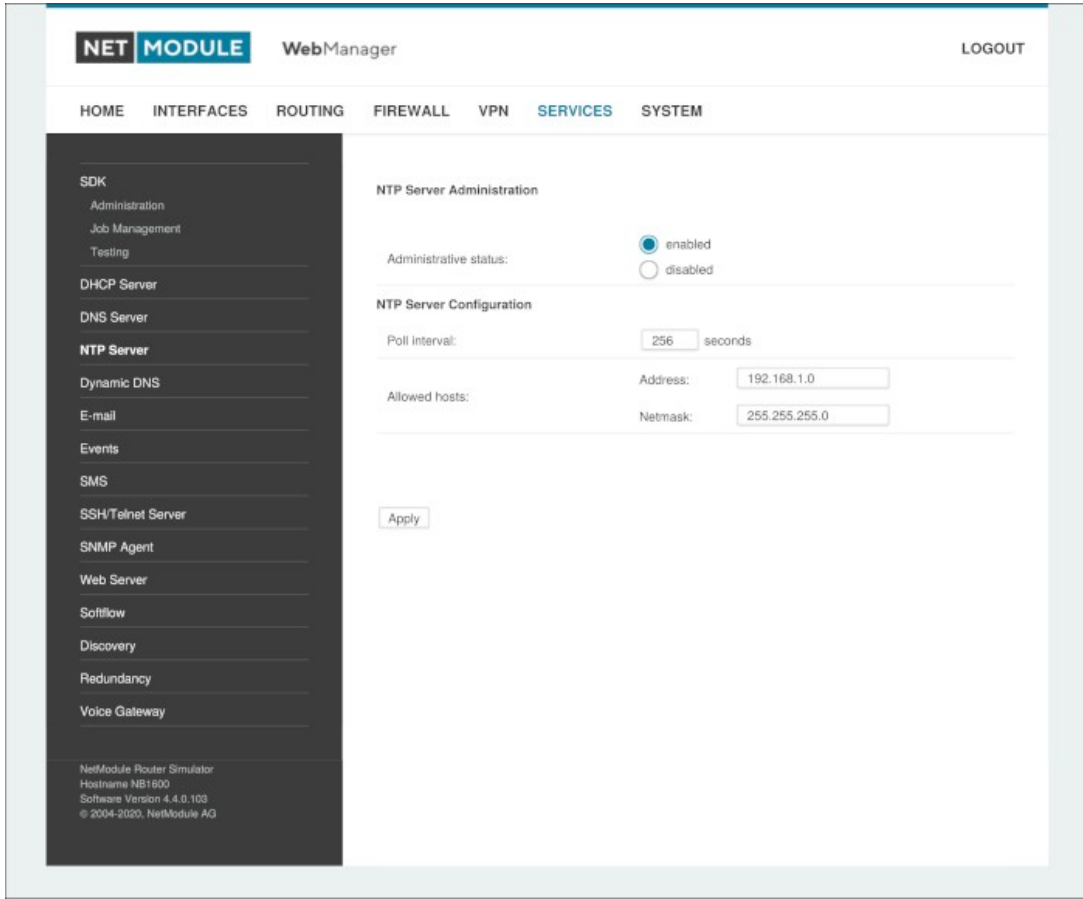
Çeşitli ana bilgisayar adları için sabit IP adresleri sunmak üzere statik ana bilgisayarları daha da yapılandırabilirsiniz.

Parametre	DNS Statik Ana Bilgisayar Ayarları
Adres (Address)	Statik ana bilgisayarın IP adresi
Ana bilgisayar adı (Hostname)	Statik ana bilgisayarın ana bilgisayar adı

Lütfen yerel bilgisayarların DNS aramalarını yönlendiricinin adresine yönlendirmeyi unutmayın.

6.7.4. NTP Sunucu

Bu bölüm, Ağ Zaman Protokolü (Network Time Protocol, NTP) sunucusu işlevini ayrı ayrı yapılandırmak için kullanılabilir.



Ekran 6.45.: NTP Sunucu

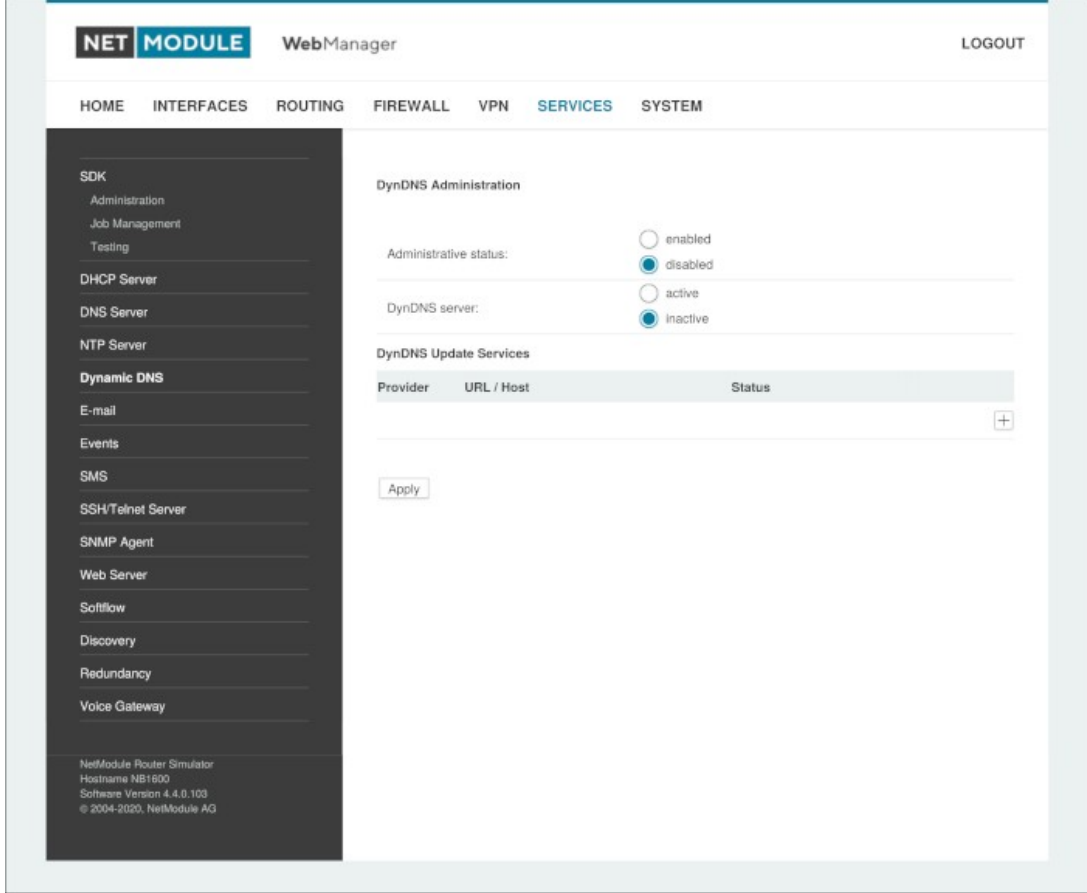
Daha sonra her arayüz için aşağıdaki ayarlar uygulanabilir:

Parametre	NTP Sunucu Ayarları
Yönetimsel durum (Administrative status)	NTP sunucusunun etkin olup olmadığını belirtir
Yoklama aralığı (Poll interval)	Zamanı ana saat sunucularıyla senkronize etmek için yoklama aralığını (64..2048 saniye) tanımlar
İzinli bilgisayarlar (Allowed hosts)	NTP sunucusunu yoklamaya izin verilen IP adresi aralığını tanımlar

Cihazın sistem saatini ayarlamak için 6.8.1'e bakınız.

6.7.5. Dinamik DNS (Dynamic DNS)

Dinamik DNS istemcisi, bir veya birden fazla DynDNS sağlayıcısına sisteminizin geçerli IP adresini söylemek için kullanılabilir. Bu adres, sunucuyla iletişim kurulurken kullanılacak olan geçerli hotlink arayüzünden veya giden arayüzden türetilir. Ayrıca, NAT senaryolarında yararlı olabilecek geçerli İnternet adresini elde etmek için dyndns.org'daki CheckIP servisini istemeyi destekliyoruz. DynDNS istemcisi, bir WAN veya VPN bağlantısı geldiğinde tetiklenecektir.



Ekran 6.46.: Dinamik DNS Ayarları

DynDNS operatörleri için destek sağlıyoruz ancak özel bir güncelleme URL'si tanımlamak da mümkün. NetModule AG yönlendiricinizin, ana bilgisayarlarınızın yönlendiricinin DNS hizmetine işaret etmesi koşuluyla kendi başına DynDNS sunucusu olarak çalışabileceğini lütfen unutmayın. Ayrıca GnuDIP protokolünü ve RFC2136 benzeri dinamik DNS güncellemelerini çalıştırabiliriz. İkincisi genellikle bir TSIG anahtarıyla güvence altına alınır.

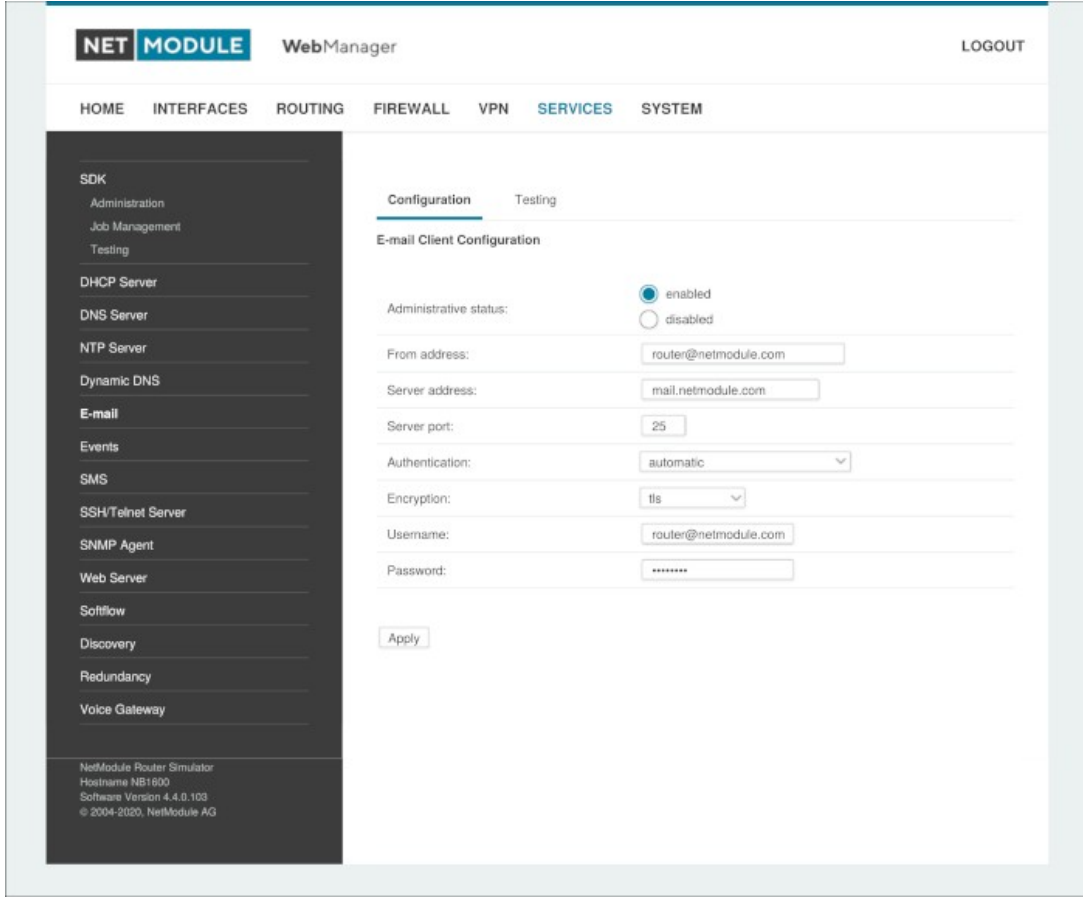


Bir DynDNS hizmeti aşağıdaki parametreleri alabilir:

Parametre	Dinamik DNS Ayarları
Servis sağlayıcı (Provider)	Listelenen sağlayıcılardan birini seçebilir veya özel bir URL sağlayabilirsiniz
Dinamik adres (Dynamic address)	Adresin sıcak bağlantıdan mı yoksa harici bir hizmet aracılığıyla mı türetildiğini belirtir
Ana bilgisayar adı (Hostname)	DynDNS servisinizin sağladığı ana bilgisayar adı (örn. mybox.dyndns.org)
Port	Hizmetin HTTP portu (genellikle 80)
Kullanıcı adı (Username)	Hizmette kimlik doğrulaması için kullanılan kullanıcı adı
Şifre (Password)	Kimlik doğrulama için kullanılan şifre
Protokol (Protocol)	Kimlik doğrulama için kullanılan protokol (HTTP, HTTPS)
Sunucu adresi (Server address)	Güncellenecek sunucunun adresi
Sunucu portu (Server port)	Güncellenecek sunucunun portu
TSIG anahtar adı (TSIG key name)	Güncellemeleri gerçekleştirmeye izin verilen TSIG anahtarının adı
TSIG anahtarı (TSIG key)	Base64'te kodlanmış TSIG anahtarı

6.7.6. E-Posta (E-Mail)

E-posta istemcisi, belirli olaylar veya SDK komut dosyaları aracılığıyla belirli bir E-posta adresine bildirim göndermek için kullanılabilir.



Ekran 6.47.: E-Posta Ayarları

Aşağıdaki ayarları uygulayarak etkinleştirilebilir.

Parametre	E-Posta İstemcisi Ayarları
E-posta istemci durumu (E-mail client status)	E-posta istemcisinin idari durumu
Gönderen e-posta adresi (From e-mail address)	Gönderenin e-posta adresi
Sunucu adresi (Server address)	SMTP sunucunun adresi
Sunucu portu (Server port)	SMTP sunucunun portu (genellikle 25)
Kimlik doğrulama yöntemi (Authentication method)	SMTP sunucusuna karşı kimlik doğrulaması için kullanılacak gerekli kimlik doğrulama yöntemini seçin
Şifreleme (Encryption)	Şifrelemeyi seçin. STARTTLS veya hiçbiri olabilir.
Kullanıcı adı (Username)	Kimlik doğrulama için kullanılan kullanıcı adı
Şifre (Password)	Kimlik doğrulama için kullanılan kullanıcı şifresi



6.7.7. Etkinlikler (Events)

Etkinlik yöneticisini kullanarak uzak sistemlerdeki olaylar hakkında bilgilendirebilirsiniz. E-posta, SMS veya SNMP tuzakları kullanılarak bir bildirim gönderilebilir.

Parametre	Etkinlik Bildirim Ayarları
E-posta adresi (E-Mail address)	Bildirim gönderileceği E-posta adresi (E-posta istemcisinin etkinleştirilmiş olması gerekir)
Telefon numarası (Phone number)	Bildirim gönderileceği telefon numarası (SMS servisinin açık olması gerekmektedir)
SNMP ana bilgisayar (SNMP host)	Tuzağın gönderileceği SNMP ana bilgisayar veya adresi
SNMP portu (SNMP port)	Uzak SNMP hizmetinin portu
Kullanıcı adı (Username)	Uzaktan SNMP hizmetine erişim için kullanıcı adı
Şifre (Password)	Uzaktan SNMP hizmetine erişim için kullanıcı şifresi
Kimlik doğrulama (Authentication)	Uzaktan SNMP hizmetine erişim için kimlik doğrulama algoritması (MD5 veya SHA)
Şifreleme (Encryption)	Uzak SNMP hizmetine erişim için şifreleme algoritması (DES veya SHA)
Motor kimliği (Engine ID)	Uzak SNMP hizmetinin motor kimliği

Mesajlar sizin tarafınızdan sağlanan bir açıklama ve kısa bir sistem bilgisi içerecektir. Tüm sistem olaylarının bir listesi ek A.2'de bulunabilir.

6.7.8. SMS

Yönetim (Administration)

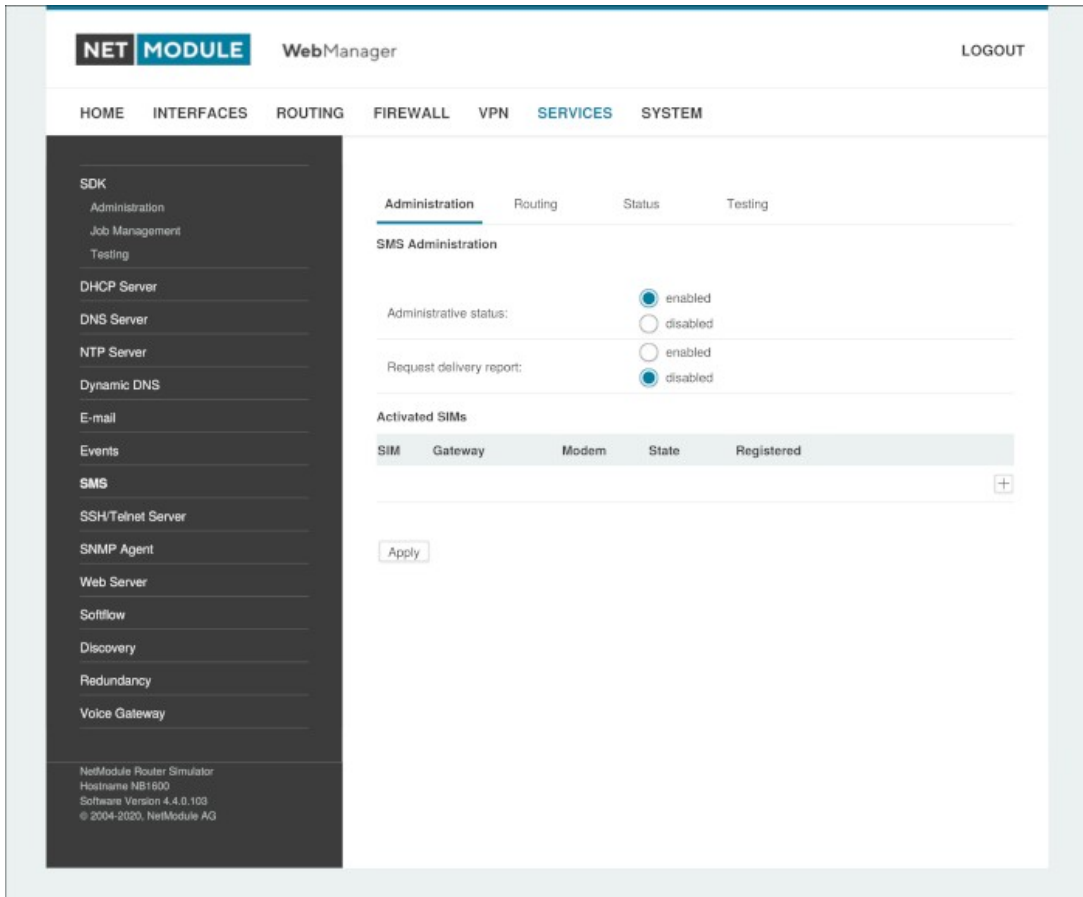
NetModule AG yönlendiricileri, SIM sağlayıcınız tarafından etkinleştirilmişse kısa mesajlar (SMS) alabilir veya gönderebilir. Mesajlar, bir SIM'e atanmış modem tarafından alınır/gönderilir, bu nedenle 6.3.3. bölümde açıklandığı gibi SMS yeteneğine sahip varsayılan bir modemi düzgün bir şekilde yapılandırmanız gerekir.

Aynı SIM'i paylaşan birden fazla WWAN arabirimi çalıştırıyorsanız sistemin SIM'leri değiştirebileceğini lütfen unutmayın. Bu nedenle, iletişim için farklı bir modem kullanılması veya SIM atanmamışsa herhangi bir işlemin durması söz konusu olabilir.

Lütfen modemlerin, başka ücretlerin uygulanabileceği yabancı ağlara dolaşımı kaydedebileceğini unutmayın. Mobil SIM'ler bölümünde (bkz. 6.3.3) sabit bir ağ (PLMN ile) manuel olarak atayabilirsiniz.

Mesaj gönderme büyük ölçüde modem kayıt durumuna ve sağlanan SMS Merkezi hizmetinin çalışıp çalışmamasına bağlıdır ve başarısız olabilir. Bir mesajın başarıyla gönderilip gönderilmediğini anlamak için `sms-report-received` olayını kullanabilirsiniz.

Alınan mesajlar SIM'lerden çekilir ve geçici olarak yönlendiricide saklanır ancak sistem yeniden başlatıldıktan sonra temizlenir. Bunları işlemek veya kopyalamak isterseniz lütfen bir SDK betiğine danışmayı düşünün.



Ekran 6.48.: SMS Yapılandırma

İlgili sayfa, SMS hizmetini etkinleştirmek ve hangisinde çalışması gerektiğini belirtmek için kullanılabilir. SIM'leri IMEI numaralarına göre tanımlarız ve istatistiklerini uçucu olmayan bir şekilde izleriz.



Parametre	SMS SIM Ayarları
SMS ađ geidi (SMS Gateway)	Kısa mesaj gndermek iin servis merkezi numarası. Genellikle SIM kartınızdan otomatik olarak alınır ancak burada sabit bir numara tanımlayabilirsiniz.

Ynlendirme ve Filtreleme (Routing & Filtering)

SMS ynlendirmeyi kullanarak, mesajlar gnderildiđinde uygulanacak giden kuralları belirleyebilirsiniz. Bir yandan, bunları etkinleřtirilmiř bir modeme iletebilirsiniz. Belirli bir numara iin, rneđin mesajların zel bir SIM zerinden gnderilmesini zorunlu kılabilirsiniz. Telefon numaraları ayrıca dzenli ifadelerle de belirtilebilir, iřte bazı rnekler:

Numara	Sonuç
+12345678	Sabit bir sayı belirtir
+1*	+1 ile bařlayan herhangi bir sayıyı belirtir
+1*9	+1 ile bařlayıp 9 ile biten herhangi bir sayıyı belirtir
+ [12]*	+1 veya 2 ile bařlayan herhangi bir sayıyı belirtir

Tablo 6.113.: SMS Numara İfadeleri

Ltfen numaraların geerli bir nek ieren uluslararası formatta girilmesi gerektiđini unutmayın. te yandan, rneđin pahalı bir hizmet veya uluslararası numara kullanmaktan kaınmak istediđinizde, giden mesajları dřrmek iin kurallar da tanımlayabilirsiniz.

Her iki kural tr de bir liste oluřturur ve sırayla iřlenir, giden mesajlar belirtilen modem zerinden iletilir veya dřrlr. Ařađıdaki kurallardan hibirine uymayan mesajlar ilk kullanılabilir modeme gnderilir.

Filtreleme, gelen mesajları gvenlik duvarı kavramına hizmet eder, bylece her modem iin dřrlr veya izin verilir. Oluřturulan kurallar sırayla iřlenir ve eřleřme olması durumunda sisteme girmeden nce gelen mesajı dřrr veya iletir. Eřleřmeyen tm mesajlara izin verilir.

Durum

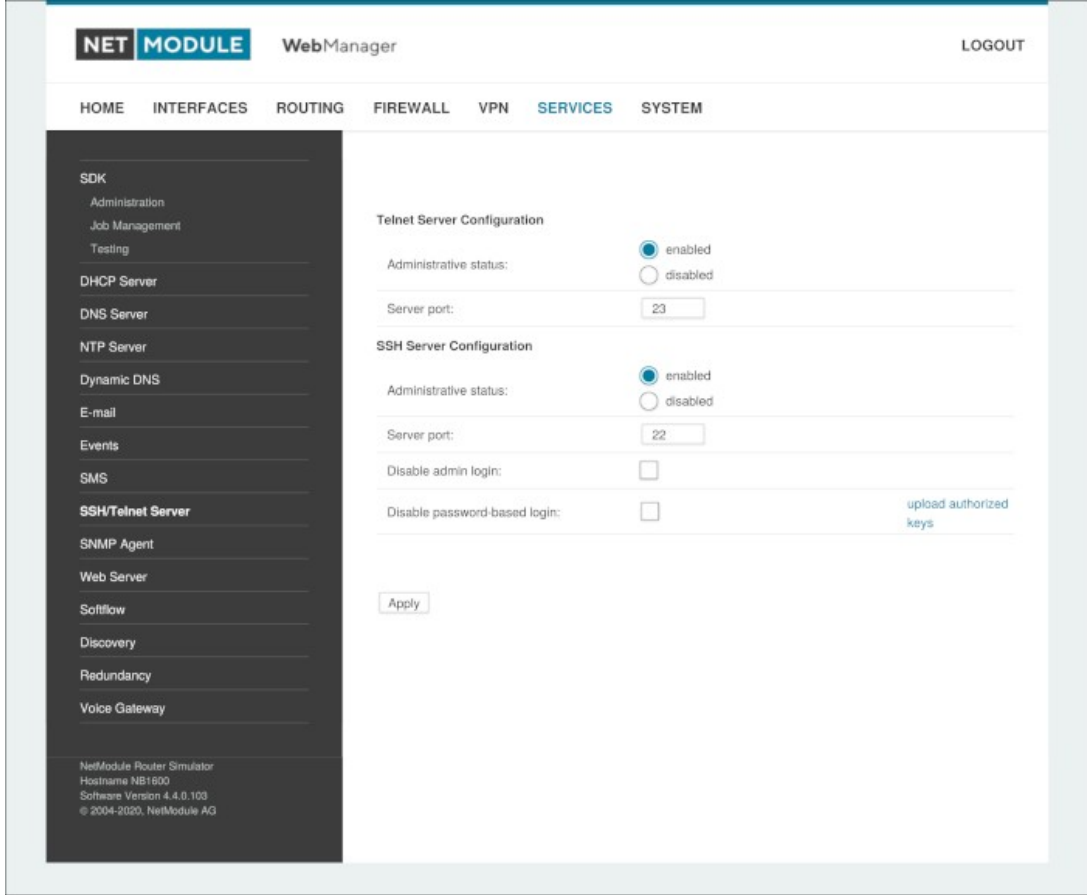
Durum sayfası, mevcut modem durumunu grntlemek ve gnderilen veya alınan mesajlar hakkında bilgi almak iin kullanılabilir. Mesajları grntlemek veya silmek iin kullanılabilen kk bir SMS gelen kutusu okuyucusu vardır. Ltfen gelen kutusunun 512 kByte flash kullanımını ařması durumunda her gece yarısı temizleneceđini unutmayın.

Test

Bu sayfa, genel olarak SMS gnderiminin veya filtreleme/ynlendirme kurallarının alıřıp alıřmadıđını test etmek iin kullanılabilir. Mesaj parası bařına maksimum uzunluk 160 karakterle sınırlıdır, ayrıca yalnızca GSM 7 bit alfabesi tarafından desteklenen karakterleri kullanmanızı neririz.

6.7.9. SSH/Telnet Sunucu

Web Yöneticisi dışında, sisteme giriş yapmak için SSH ve Telnet servisleri kullanılabilir. Geçerli kullanıcılar arasında root ve admin ve Kullanıcı Hesapları bölümünde oluşturulabilecek ek kullanıcılar bulunur. Lütfen unutmayın, normal bir sistem kabuğu yalnızca root kullanıcısı için sağlanacaktır, CLI diğer tüm kullanıcılar için başlatılacaktır, normal kullanıcılar ise yalnızca durum değerlerini görüntüleyebilecektir, admin kullanıcısı sistemi değiştirmek için ayrıcalıklar elde edecektir.



Ekran 6.49.: SSH ve Telnet Sunucu

Bu servislerin WAN arayüzünden de erişilebilir olacağını unutmayın. Şüphenez varsa, lütfen geçerli güvenlik duvarı kurallarını uygulayarak bunlara erişimi devre dışı bırakmayı veya kısıtlamayı düşünün. Telnet servisine aşağıdaki parametreler uygulanabilir:

Parametre	Telnet Sunucu Ayarları
Yönetimsel durum (Administrative status)	Telnet hizmetinin etkin mi yoksa devre dışı mı olduğu
Sunucu portu (Server port)	Hizmetin TCP portu (genellikle 23)



SSH servisine aşağıdaki parametreler uygulanabilir:

Parametre	SSH Sunucu Ayarları
Yönetimsel durum (Administrative status)	SSH hizmetinin etkin mi yoksa devre dışı mı olduğu
Sunucu portu (Server portu)	Hizmetin TCP portu (genellikle 22)
Yönetici girişini kapat (Disable admin login)	Yönetici kullanıcıları için oturum açmayı devre dışı bırak
Şifre bazlı girişi kapat (Disable password-based login)	Bu seçeneği aktif hale getirdiğinizde tüm kullanıcıların yönlendiriciye yüklenebilen SSH anahtarları ile kimlik doğrulaması yapması gerekecektir.



6.7.10. SNMP Ajanı (SMNP Agent)

NetModule AG yönlendiricileri, temel MIB tablolarını (ifTable gibi) ve birden fazla sistemi yönetmek için ek kurumsal MIB'leri destekleyen bir SNMP daemon'u ile donatılmıştır.

Parametre	Desteklenen MIB'ler
.1.3.6.1.2.1	MIB-II (RFC1213), SNMPv2-MIB (RFC3418)
.1.3.6.1.2.1.2.1	IF-MIB (RFC2863)
.1.3.6.1.2.1.4	IP-MIB (RFC1213)
.1.3.6.1.2.1.10.131	TUNNEL-MIB (RFC4087)
.1.3.6.1.2.25	HOST-RESOURCES-MIB (RFC2790)
.1.3.6.1.6.3.10	SNMP-FRAMEWORK-MIB
.1.3.6.1.6.3.11	SNMPv2-SMI (RFC2578)
.1.0.8802.1.1.2	LLDP-MIB
.1.0.8802.1.1.2.1.5.4795	LLDP-EXT-MED-MIB
.1.3.6.1.4.1.31496	VENDOR-MIB

VENDOR-MIB tabloları sistem ve WWAN, GNSS ve WLAN arayüzleri hakkında bazı ek bilgiler sunar. Bunlara aşağıdaki OID'ler üzerinden erişilebilir:

Parametre	Üretici MIB OID Atama
NBAdminTable	.1.3.6.1.4.1.31496.10.40
NBWwanTable	.1.3.6.1.4.1.31496.10.50
NBGnssTable	.1.3.6.1.4.1.31496.10.51
NBDioTable	.1.3.6.1.4.1.31496.10.53
NBWlanTable	.1.3.6.1.4.1.31496.10.60
NBWanTable	.1.3.6.1.4.1.31496.10.22

Şunlar için olanaklar sunarlar:

- Cihazı yeniden başlatma
- FTP/TFTP/HTTP aracılığıyla yeni bir sistem yazılımına güncelleme
- FTP/TFTP/HTTP aracılığıyla yeni bir sistem yapılandırmasına güncelleme
- WWAN/GNSS/WLAN/DIO bilgilerini alma

VENDOR-MIB'imiz ekte listelenmiştir veya doğrudan yönlendiriciden indirilebilir.



SNMP Yapılandırma (SNMP Configuration)

The screenshot shows the NET MODULE WebManager interface. The top navigation bar includes 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. The 'SERVICES' tab is active. The left sidebar lists various services, with 'SNMP Agent' highlighted. The main content area displays the 'SNMP Agent Configuration' page. It has two tabs: 'Configuration' and 'Authentication'. The 'Configuration' tab is active. The settings are as follows:

- Administrative status: enabled, disabled
- Operation mode: v1 | v2c | v3, v3 only
- Contact:
- Location:
- Listening port:

There is an 'Apply' button at the bottom left and a 'Download MIB' link at the bottom right. The footer of the interface reads: 'NetModule Router Simulator, Hostname: NB1800, Software Version: 4.4.0.104, © 2004-2020, NetModule AG'.

Ekran 6.50.: SNMP Ajanı

Parametre	SNMP Yapılandırma
Yönetimsel durum (Administrative status)	SNMP aracısını etkinleştirin veya devre dışı bırakın
Çalışma modu (Operation mode)	Aracının uyumluluk modunda mı yoksa yalnızca SNMPv3 için mi çalışması gerektiğini belirtir
İrtibat (Contact)	Sistem bakımıcısı veya diğer iletişim bilgileri
Konum (Location)	Cihazın konumu
Dinleme portu (Listening port)	SNMP ajanı port

SNMP aracısı etkinleştirildikten sonra, SDK betikleri kullanılarak SNMP tuzakları oluşturulabilir.



SNMP Kimlik Doğrulama (SNMP Authentication)

SNMPv3'te çalışırken, aşağıdaki kimlik doğrulama ayarlarını yapılandırmak mümkündür:

Parametre	SNMPv3 Kimlik Doğrulama
Kimlik doğrulama (Authentication)	Kimlik doğrulamayı tanımlar (MD5 veya SHA)
Şifreleme (Encryption)	Kullanılacak gizlilik protokollerini tanımlar (DES veya AES)

Genel olarak, yönetici kullanıcısı herhangi bir değeri okuyabilir ve yazabilir. Diğer tüm sistem kullanıcılarına okuma erişimi verilecektir. SNMPv1/v2c'de kimlik doğrulama/şifreleme yoktur ve herhangi bir değer ayarlamak için kullanılmamalıdır. Ancak, yönetim erişimi verilecek topluluklarını ve yetkili ana bilgisayarını tanımlamak mümkündür.

Parametre	SNMPv1/v2 Kimlik Doğrulama
Okuma iznli topluluk (Read community)	Okuma erişimi için topluluk adını tanımlar
Yönetici iznli topluluk (Admin community)	Yönetici erişimi için topluluk adını tanımlar
İzinli ana bilgisayar (Allowed host)	Yönetici erişimine izin verilen ana bilgisayarı tanımlar

SNMP şifrelerinin 8 karakterden uzun olması gerektiğine dikkat edilmelidir. Daha kısa şifreler SNMP için iki katına çıkar (örneğin admin01, admin01admin01 olur).

SNMP'de parola ifadelerinin kullanılması nedeniyle, SNMP sunucusuna karşı kimlik doğrulaması yapabilecek kullanıcıların şifrelerinin saklanması zorunludur. Daha fazla bilgi için lütfen 6.8.2 bölümüne bakın. SNMP daemon'unun WAN arayüzlerini de dinlediğini ve bu nedenle güvenlik duvarıyla erişimi kısıtlamanın önerildiğini lütfen unutmayın.

Tipik SNMP Komutları

MIB değerlerini ayarlamak ve uzantıları tetiklemek genellikle SNMPv3 yönetici kullanıcısıyla sınırlıdır. SNMP v1/2c için bir yönetici ana bilgisayarını belirtmek mümkündür. SNMP uzantıları aşağıdaki gibi okunabilir ve tetiklenebilir:

Sistemin yazılım sürümünü edinme:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.1.0
```

Çekirdek sürümünü alma:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.2.0
```

Seri numarasını alma:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.3.0
```

Mevcut yapılandırma açıklamasını alıyorum:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.4.0
```

Mevcut yapılandırma karmasını alıyoruz:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.5.0
```



Cihazı yeniden başlatma:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.10.0 i 1
```

Yapılandırma güncellemesi başlatma:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.11.0 s "http://server/directory"
```

TFTP, HTTP, HTTPS ve FTP URL'lerini kullanabilirsiniz (bir kullanıcı adı/şifre veya bir port belirtmek henüz desteklenmiyor). Lütfen yapılandırma güncellemelerinin belirtilen dizinde <seri-numarası>.zip adlı bir zip dosyası beklediğini unutmayın.

Yapılandırma güncelleme durumunu alma:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.12.0
```

Dönüş değeri şunlardan biri olabilir: başarılı(succeeded) (1), başarısız(failed) (2), devam ediyor(inprogress)(3), başlatılmadı(notstarted)(4).

Yazılım güncellemesi çalıştırma:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.13.0 s "http://server/directory"
```

Yazılım güncelleme durumunu alma:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.14.0
```

Dönüş değeri şunlardan biri olabilir: başarılı(succeeded) (1), başarısız(failed) (2), devam ediyor(inprogress)(3), başlatılmadı(notstarted)(4).

Güncelleme işleminin ayarlanması:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.15.0 i 1
```

Varsayılan olarak, güncelleme işlemi tetiklendiğinde yazılım veya yapılandırmanın anında güncellenmesiyle sonuçlanan güncelleme(update) (0) olarak ayarlanır. Ayrıca, işlem yalnızca yazılımı veya yapılandırma paketini depolayacak olan depola(store) (1) olarak da ayarlanabilir. Daha sonra aşağıdaki anahtar operatörleri kullanılarak etkinleştirilebilir.

**Alternatif bir yazılıma geçiş:**

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.16.0 i 0
```

Dönüş değeri yazılım güncelleme durumundan türetilebilir.

Alternatif yapılandırmaya geçiliyor:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.16.0 i 1
```

Dönüş değeri yapılandırma güncelleme durumundan türetilebilir.

Alternatif yapılandırma açıklamasını alma:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.17.0
```

Alternatif yapılandırma karmasını alma::

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.18.0
```

Alternatif yazılım sürümünü edinme:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.19.0
```

Alternatif yazılım karma değerini elde etmek:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
1.3.6.1.4.1.31496.10.40.20.0
```

Dijital OUT1'in ayarlanması:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.10.0 i 0  
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.10.0 i 1
```

Dijital OUT2'nin ayarlanması:

```
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.11.0 i 0  
snmpset -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.3.6.1.4.1.31496.10.53.11.0 i 1
```

Bulunan cihazların listelenmesi:

```
snmpget -v 3 -u admin -n "" -l authNoPriv -a MD5 -x DES -A admin01admin01 192.168.1.1  
.1.0.8802.1.1
```



6.7.11. Let's Encrypt

Bu hizmet, Let's Encrypt tarafından sağlanan PKI'yi kullanarak yönlendiricinin web arayüzü için otomatik olarak TLS sertifikaları vermenizi sağlar. HTTPS etkinleştirilirse, Let's Encrypt etkinleştirilirse web arayüzü otomatik olarak Let's Encrypt sertifikasını kullanır. Let's Encrypt sertifikaları verebilmek ve kullanabilmek için aşağıdaki ön koşulların karşılandığından emin olun:

- HTTP ve HTTPS, web sunucusunda standart 80 ve 443 portlarında etkinleştirilmelidir
- Yönlendirici, Let's Encrypt için yapılandırılmış alan adı kullanılarak TCP 80 ve 443 portları üzerinden internette erişilebilir olmalıdır

Let's Encrypt bileşeni etkinleştirilir etkinleştirilmez, yapılandırılan alan için otomatik olarak bir sertifika istemeye başlar. Ayrıca, sertifikanın yenilenmesi gerekip gerekmediğini günde bir kez kontrol eder ve gerekirse yeni bir sertifika ister.

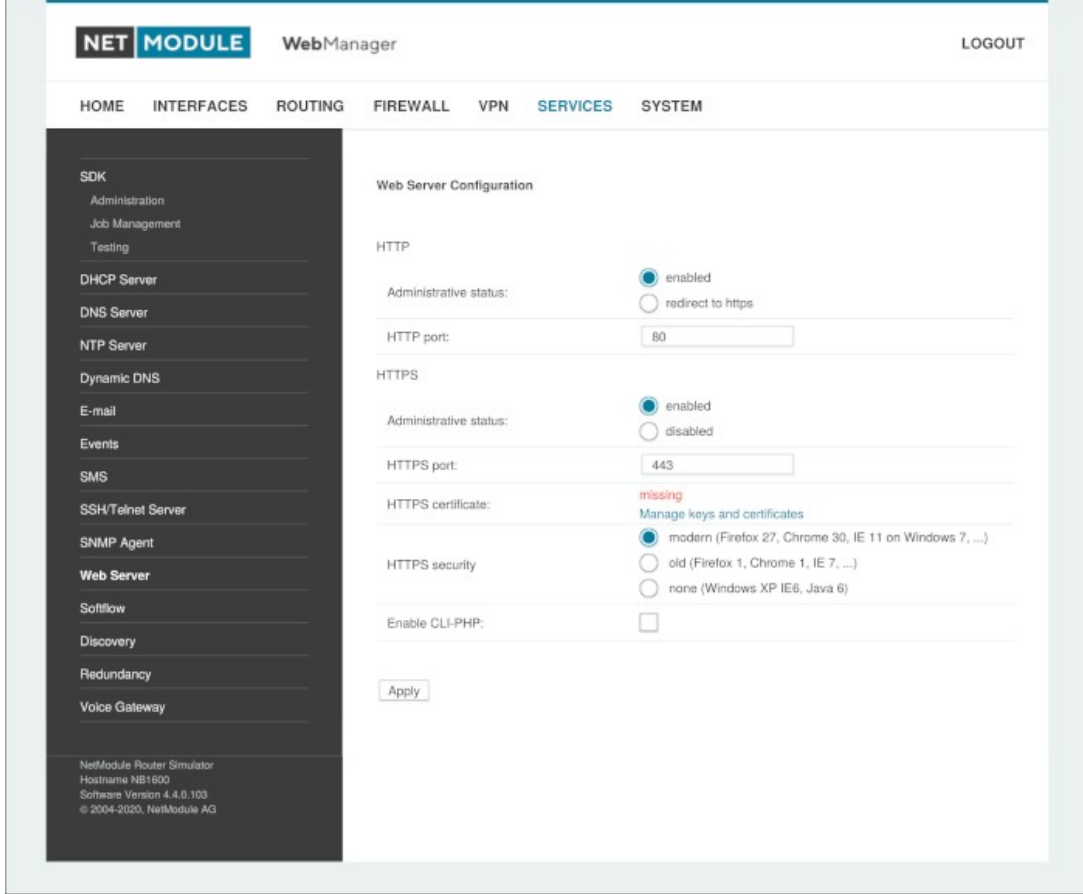
Parametre	Let's Encrypt Ayarları
Etkinleştir (Enable)	Bileşeni etkinleştirir/devre dışı bırakır
Etki alanı (Domain)	Sertifika talebinde bulunulacak alan adı
Sertifika durumu (Certificate state)	Sertifikanın yüklü olup olmadığını veya eksik olup olmadığını ya da devrede olup olmadığını gösterir
Sertifika geçerlilik süresi (Certificate valid not before)	Yüklenen sertifikanın geçerliliğinin başladığı zaman
Sertifikanın geçerliliğinin sona erdiği tarih (Certificate valid not after)	Yüklü sertifikanın geçerliliğinin sona erdiği zaman
Sertifikayı yenile (Renew Certificate)	Sertifikanın yenilenmesini manuel olarak talep etmenize olanak tanır. Bunun yalnızca yenileme zamanı geldiğinde işe yaradığını unutmayın.
Sertifikayı sil (Delete Certificate)	Yüklü sertifikayı silin. Bu yalnızca Let's Encrypt devre dışı bırakıldığında kullanılabilir.

Hata ayıklama için CLI'da sertifikaları talep eden ACME istemcisinin günlüğünü gösteren tail-scripts komutunu kullanabilirsiniz. Ya da son sertifika talebinin günlüğünü şu dosyada bulabilirsiniz:

```
/etc/acme/<DOMAIN>/issue.log
```

6.7.12. Web Sunucu (Web Server)

Bu sayfa, Web Yöneticisine HTTP/HTTPS üzerinden erişmek için farklı portları yapılandırmak için kullanılabilir. WAN arayüzü üzerinden web hizmetine erişirken HTTPS kullanmanızı şiddetle öneririz çünkü iletişim şifrelenecek ve böylece sistemin kötüye kullanılması önlenecektir. HTTPS'yi etkinleştirmek için 6.8.8 bölümünde bir sunucu sertifikası oluşturmanız veya yüklemeniz gerekir.



Ekran 6.51.: Web Sunucu

Parametre	Web Sunucu Ayarları
Yönetimsel durum (Administrative Status)	Web sunucusunu etkinleştirin veya devre dışı bırakın
HTTP port	HTTP bağlantıları için web sunucusu bağlantı noktası
HTTPS port	HTTPS bağlantıları için web sunucusu bağlantı noktası
CLI-PHP'yi etkinleştir (Enable CLI-PHP)	CLI-PHP hizmetini etkinleştirin (bkz. bölüm 7.17)



6.7.13. MQTT Broker

MQTT Broker, MQTT istemcileri arasında MQTT iletilerini dağıtmak için kullanılabilir. MQTT Broker'a erişimi kısıtlamak istiyorsanız lütfen uygun güvenlik duvarı kurallarını ayarlayın. TLS şifrelemesi için anahtarlar ve sertifikalar Anahtarlar ve Sertifikalar aracılığıyla yönetilir (bkz. bölüm 6.8.8). MQTT Broker hizmeti aşağıdaki parametreleri alabilir:

Parametre	MQTT Broker Ayarları
Yönetimsel durum (Administrative Status)	Hizmeti etkinleştirin veya devre dışı bırakın
Port	Dinlenecek ağ bağlantı noktasını belirtir
TLS Şifreleme (TLS Encryption)	Hizmet için TLS şifrelemesini etkinleştirir veya devre dışı bırakır



6.7.14. Softflow

Bu sayfa, NetFlow trafik verilerini dışarı aktarmak için kullanılan ağ trafiği analizörü daemon softflowd'u yapılandırmak için kullanılabilir.

Parametre	Softflow Ayarları
Arayüz (Interface)	Trafiği dinlemek için arayüz
Ana bilgisayar adresi (Host Address)	Trafik verilerinin hedef adresi
Port	Hedef adresin limanı
Protokol versiyonu (Protocol Version)	Verilerin protokol versiyonu
Azami akış sayısı (Maximum Flows)	Eşzamanlı olarak izlenecek maksimum akış sayısı
İzleme seviyesi (Track Level)	Bir akışı tanımlamak için kullanılması gereken akış elemanları
Örnek oranı (Sample Rate)	Periyodik örnekleme oranı



6.7.15. Keşif (Discovery)

Bu sayfa, diğer ana bilgisayarları keşfetmek ve onlar tarafından keşfedilmek için kullanılacak keşif protokollerini etkinleştirmek için kullanılabilir.

Parametre	Keşif Ayarları
Yönetimsel durum (Administrative status)	Yönetimsel durum
Etkinleştirilmiş protokoller (Enabled protocols)	Etkinleştirilmiş keşif protokollerinin listesi

Aşağıdaki protokoller desteklenmektedir:

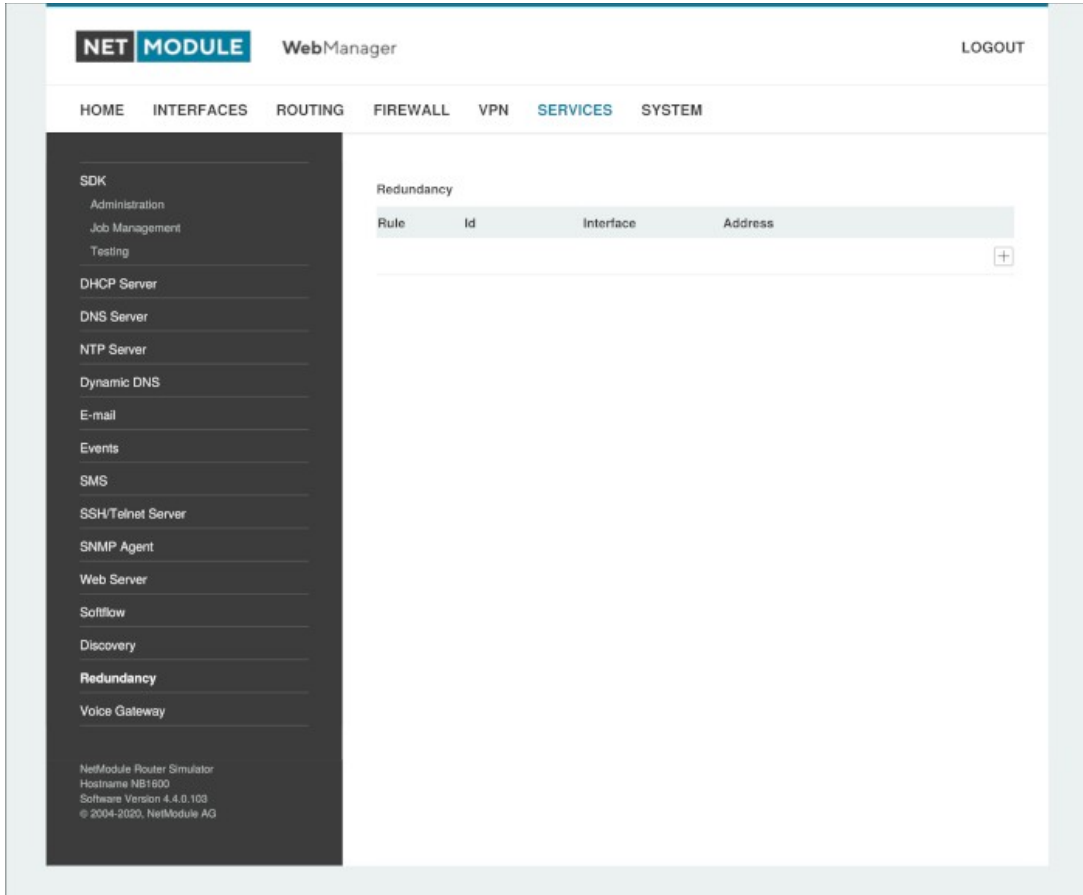
Parametre	Keşif Yapılandırma
LLDP	Link Layer Discovery Protocol
CDP	Cisco Discovery Protocol
FDP	Foundry Discovery Protocol
SONMP	Nortel Discovery Protocol
EDP	Extreme Discovery Protocol
IRDP	ICMP Router Discovery Protocol

IRDP, RFC1256'yı uygular ve ayrıca yerel olarak bağlı ana bilgisayarları nexthop ağ geçidi hakkında bilgilendirebilir. Keşfedilen tüm ana bilgisayarlar LLDP-MIB'ye maruz bırakılacak ve SNMP veya CLI/GUI üzerinden sorgulanabilir.

6.7.16. Yedeklilik (Redundancy)

Bu sayfa, aralarında Sanal Yönlendirici Yedeklilik Protokolü'nü (VRRP) çalıştırarak yedekli bir NetModule AG yönlendirici çifti (veya diğer sistemler) kurmak için kullanılabilir. Tipik bir VRRP senaryosu, birinci ana bilgisayar ve diğerini yedek cihazı oynayan bir ana bilgisayar tanımlar, her ikisi de tüm LAN ana bilgisayarlarının ARP önbelleğini güncellemek ve böylece paketleri buna göre yönlendirmek için gereksiz ARP mesajları tarafından dağıtılacak bir sanal ağ geçidi IP adresi tanımlar.

Ortağa artık ulaşılamadığında (çoklu yayın paketleri aracılığıyla kontrol edilir) yaklaşık 3 saniye içinde bir devralma gerçekleşir. Bu, bir cihaz yeniden başlatıldığında veya Ethernet bağlantısı kesildiğinde olabilir. Aynı durum WAN bağlantısı kesildiğinde de geçerlidir.



Ekran 6.52.: VRRP Yapılandırma

DHCP etkinleştirilmişse, sunucunun sunduğu DHCP ağ geçidi adresini yeniden yapılandırmanız ve sanal ağ geçidi adresine işaret etmelerine izin vermeniz gerektiğini lütfen unutmayın. Çakışmaları önlemek için yedekleme aygıtında DHCP'yi kapatabilir veya daha da iyisi, herhangi bir kiralama çoğaltmasını önlemek için DHCP kiralama aralığını her iki yönlendiriciye bölebilirsiniz.

Parametre	Yedeklilik Ayarları
Yönetimsel durum (Administrative status)	Yönetimsel durum
Rol (Role)	Bu sistemin rolü (ana veya yedek)
VID	Sanal Yönlendirici Kimliği (teorik olarak birden fazla örnek çalıştırabilirsiniz)
Arayüz (Interface)	VRRP'nin gerçekleştirileceği arayüz



Sanal ađ geidi adresi (Virtual gateway address)

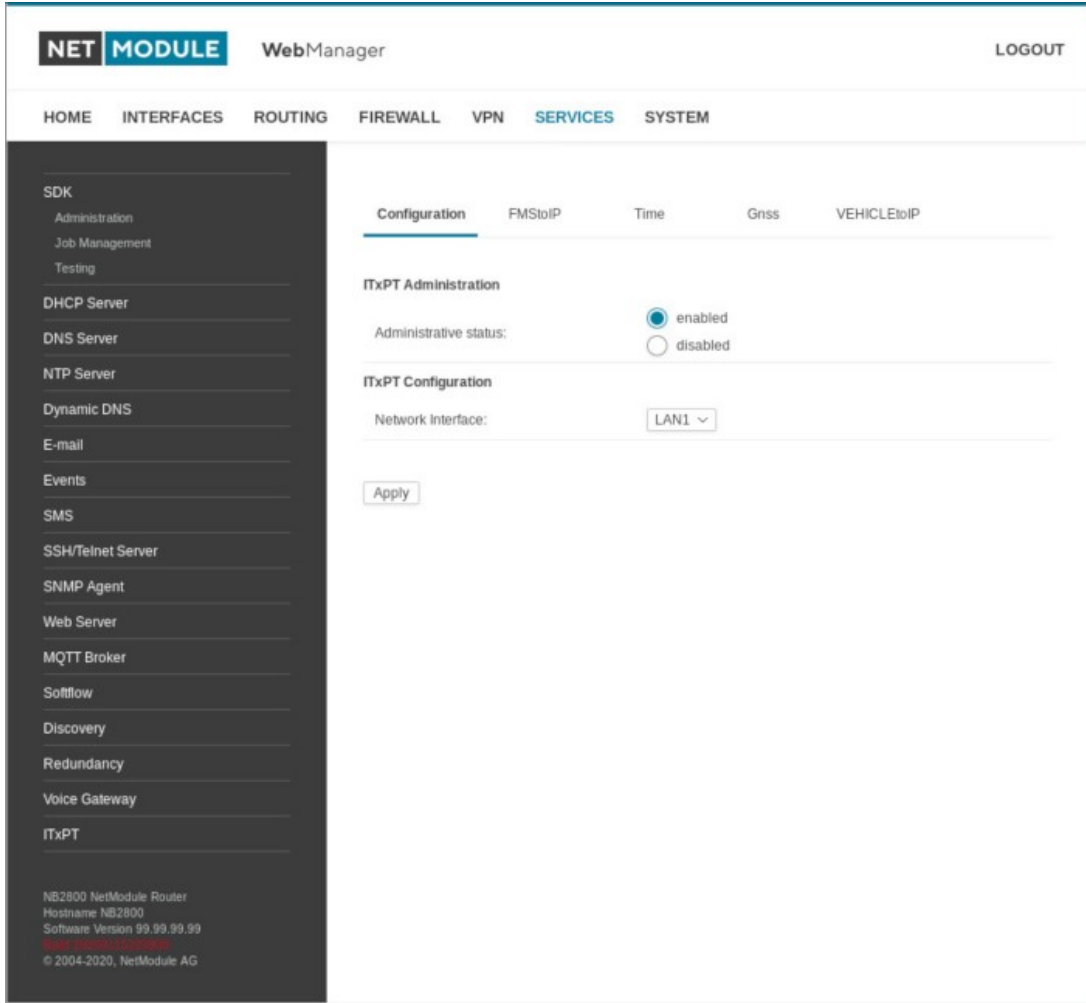
Katılımcı ana bilgisayarlar tarafından oluşturulan sanal ađ geidi adresi

Ana yönlendiriciye 100, yedek yönlendiriciye 1 öncelik atıyoruz. Lütfen üçüncü taraf cihazınızın önceliđini uygun şekilde uyarlayın.

6.7.17. ITxPT

Bu, ITxPT standardı v2.0.1'in bir entegrasyonudur. (bkz. [ITxPT Yerleşik Mimarisi Özellikleri v2.0.1](#))

Yapılandırma



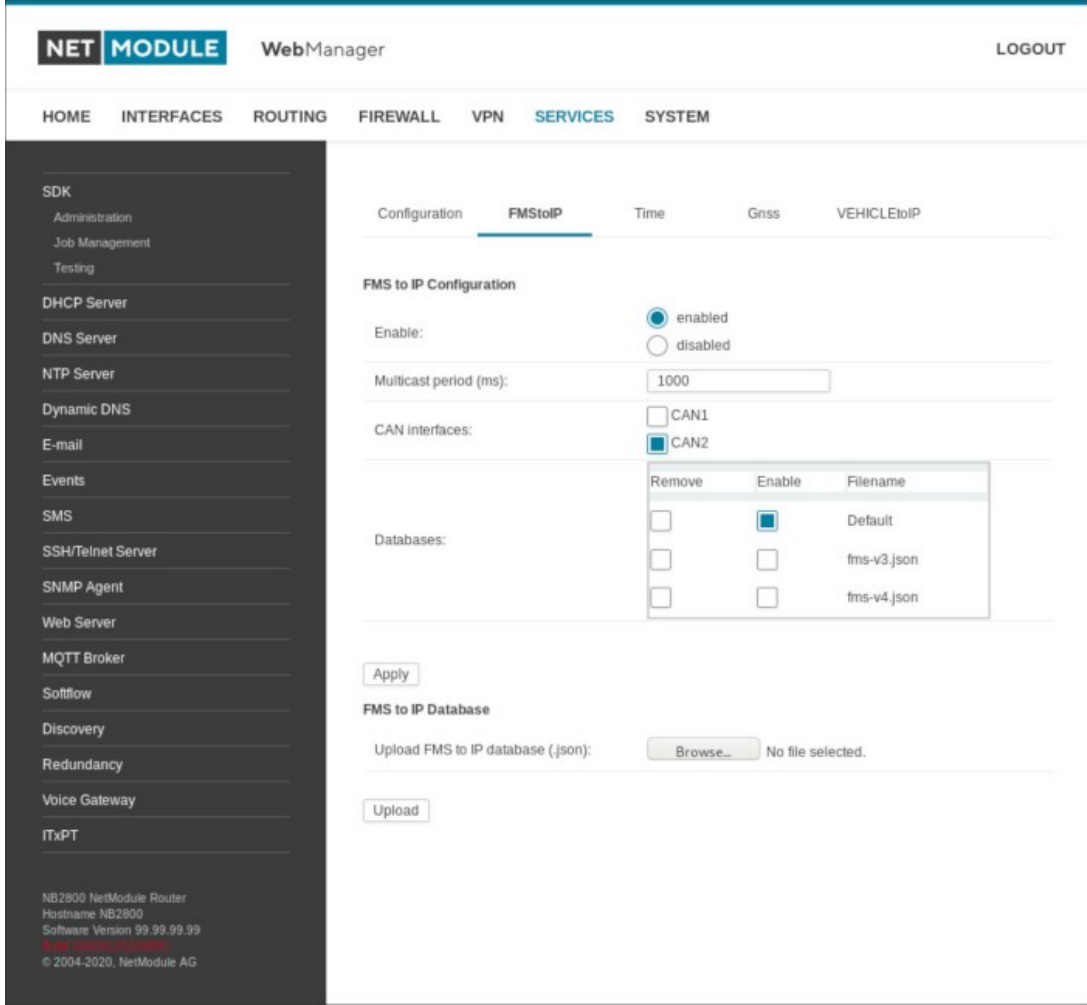
Ekran 6.53.: ITxPT Yapılandırma

Aşağıdaki parametreler ayar yapmak için kullanılabilir:

Parametre	ITxPT Yönetimi
Yönetimsel durum (Administrative status)	ITxPT işlevselliğinin etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.
Ağ arayüzü (Network Interface)	Servisin üzerinde çalışacağı ağ arayüzünü belirtir.



Parametre	ITxPT Yönetimi
Çoklu yayın TTL (Multicast TTL)	Çoklu yayın yönlendirmesi (ITxPT Hizmeti tarafından kullanılır) burada yapılandırılabilir ve bir daemon tarafından yönetilir. Smc yönlendirme daemon'u, birden fazla ağ arayüzünde kullanılabilir olacak şekilde yapılandırılabilir ve yönlendiricileri geçen ITxPT hizmetinin atlama sınırını sınırlama veya genişletme olanağı sağlar. IPv4 çoklu yayında, yönlendiricilerin her arayüze atanmış bir TTL eşiği vardır. Yalnızca arayüzün eşiğinden büyük bir TTL'ye sahip çoklu yayın paketleri iletilir. Çoklu yayın TTL'si 0 ile 255 arasında herhangi bir değere ayarlanabilir. Varsayılan ayar 0'dır.
mDNS yansıtıcısını etkinleştir (Enable mDNS reflector)	Yönlendirilen ağlar genelindeki tüm ağ arayüzlerine gelen mDNS (ITxPT Hizmeti tarafından kullanılır) isteklerini yansıtın, etkinleştirilmeli veya devre dışı bırakılmalıdır. Bunu yapmanın, güvenilmeyen ağlarınızdaki herhangi bir cihazın güvenilen ağlarınıza mDNS istekleri gönderebileceği anlamına geleceğini unutmayın.
Zaman (Time)	ITxPT Hizmet Süresinin etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.
GNSS	ITxPT Hizmeti GNSS'nin etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.
MQTT	ITxPT Hizmeti MQTT'nin etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.

FMS'ten IP'ye (FMS to IP)*Ekran 6.54.: ITxPT FMStoIP*

Bu sayfada FMS'den IP işlevselliğini yapılandırabilirsiniz.

Parametre	FMS to IP Seçenekleri
Etkinleştir (Enable)	FMS'den IP işlevselliğinin etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.
Çoklu yayın periyodu (Multicast period)	FMS'den IP'ye çoklu yayının ne sıklıkla gönderildiği. Gelen can mesajlarını hemen yönlendirmek için sıfıra ayarlayın.
CAN arayüzleri (CAN interfaces)	İşlenmesi gereken arayüzleri seçin (çoklu seçim).
Veritabanları (Databases)	Can-data'nın işlenmesinde kullanılacak FMS'den IP veritabanlarını seçin (çoklu seçim).



FMS'ten IP'ye veritabanı biçimi (FMS to IP database format)

Json dosya biçimi kullanılır. Veritabanı dosyası gelen veri paketlerini açıklar. FMS standardında kullanılan herhangi bir sinyali tanımlamak için iki temel bileşen vardır. Parametre Grup Numarası (Parameter Group Number, PGN) ve Şüpheli Parametre Numarası (Suspect Parameter Number, SPN). PGN bir veya daha fazla sinyal içerir. SPN bir sinyale benzersiz bir tanımlayıcı vermek için kullanılır. Daha fazla bilgi SAE-J1939 standardında bulunabilir.

```
[
  {
    "name": "EBFF",
    "pgn": 60415,
    "length": 8,
    "spns": []
  },
  {
    "name": "CCVS ",
    "pgn": 65265,
    "length": 8,
    "spns": [
      {
        "byteSize": 2,
        "offset": 1,
        "formatGain": 0.00390625,
        "formatOffset": 0,
        "units": "km/h",
        "name": "WheelSpeed",
        "number": 84,
        "type": 0
      },
      {
        "bitSize": 2,
        "bitOffset": 4,
        "offset": 3,
        "descriptions": [
          "Pedalreleased",
          "Pedaldepressed"
        ],
        "name": "BrakeSwitch",
        "number": 597,
        "type": 1
      }
    ]
  }
]
```

En üst düzey yapı bir dizidir. Aşağıdaki türlere sahip bir PGN tanımlayan PGN nesnelere sahiptir:

PGN Tanımı

Parametre	PGN Tanımı
Ad (name)	Pgn'nin adı.
pgn	Ondalık olarak PGN numarası.
uzunluk (length)	CAN mesajının uzunluğu.
spns	SPN nesnelere içeren dizi

Kod çözme gerekmiyorsa "spns" dizisi boş bırakılabilir.

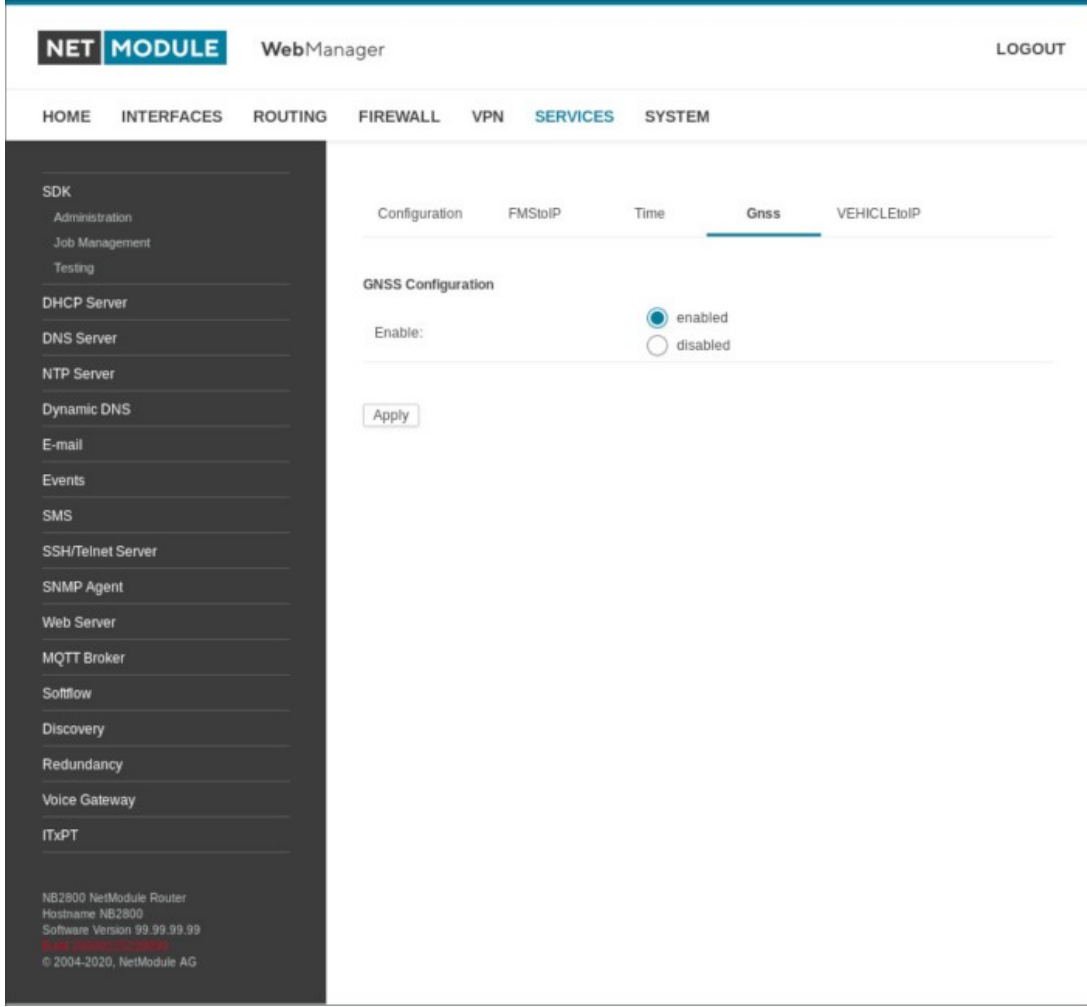
SPN Tanımı

SPN'ler sayısal (numerical), durumsal (status) ve metinsel (string.) olmak üzere üç türe ayrılır.

Parametre	Sayısal SPN
byteSize	Verinin bayt cinsinden boyutu.
offset	CAN-data'daki ofset.
formatGain	Değeri vermek için kullanılan sayısal faktör.
formatOffset	Değerin sayısal ofseti.
Birimler (units)	Değerin fiziksel birimi.
Ad (name)	SPN'nin adı
Sayı (number)	SPN numarası
Tip (type)	0 -> Sayısal SPN

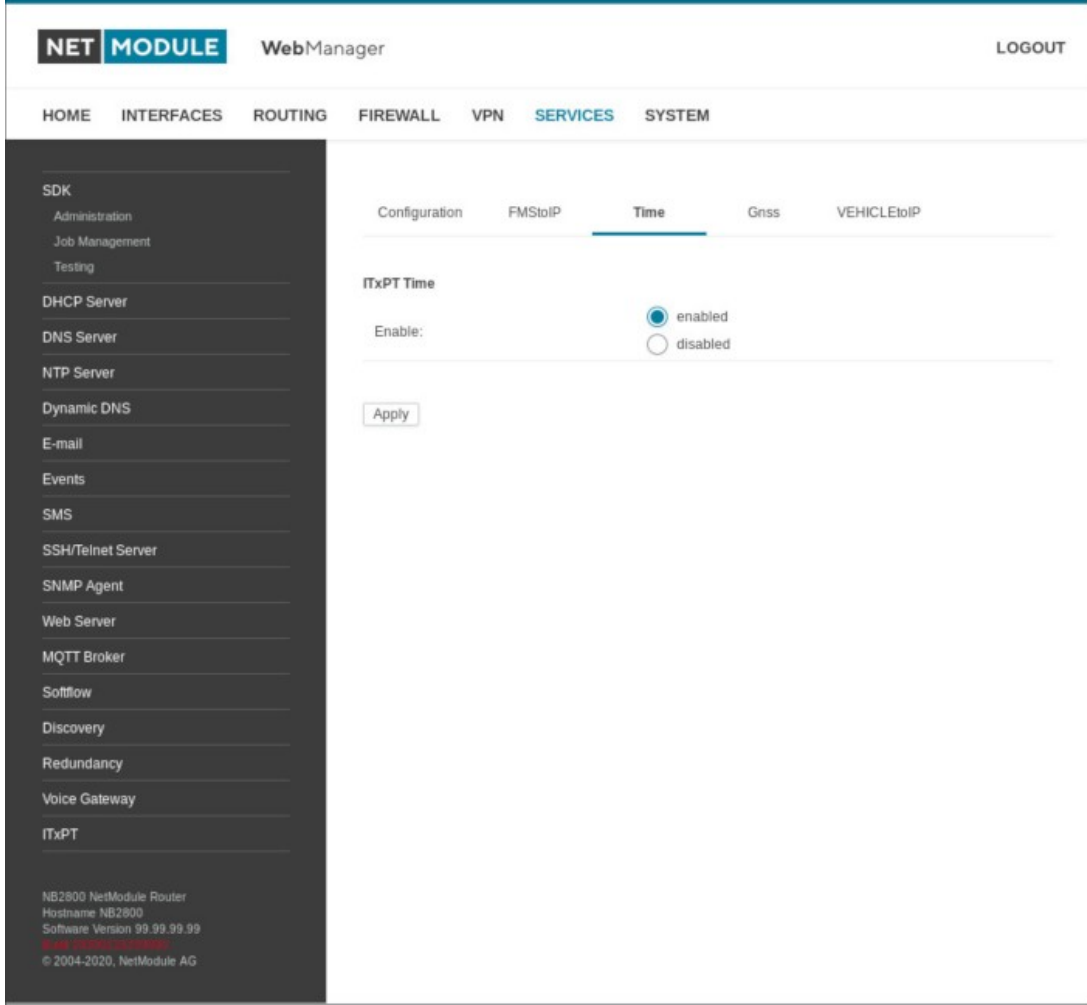
Parametre	Durumsal SPN
bitSize	Verinin bit cinsinden boyutu.
bitOffset	Bayttaki bit cinsinden ofset.
offset	CAN-data'daki ofset.
Açıklamalar (descriptions)	Durum açıklamasını içeren dizi.
Ad (name)	SPN'nin adı
Sayı (number)	SPN numarası
Tip (type)	1 -> Durumsal SPN

Parametre	Metinsel SPN
Ad (name)	SPN'nin adı
Sayı (number)	SPN numarası
Tip (type)	2 -> Metinsel SPN



Ekran 6.55.: ITxPT GNSS

Parametre	ITxPT GNSS
Etkinleştir (Enable)	ITxPT GNSS'in etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.

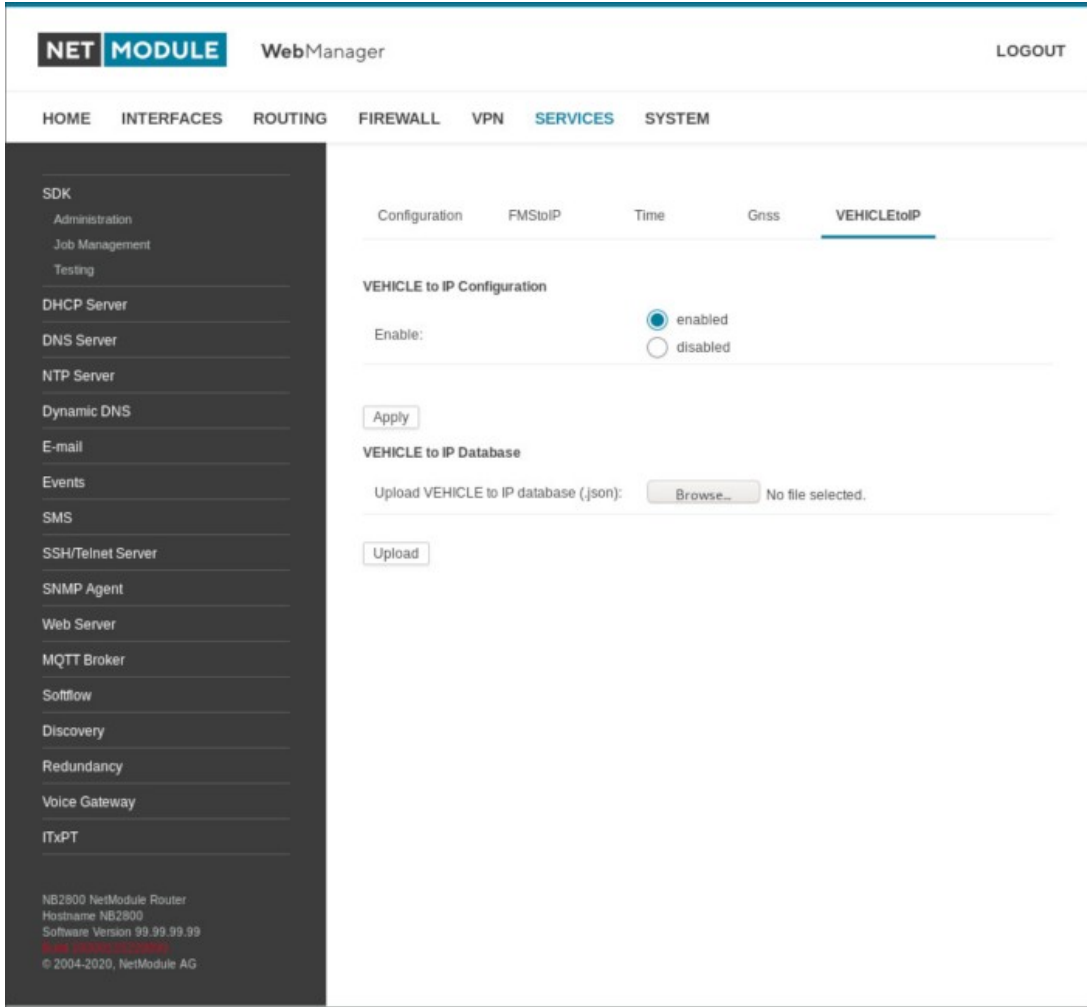
ITxPT Zaman (ITxPT Time)

Ekran 6.56.: ITxPT Zaman

Parametre	ITxPT Zaman
Etkinleştir (Enable)	ITxPT Time'in etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir.



Araçtan IP'ye (VEHICLE to IP)



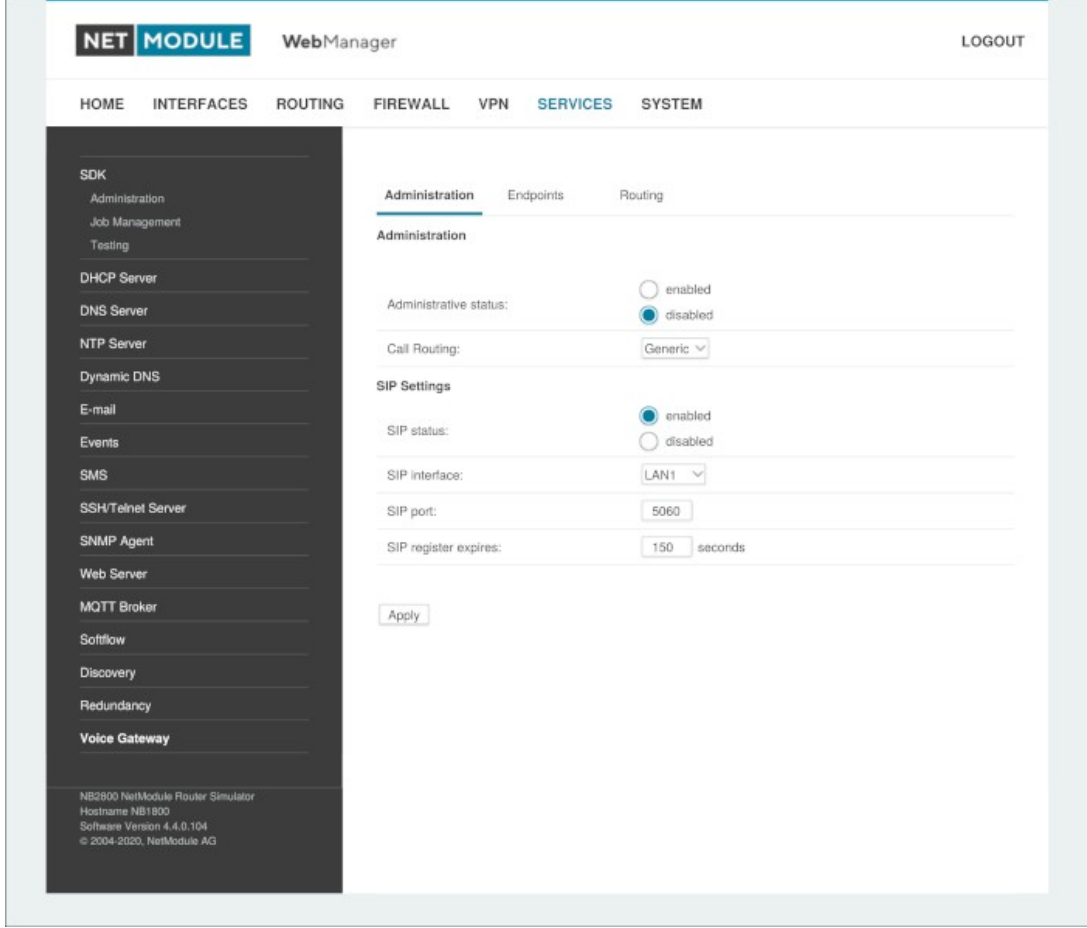
Ekran 6.57.: ITxPT VEHICLEtoIP

Parametre	ITxPT Vehicle To IP
Etkinleştir (Enable)	ITxPT VEHICLEtoIP'nin etkinleştirilmesi mi yoksa devre dışı bırakılması mı gerektiğini belirtir. Bu hizmeti etkinleştirmek için bir VEHICLEtoIP veritabanı gereklidir.

6.7.18. Ses Ağ Geçidi (Voice Gateway)

Donanımınıza bağlı olarak, yönlendiricinizde mobil aramaları VoIP istemcilerine bağlamak veya tam tersi yönde kullanmak için kullanılacak bir ses ağ geçidi kurabilirsiniz.

Yönetim



Ekran 6.58.: Ses Ağ Geçidi Yönetimi

Aşağıdaki parametreler ayar yapmak için kullanılabilir:

Parametre	Ses Ağ Geçidi Yönetim Ayarları
Yönetimsel durum (Administrative status)	Ağ geçidinin etkinleştirilip etkinleştirilmeyeceğini belirtir
Çağrı yönlendirme (Call routing)	Çağrı yönlendirmesinden kimin sorumlu olacağını tanımlar. SDK belirtilmişse, çağrıları yönlendirmekten ve kabul etmekten sorumlu olacak bir betik (örneklere bakın) yüklemeniz gerekir. Aksi takdirde statik yönlendirme yapılandırması kullanılacaktır.
SIP durumu (SIP status)	SIP aracısının etkinleştirilip etkinleştirilmeyeceğini belirtir
SIP arayüzü (SIP Interface)	Aracının gelen çağrıları dinlemesi gereken arayüzü (LAN veya WAN) belirtir
SIP port	Aracının dinleme bağlantı noktasını belirtir
SIP kaydı sonu (register expires)	Kayıt aralığını saniye cinsinden belirtir



Aynı SIM kartını paylaşan birden fazla WWAN arayüzü çalıştırıyorsanız, sistemin çalışma sırasında SIM kartlarını değiştirebileceğini ve bunun da sesli iletişim için farklı ayarlara yol açabileceğini lütfen unutmayın.

Ses Uç Noktaları (Voice Endpoints)

Bu sayfada sesli iletişim için kullanılan uç noktaları etkinleştirebilirsiniz, aşağıdaki türler desteklenmektedir:

Parametre	Ses Ağ Geçidi Uç Nokta Türü
Voice-Over-Mobile	GSM/UMTS/LTE aramaları için uç nokta (mobil veya sabit hat telefonlarına yapılan aramalar için kullanılabilir)
SIP (registrar)	Kayıt kuruluşunuza kayıtlı bir istemci olabilen SIP uç noktası
SIP (direct)	Kayıt olmadan doğrudan bir SIP aracısına yönlendirilen çağrılar için uç nokta
SIP (user-agent)	Uzak bir kayıt kuruluşuna doğru SIP kullanıcı aracısı olarak hareket eden uç nokta

Ekipmanınıza bağlı olarak, daha iyi bir ses deneyimi için modemin ses profilini ayarlamanızı öneririz. Aşağıdaki profiller mevcuttur:

Parametre	Voice-Over-Mobile Ses Profilleri
Ahize (Handset)	Hafif bir yankı, kısa gecikme (16 ms'den az dağılım) sağlar. Bu mod, Yankı Geri Dönüş Kaybı'nın (Echo Return Loss, ERL) genellikle yüksek olduğu iyi tasarlanmış bir ahize ile kullanım için tasarlanmıştır. Tam çift yönlü performans bu modda elde edilmesi en kolay olanıdır.
Kulaklık (Headset)	Orta düzeyde yankı, kısa gecikme (16 ms'den az dağılım) sağlar. Bu mod, yankının yüksek ancak gecikmenin düşük olduğu durumlarda kullanılmak üzere tasarlanmıştır. Çok çeşitli yankı özellikleri ve gürültü alımına sahip çeşitli farklı kulaklıklar mevcuttur. Tüm kulaklıklarda yankı gecikmesi genellikle kısa (< 16 ms) olsa da, yankı geri dönüş kaybı özellikleri önemli ölçüde değişebilir ve ahize tasarımcısı tarafından önceden iyi bilinmez. Bu mod daha sağlamdır ve yankı iptalinde daha agresiftir.
Hoparlör (Speakerphone)	Aşırı akustik bozulma ile yüksek yankı durumlarını yönetin. Bu mod, yüksek ses ve yüksek bozulmaya sahip bir araç kiti veya hoparlörlü telefon uygulamalarıyla kullanım için tasarlanmıştır. Bu durumda akustik yankı negatif ERL'ye sahiptir ve tamamen iptal edilmesi imkansızdır. Yarı çift yönlü bir şekilde çalışır ve yankı seslerinin duyulmasını önlemek için tüm sinyali susturmada çok agresif olacaktır.

Parametre	Voice-Over-Mobile Uç Nokta Ayarları
Modem	Mobil üzerinden sesli aramalar için kullanılacak modemi belirtir
Ses profili (Audio profile)	Modemin ses profilini belirtir
Ses seviyesi (Volume level)	Modemin ses seviyesini belirtir - 1 = düşük



Parametre	Uç Nokta Ayarları SIP (registrar)
Abone (Subscriber)	Kayıtlı bir SIP istemcisi için abone adı
Kullanıcı adı (Username)	Kayıtlı bir SIP istemcisinin kullanıcı adı
Şifre (Password)	Kayıtlı bir SIP istemcisinin kullanıcı şifresi

Parametre	Uç Nokta Ayarları SIP (direct)
Abone (Subscriber)	SIP aracısının abone adı
Ana bilgisayar (Host)	SIP aracısının IP adresi
Port	SIP aracısının portu
Kullanıcı adı (Username)	SIP aracısında kimlik doğrulaması için kullanıcı adı
Şifre (Password)	Kimlik doğrulama için kullanılan parola

Parametre	Uç Nokta Ayarları SIP (user-agent)
Ana bilgisayar (Host)	SIP kayıt sunucusunun IP adresi
Port	SIP kayıt sunucusunun portu
Etki alanı (Domain)	SIP kayıt sunucusunun etki alan adı
Abone (Subscriber)	Abonenin SIP kayıt sunucusundaki adı
Kullanıcı adı (Username)	SIP kayıt sunucusunda kimlik doğrulaması için kullanıcı adı
Şifre (Password)	Kimlik doğrulaması için kullanılan parola
Kayıt (Register)	Kullanıcı aracısının SIP kayıt sunucusunda kayıt yaptırıp yaptırmayacağını seçer
Kayıt sonlanır (Expires)	Kayıttan sonra saniye cinsinden son kullanma süresi tekrar tetiklenecektir



Ses Yönlendirme (Voice Routing)

Bu sayfa uç noktalar arasında genel ses yönlendirmesini yapılandırmak için kullanılabilir.

Gelişmiş yönlendirme olanakları, niteliklerine (telefon numarası gibi) ve diğer sistemle ilgili durum bilgilerine (örneğin, uç nokta başına çağrı sayısı/süresi, kayıt durumu vb.) göre sesli çağrılar gönderebilen SDK arayüzü aracılığıyla sağlanır. SDK'yı kullanarak ayrıca bir çağrıyı başlatabilir veya kabul edebilir, ses seviyesini ayarlayabilir veya bir kapatma işlemi yapabilirsiniz.

Basit senaryolar için genel yöntem yeterli olmalı ve aşağıdaki gibi yapılandırılabilir:

Parametre	Ses Ağ Geçidi Yönlendirme Ayarları
Kaynak (Source)	Kaynak uç noktasını (yani çağrının geldiği yeri) belirtir
Mode	Çağrıya uygulanacak eylem türü: DROP çağrıyı sessizce sonlandıracak, ROUTE çağrıyı belirtilen uç noktaya yönlendirecektir.
Varış noktası (Destination)	Hedef uç noktayı belirtir (yani çağrının nereye yönlendirileceğini)

İstemci Yapılandırma (Client Configuration)

Herhangi bir SIP istemcisi, yönlendiriciyi kayıt kuruluşu/proxy'si olarak kullanacak şekilde yapılandırılmalıdır.

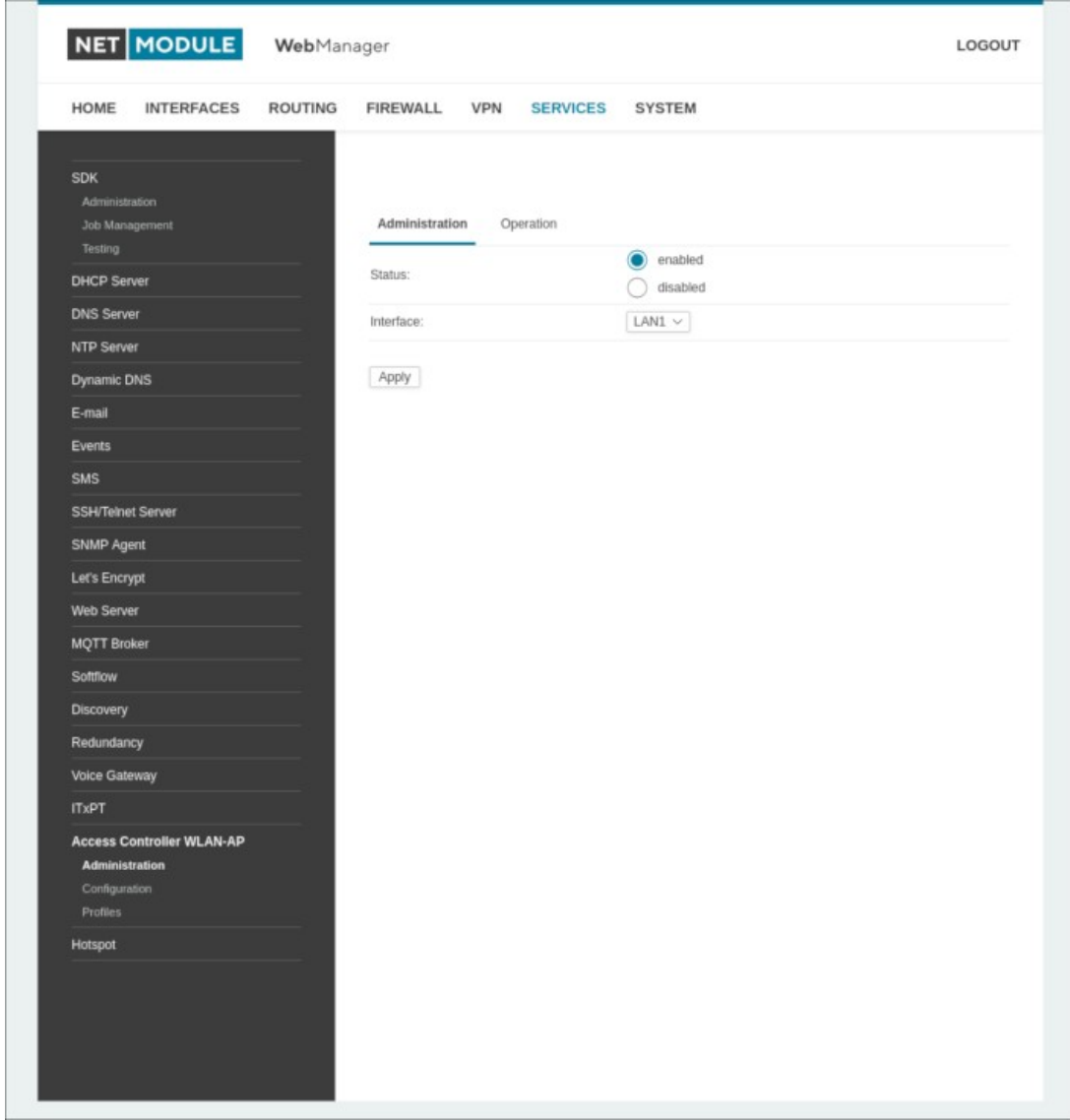
Parametre	X-Lite Yapılandırma
Kullanıcı ID (User ID)	Başlıklarda kullanılan SIP kullanıcı adı (yani abone adı)
Etki alanı (Domain)	Başlıklardan kullanılan SIP Etki Alanı (isteğe bağlı)
Kimlik doğrulama adı (Authorization name)	Kimlik doğrulama için gerekli kullanıcı adı (yani abone adı)
Şifre (Password)	Kimlik doğrulama için kullanılan parola
Ekran adı (Display name)	El cihazında görüntülenecek isim



6.7.19. Erişim Denetimcisi WLAN-AP (Access Controller WLAN-AP)

Bu bölüm, NetModule AP3400 erişim noktası cihazları için Erişim Denetleyicisini (Access Controller, AC) yapılandırmak için kullanılabilir. AC, AP3400 yapılandırmalarını oluşturabilir, yapılandırmayı itebilir ve AP3400 cihazlarının geçerli durum bilgilerini okuyabilir. AC, 15 adede kadar AP3400 cihazını yönetebilir. Farklı cihaz durumları arasında ayırım yapılacaktır.

Parametre	AC Aygıt Durumları
Araştırılıyor (discovering)	NRSW bu cihaz için geçerli bir yapılandırmaya sahip ancak cihaz keşfedilmedi
Bulundu (discovered)	Aygıt keşfedildi ancak geçerli bir yapılandırma mevcut değil
Yönetilmiyor (unmanaged)	Aygıt keşfedildi, NRSW aygıt için geçerli bir yapılandırmaya sahip ve şu anda yapılandırmayı aygıtı gönderiyor
Yönetilen (managed)	NRSW yapılandırmayı cihaza başarıyla gönderiyor ve durum bilgisi alıyor
Güncelle (update)	Cihaz güncelleme işlemini çalıştırıyor
Yeniden başlat (reset)	Cihaz yeniden başlama işlemi gerçekleştiriyor
Kayıp (lost)	Örneğin yönetilen cihazın yeniden başlatılması sonrasında NRSW ile yönetilen cihaz arasındaki iletişim kayboldu.

Yönetim (Administrator)

Ekran 6.59.: AC WLAN-AP Yönetimi

Parametre	AC Yönetim Ayarları
Durum (Status)	AC işlevselliğini etkinleştirir veya devre dışı bırakır
Arayüz (Interface)	AC'nin dinlediği arayüz



Parametre	AC Yönetim Ayarları
Çalıştırma komutu (Operation command)	Gerçekleştirilecek işlem türünü seçer. 'Firmware güncellemesi' veya 'sıfırlama' işlemi için parametre listesi için aşağıdaki tabloya bakın
ID	Klimanın çalışabileceği bulunan cihazların listesi.

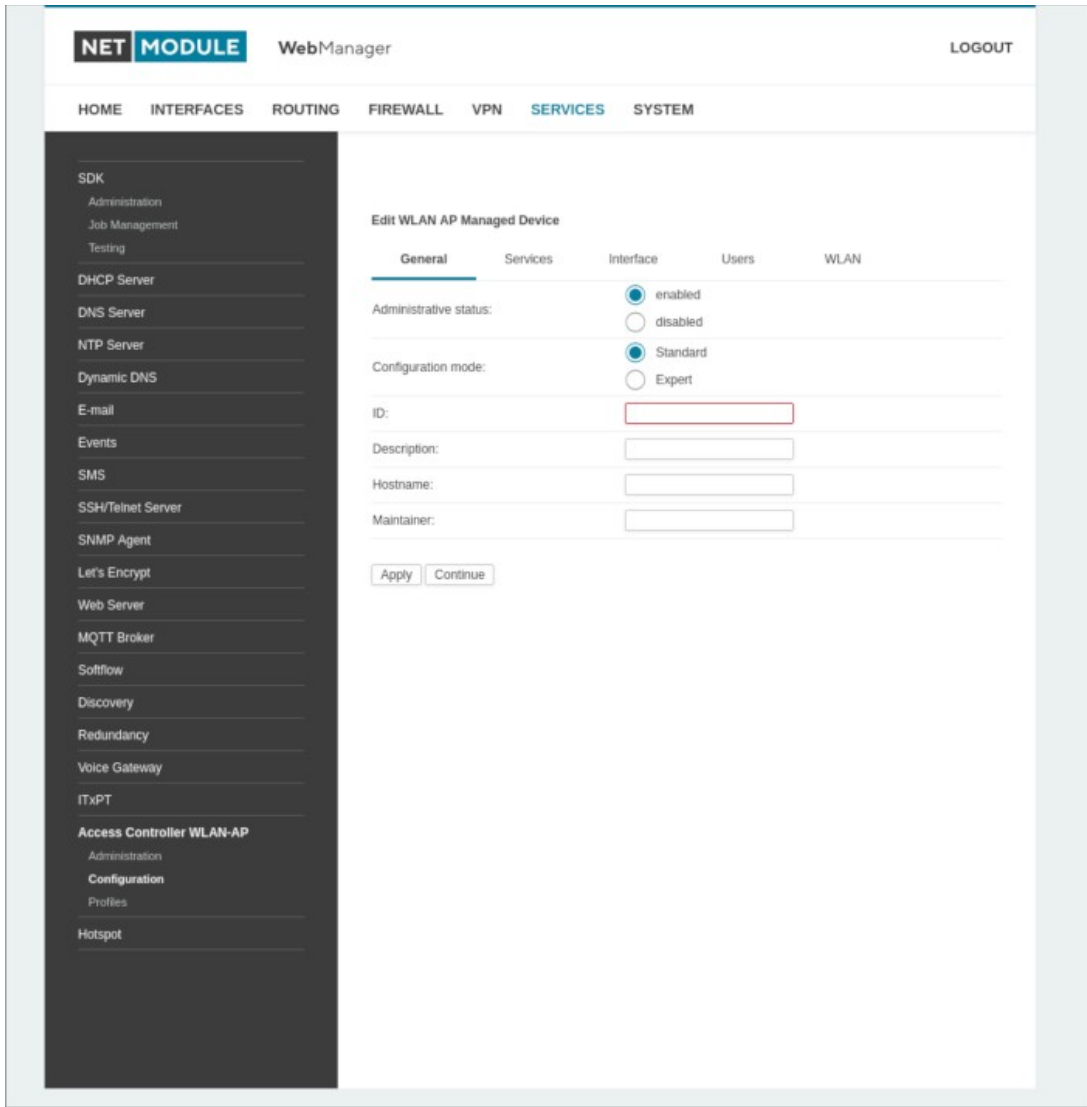
Seçilen işlem ID altında listelenen tüm seçili aygıtlarda gerçekleşecektir. Uygula düğmesine bastıktan sonra seçilen işlem son olarak gerçekleştirilecektir.

Parametre	AC Çalışma Ayarları - Aygıt Yazılımı Güncellemesi
Donanım yazılımı güncelle (Firmware update)	NM AP3400 için bir FW'yi NM Router'ın dahili depolama alanına yükleme veya silme olanağı.

Parametre	AC Çalışma Ayarları – Yeniden Başlat
Fabrika ayarlarına sıfırlama (Factory reset)	Fabrika ayarlarına sıfırlama işlemi gerçekleştirin.
Yeniden başlat (Reboot)	Yeniden başlatma işlemi gerçekleştirin.
Ağı yeniden başlat (Restart network)	Ağ arayüzlerini yeniden başlatın.

Yapılandırma

Yapılandırma sayfasıyla AP3400'ü kendiniz yapılandırmak mümkündür. Yapılandırma için cihazın seri numarası olan benzersiz bir kimliğe sahip olmak gerekir. Cihaz kimliği AC durum sayfasında ve yapılandırma sırasında cihaz keşfedildiyse kimlik alanındaki açılır menü aracılığıyla gösterilecektir.



Ekran 6.60.: AC WLAN-AP Yapılandırma

Parametre	AC Yapılandırma – Genel Ayarlar
Yönetimsel durum (Administrative status)	Etkinleştirildiğinde ID ile belirtilen cihaz AC tarafından kontrol edilecektir.
Yapılandırma durumu (Configuration mode)	'Standart' seçeneği GUI üzerinden yapılandırılan parametreleri kullanır. 'Uzman modu' AP3400 için kendi kendine oluşturulmuş bir yapılandırma dosyasını yükleme olanağını açar. Uzman modu dosyasının yapılandırma için NetModule JSON şemasına uyması gerekir. Uzman modu seçeneği seçiliyken kopyala'ya tıklayarak mevcut yapılandırmanın JSON formatında bir kopyasını indirmek mümkündür.
ID	Yönetilen cihazın benzersiz kimliği (seri numarası). Seçilebilir olan tüm keşfedilen cihazlar bu alana çift tıklanarak gösterilecektir.
Açıklama (Description)	Yönetilen cihazın kısa açıklaması
Ana bilgisayar (Hostname)	Yönetilen cihazın ana bilgisayar adı
Bakımcı (Maintainer)	Yönetilen cihazın bakımcısı



Parametre	AC Yapılandırma – Servis Ayarları – HTTP
HTTP durumu (HTTP status)	Yönetilen cihaz için HTTP'yi etkinleştirir veya devre dışı bırakır
HTTP port	AP3400 için HTTP portu

Parametre	AC Yapılandırma – Servis Ayarları – HTTPS
HTTPS durumu (HTTP status)	Yönetilen cihaz için HTTPS'yi etkinleştirir veya devre dışı bırakır
HTTPS port	AP3400 için HTTPS portu
HTTPS sertifikası (HTTPS certificate)	AP3400 için sertifika oluşturma olanağını ekler

Parametre	AC Yapılandırma – Servis Ayarları – GUI
Durum (Status)	GUI işlevselliğini etkinleştirir veya devre dışı bırakır

Parametre	AC Yapılandırma – Servis Ayarları – SSH
SSH durumu (SSH status)	Yönetilen cihaz için SSH'yi etkinleştirir veya devre dışı bırakır
SSH port	AP3400 için SSH portu

Parametre	AC Yapılandırma – Arayüz Ayarları
IP modu (IP mode)	Yönetilen cihaz için IP modunu seçer. 'DHCP IPv4' seçeneğini kullanarak yönetilen cihazlar DHCP sunucusundan bir IP adresi elde edecektir. 'Statik', AP3400'ün aşağıdaki parametrelerle verilen IP adresini ve ağ maskesini kullanacağı anlamına gelir.
Adres (Address)	AP3400'ün kullanacağı IP adresi
Ağ maskesi (Netmask)	AP3400'ün kullanacağı ağ maskesi

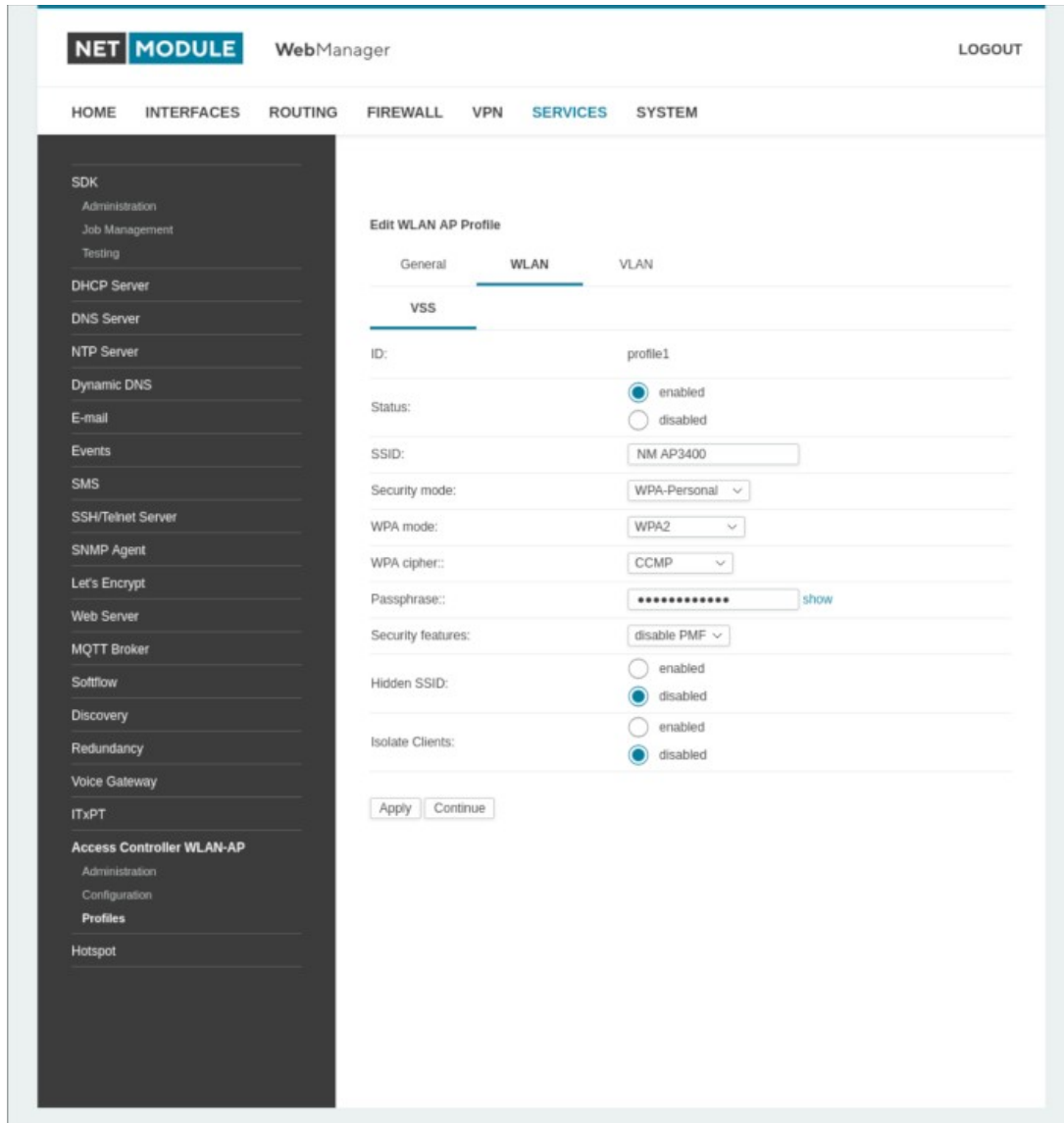
Parametre	AC Yapılandırma – Kullanıcı Ayarları
Kullanıcı adı (Username)	Yönetilen cihaz için kullanılan kullanıcı adı
Şifre (Password)	Yönetilen cihaz için kullanılan kullanıcı şifresi



Parametre	AC Yapılandırma – WLAN Ayarları
Yönetimsel durum (Administrative status)	AP3400'ün belirtilen radyosunu etkinleştirir veya devre dışı bırakır
Çalıştırma modu (Operation mode)	AP3400'ün seçili radyo modülü için çalışma modu. Yalnızca 'Erişim Noktası' (Access Point) modu desteklenmektedir
Ülke (Country)	AP'nin faaliyet gösterdiği ülkeyi seçin
Çalıştırma tipi (Operation type)	İstenen IEEE 802.11 çalışma modunu belirtir
Radyo bantı (Radio band)	Bağlantılar için kullanılacak radyo bandını seçer, modülünüze bağlı olarak 2,4 veya 5 GHz olabilir
Bant genişliği (Bandwidth)	Kanal bant genişliği çalışma modunu belirtin
Kanal (Channel)	Kullanılacak kanalı belirtir
Tx gücü (Tx power)	dBm cinsinden kullanılan maksimum iletim gücünü belirtir.
Profil ID'leri (Profile IDs)	AP3400'ün kullanması gereken profiller (bkz. profiller bölümü)

Profiller

NetModule Erişim Denetleyicisi ile 10'a kadar farklı profil yapılandırmak mümkündür. Her profil ile şifreleme ve VLAN ile bağımsız bir SSID yapılandırmak mümkündür.



Ekran 6.61.: AC WLAN-AP Profilleri

Parametre	AC Profil Genel Ayarları
ID	Profil için benzersiz ad
Açıklama (Description)	Profilin açıklaması

Parametre	AC Profil WLAN Ayarları
Durum (Status)	Bu profili etkinleştirir veya devre dışı bırakır
SSID	Ağ adı (SSID olarak adlandırılır)
Açıklama (Description)	Profilin açıklaması
Güvenlik modu (Security mode)	İstenilen güvenlik modu
WPA modu (WPA mode)	İstenilen şifreleme yöntemi. WPA3, WPA2 ve WPA1'e tercih edilmelidir.
WPA şifresi (WPA cipher)	Kullanılacak WPA şifresi, varsayılan olarak her ikisini de (TKIP ve CCMP) çalıştırmaktır



Şifre (Passphrase)	WPA-Personal ile kimlik doğrulama için kullanılan parola, aksi takdirde WPA-EAP-TLS için anahtar parola. WPA-Personal durumunda: Parola en az 8 ila 63 karakter uzunluğunda olmalıdır.
Güvenlik özellikleri (Security features)	Korunan Yönetim Çerçevesini Etkinleştirir (Protected Management Frames)
Gizli SSID (Hidden SSID)	SSID'yi gizle
İstemcileri izole et (Isolate clients)	İstemciden istemciye iletişimi devre dışı bırakır
RADIUS sunucu (RADIUS server)	RADIUS sunucu adresi
RADIUS secret (RADIUS şifresi)	RADIUS sunucusuna karşı kimlik doğrulaması için kullanılan sır
Kimlik doğrulama portu (Authentication port)	Kimlik doğrulama için kullanılan port
Hesap portu (Accounting port)	Hesap mesajları için kullanılan port

Parametre	AC Profil VLAN Ayarları
VLAN ID	Profil için VLAN kimliği. Bu profille hiçbir VLAN kimliği kullanılmayacaksa parametrenin boş olması gerekir



6.7.20. Hotspot

Bu bölüm, yönlendiricide bir tutsak (captive) portal sağlayan bir erişim noktası (Coova Chilli tabanlı) hizmeti kurmak için kullanılabilir; bu, internet erişimi verilmeden önce bağlanan herhangi bir istemciyi bir açılış sayfasına yönlendirir.

Parametre	HotSpot Temel Ayarlar
Adı (Name)	Captive portalın adı
Arayüz (Interface)	Atfedilen Arayüz
Adres (Address)	Seçilen IP Adresi
Mod (Mode)	Seçilen modu açıklar

Yönetim

Parametre	HotSpot Yönetim Ayarları
Durum (Status)	Captive portalı etkinleştir/devre dışı bırak
Arayüz (Interface)	Atfedilen arayüzü seçin
Ağ (Network)	Ağ adresi
Ağ maskesi (Netmask)	Ağ maskesi
Yerel adres (Local address)	Yerel IP adresi
Portal adı (Portal name)	Portalın adı
Günlük kaydı (Logging)	Etkinleştirilirse Hotspot örneği daha fazla günlük kaydı gösterecektir

Parametre	Açılış Sayfası
Durum	Önceden tanımlanmış portal kuruluysa veya başka bir şey varsa, portalın durumu ve düzenleme olanağı
Yükle (Upload)	Özel açılış sayfasını yükleyin
İndir (Download)	Yüklü varsayılan açılış sayfasını indirin

Gelişmiş

İki operasyonel mod mevcuttur. Yalnızca şartlara dayalı hizmet (ToS) modu bir Hizmet Şartları sayfası gösterir ve kullanıcı İnternet'e erişmeden önce bu şartları kabul etmek zorundadır. İkinci mod, harici bir RADIUS sunucusu gerektiren bir RADIUS yapılandırması kullanmak içindir. Bu modda kullanıcı İnternet'e erişmeden önce kullanıcı girişi ve parola alanı olan bir esir portal web sayfası alır.

Parametre	Gelişmiş Ayarlar
Çalışma Modu (Operational Mode)	Yalnızca Şartlar Hizmeti veya RADIUS yapılandırması kullanıldı, aşağıdaki tablolarda ayrıntılara bakın
Yerel arayüzlere erişim (Access local interfaces)	Seçilirse, kullanıcı yönlendiricinin yerel arayüzüne bağlı olan hizmetlere ulaşabilir
DHCP başlangıç (DHCP start)	Bağlı istemciler için DHCP aralığı, 2'den başlar
DHCP son (DHCP end)	Bağlı istemciler için DHCP aralığı 254'te sona erer



Parametre	Yalnızca Şartlara Dayalı Hizmet
Bant Genişliği Sınırlaması Aşağı (Bandwidth Limitation Down)	Bu seçenek, Hotspot arayüzüne bağlı ve kimliği doğrulanmış her kullanıcının/cihazın bant genişliğini (yükleme/indirme) sınırlar.
Bant Genişliği Sınırlaması Yukarı (Bandwidth Limitation Up)	"Bant Genişliği Sınırlaması Aşağı" bölümüne bakın
Trafik sınırlama (Traffic Limitation)	Bu seçenekle kullanıcı/istemci başına veri tüketimini sınırlamak mümkündür. Verilen trafik sınırına ulaşıldıktan sonra kullanıcı/istemci tekrar giriş sayfasına yönlendirilecektir.
Etkin Olmama Zaman Aşımı (Inactivity Timeout)	Bir istasyon bu zaman aşımı süresi içerisinde hiçbir şey göndermezse kullanıcı otomatik olarak oturumdan çıkarılır
Oturum Zaman Aşımı (Session Timeout)	Maksimum oturum süresini saniye cinsinden ayarlayın. Varsayılan oturum zaman aşımı 0, sınırsız süre anlamına gelir. Oturum zaman aşımına ulaşıldıktan sonra istemci oturumu kapatılacaktır.

Parametre	RADIUS Ayarları
Birincil RADIUS sunucusu (Primary RADIUS server)	Birincil yarıçap sunucusunun IP adresi
İkincil RADIUS sunucusu (Secondary RADIUS server)	İkincil yarıçap sunucusunun IP adresi
Paylaşılan sır (Shared Secret)	Her iki sunucu için Radius paylaşımlı sırrı
Kimlik doğrulama portu (Authentication Port)	Yarıçap kimlik doğrulama istekleri için kullanılacak UDP bağlantı noktası numarası (varsayılan 1812)
Hesap portu (Accounting Port)	Yarıçap muhasebesi istekleri için kullanılacak UDP bağlantı noktası numarası (varsayılan 1813)
Hesap aralığı (Accounting Interval)	Bu aralık, Hotspot işleminin hesaplama bilgilerini yarıçap sunucusuna hangi saniyelerde bildireceğini belirtir. RADIUS tarafından aksi belirtilmediği sürece RADIUS hesaplaması için varsayılan ara aralık (varsayılan olarak 0'dır, yani sınırsızdır)
Yalnızca hesap dışı trafik (Account external traffic only)	Etkinleştirilirse Hotspot işlemi yalnızca harici trafiği bildirecektir. Bu, Walled Garden trafiği gibi dahili trafiğin yok sayılacağı anlamına gelir
Hesap SSID (Account SSID)	Etkinleştirildiğinde, Hotspot işlemi, RADIUS Aranan İstasyon Kimliğinin MAC'ini, iki nokta üst üste işaretiyle ayrılmış geçerli WLAN arayüzünün SSID'siyle ekleyecektir.
Change of Authorization (CoA)	Bu, bir RADIUS sunucusunun etkin bir istemci oturumunu ayarlamasına olanak tanır.
MAC kimlik doğrulaması (MAC authentication)	Bu seçenek verilirse, Radius tüm kullanıcıların kimlik doğrulamasını MAC adreslerine göre yapmaya çalışacaktır

UAM

Evrensel Erişim Yöntemi (UAM) ayarlarıyla, erişim noktası için harici hizmetleri (örneğin harici özel açılış sayfası) yapılandırmak mümkündür.



Parametre	Kullanıcı Tarafından Yönetilen Erişim
Harici UAM Sunucusu (External UAM Server)	İstemcileri doğrulamak için kullanılacak web sunucusunun URL'si
UAM Port	Kimlik doğrulaması yapan istemciler için bağlanılacak TCP portu (varsayılan = 3990). Kimliği doğrulanmamış bir istemci internete erişmeye çalışırsa istemci yönlendiricinin yerel IP adresinin bu portuna yönlendirilecektir
Harici UAM AnaSayfası (External UAM Homepage)	Kimliği doğrulanmamış kullanıcıları yönlendirecek ana sayfanın URL'si. Belirtilmezse bu varsayılan olarak uam sunucusuna gider
UAM Sırrı (UAM Secret)	Harici uam sunucusu ve hotspot arasında paylaşılan sır. Bu sır, güvenliği tehlikeye atmamak için ayarlanmalıdır.

Not: Harici bir UAM sunucusu veya UAM ana sayfası kullanmıyorsanız, varsayılan değerleri kullanmak için yapılandırma parametresini boş bırakın.

Walled Garden

Walled Garden ayarlarıyla, müşteriye/kullanıcıya bir hesap olmadan veya ToS anlaşmalarını kabul etmeden web sayfaları gibi ücretsiz hizmetler sunmak mümkündür. Bir URL ve açıklama aracılığıyla yapılandırılan hizmetler, esir portal tarafından yok sayılacak ve kullanıcı hizmetlere doğrudan ulaşacaktır. Duvarlı bahçenize ekleme yapmak, kredi kartı ödeme ağ geçitlerine, topluluk web sitesine veya diğer herkese açık kaynaklara erişim sağlamak için yararlıdır.

Parametre	Walled Garden
Açıklama (Description)	Açıklama
URL	Seçeneğin her kullanımı için bir alan adı öneki

Örnek

Bu bölüm, NetModule AG bağımsız erişim noktası çözümünün bir örnekle nasıl yapılandırılacağını açıklar.

- Mobil arayüz üzerinden WAN uplink
- WLAN
 - 2,4 GHz çalışma modu
 - Kanal 1S
 - SSID adı „Erişim Noktası“ (Hotspot)
 - Güvenlik seçeneği olmayan genel wlan
- Erişim Noktası
 - Captive portal adı: „Erişim Noktası“
 - Ağ: 192.168.200.0/24
 - Çalışma modu: „sadece şartlara tabi hizmet“ (terms-only service)



Yapılandırma

(Mobile->Interfaces->Connection)

The screenshot displays the Hirschmann NetModule WebManager interface. The top navigation bar includes 'NET MODULE', 'WebManager', and 'LOGOUT'. Below this, a menu bar lists 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. The 'INTERFACES' section is active, showing a sidebar with various configuration options like WAN, Ethernet, Mobile, WLAN, Bridges, USB, Serial, Digital I/O, and GNSS. The main content area is titled 'Mobile Interfaces' and contains a table with the following data:

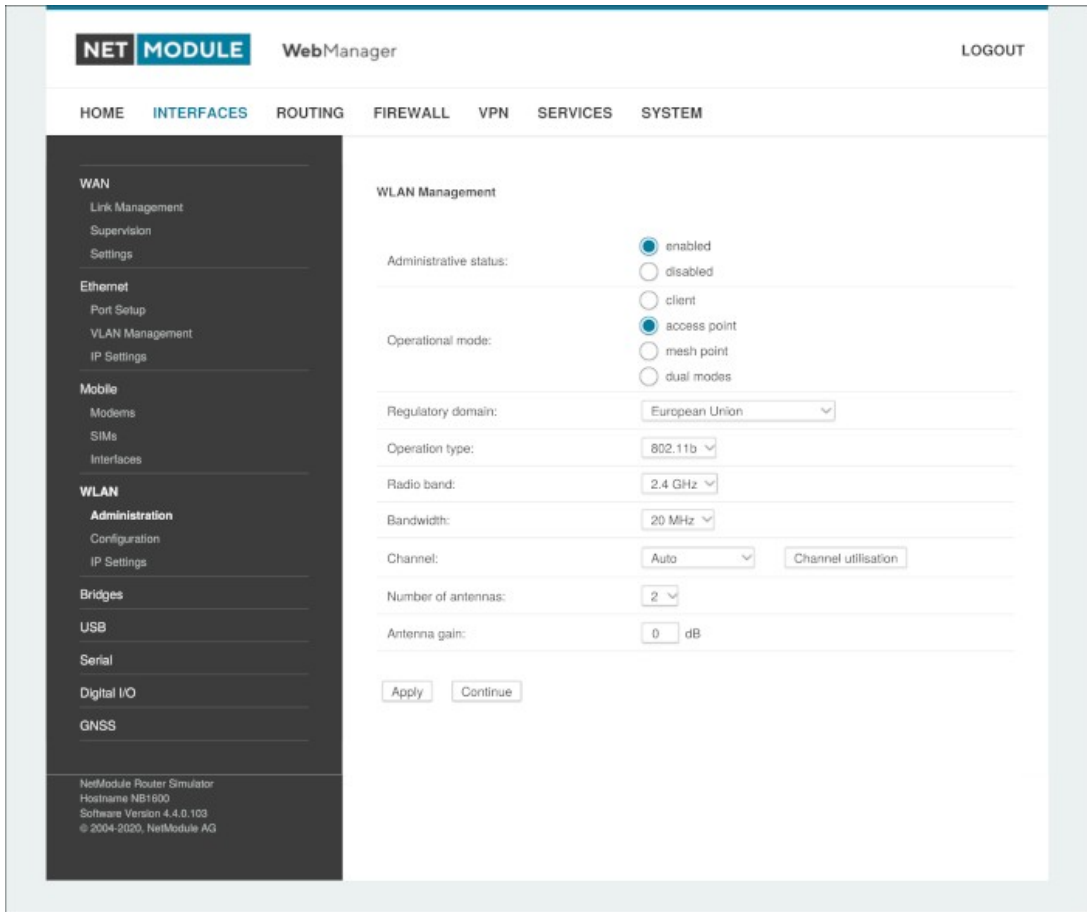
Interface	Modem	SIM	PDP	Number	Service	APN / User		
WWAN1	Mobile1	SIM1	PDP1	*99***1#	automatic	internet.telekom / tm	-	+

Ekran 6.62.: Mobil WWAN Yapılandırma

Mobil WWAN arayüzünü yapılandırın.

WLAN Yönetimi (WLAN Administration)

(Interfaces->WLAN->Administration)

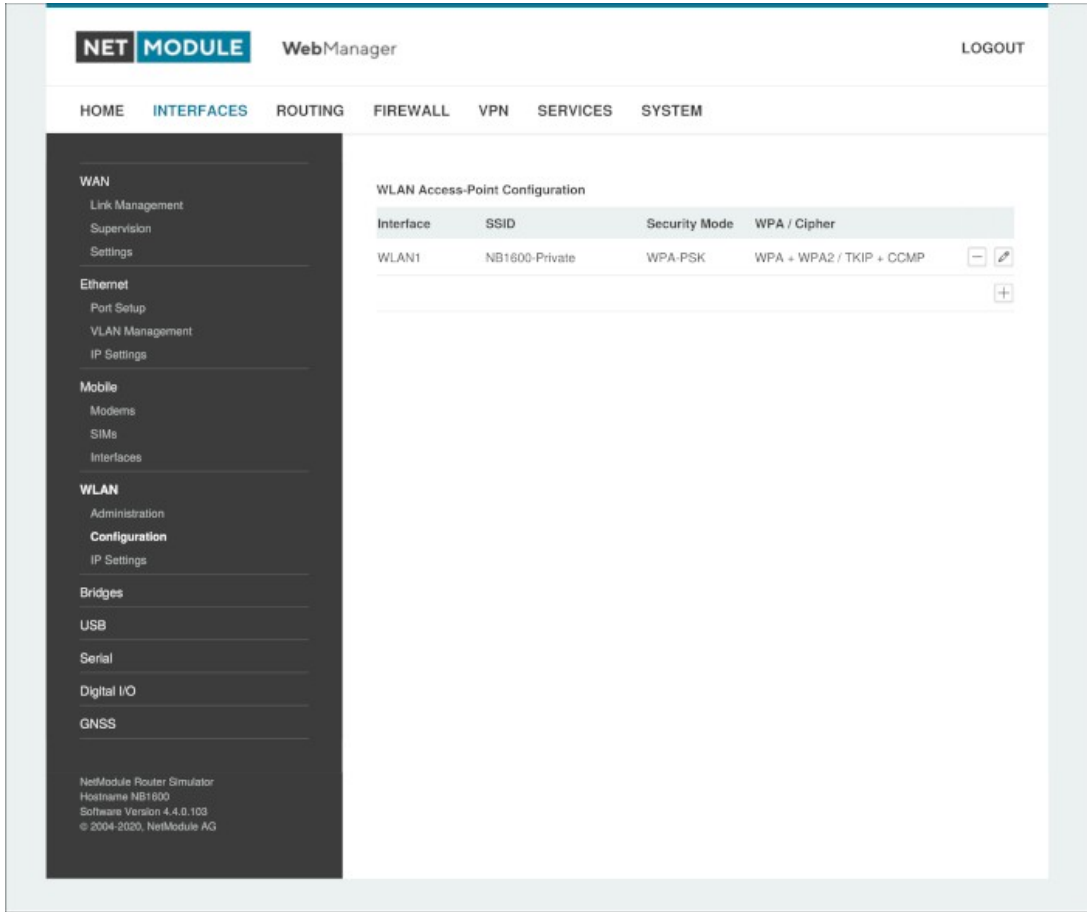
*Ekran 6.63.: WLAN Yönetimi*

Enable administration status and configure WLAN interface as follows:

Parametre	Ayar
Düzenleyici etki alanı (Regulatory domain)	Erişim noktasının kullanıldığı ülke
Çalıştırma tipi (Operation type)	En iyi uyumluluğu elde etmek için mümkünse 802.11n veya 802.11ac kullanın
Radyo bantı (Radio band)	2.4 Ghz'te çalışma
Bant genişliği (Bandwidth)	20Mhz
Kanal (Channel)	1 (2412 MHz)

WLAN Yapılandırma (WLAN Configuration)

(Interfaces->WLAN->Configuration)

*Ekran 6.64.: WLAN Yönetimi*

Devam et'e (continue) basın ve erişim noktası yapılandırma sayfasını takip edin. "Düzenle" (Edit) düğmesine tıklayarak WLAN arayüzünü ekleyin.

Parametre	Ayar
SSID	Hotspot
Güvenlik modu (Security mode)	Hiçbiri (none)

“Uygula” (Apply) butonunu kullanarak yapılandırmayı uygulayın.



Hotspot Arayüzü (Hotspot Interface)

(Services->Hotspot)

“+” düğmesine tıklayarak erişim noktası arayüzünü ekleyin

Yönetim durumunu etkinleştirin ve aşağıdaki yapılandırma ile devam edin:

Parametre	Ayar
Arayüz (Interface)	Arayüz olarak “WLAN1”i seçin
Portal adı (Portal name)	Portal adı olarak “Hotspot” yazın

“Uygula” (Apply) butonunu kullanarak yapılandırmayı uygulayın.

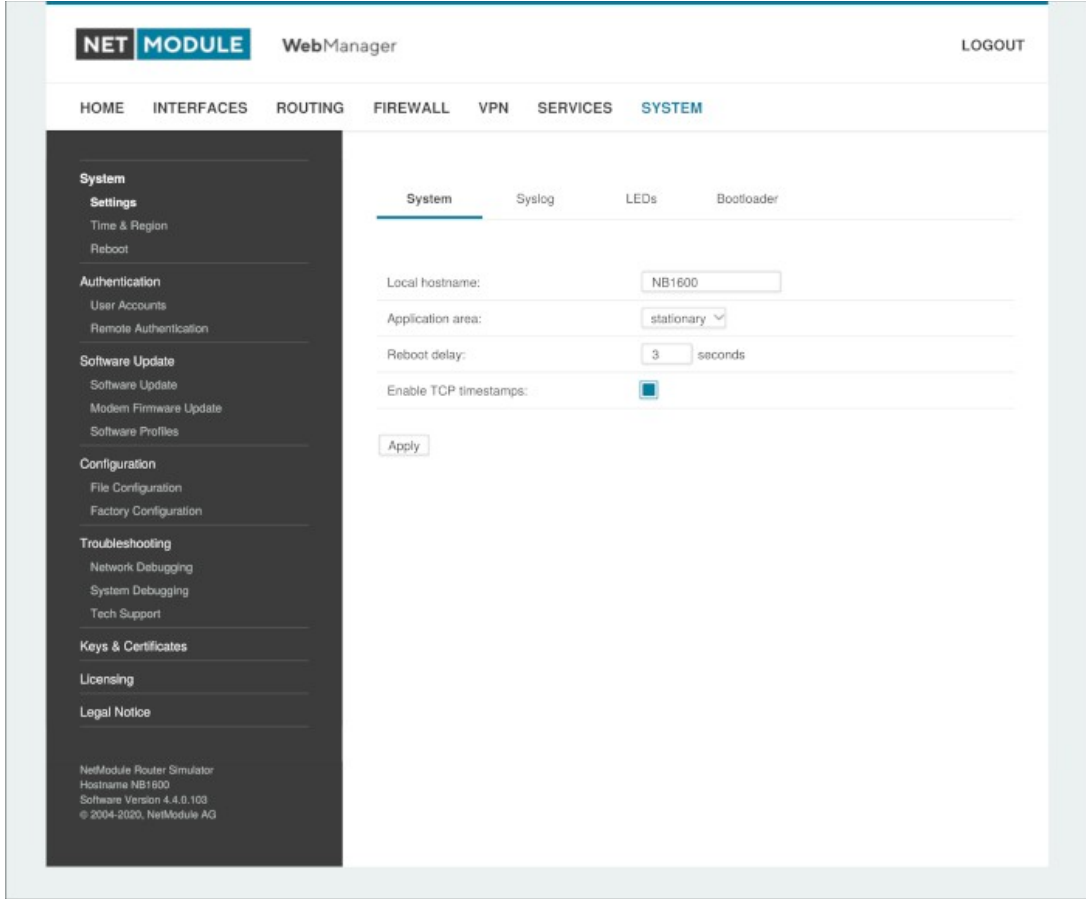
Sonuçlar (Results)

Artık bağlanan istemci ilk olarak captive portal sitesine yönlendirilecektir.

6.8. SİSTEM

6.8.1. Sistem

Sistem Ayarları



Ekran 6.65.: Sistem

Sistem

Aşağıdaki sistem parametreleri ayarlanabilir:

Parametre	Sistem Ayarları
Sistemin adı (Local hostname)	Sistemin (yönlendiricinin) adı
Uygulama alanı (Application area)	Mobil ortamlarda çalışırken kayıt zaman aşımı veya diğer uyarlamalar gibi sistem davranışını etkileyen istenen uygulama alanı.
Yeniden başlatma gecikmesi (Reboot delay)	Düzenli sistem yeniden başlatmalarından önce beklenecek saniye sayısı (sistem yeniden başlatma olayları <code>system-rebooting</code> için gerekli olabilir)



Parametre	Sistem Ayarları
TCP zaman damgalarını etkinleştir (Enable TCP timestamps)	Sistem genelinde TCP iletişimi için TCP zaman damgalarını etkinleştirin. Bu, Sarılmış Sıralı Numaralara Karşı Koruma (Protection Against Wrapped Sequence, PAWS) için gereklidir, ancak bu zaman damgaları etkinleştirildiğinde uzak bir saldırgan sistemin çalışma süresini tahmin edebilir. Çalışma süresi, çekirdek gibi ana sistem bileşenlerinin yaşı için bir alt sınırdır. Sistemin 3 yıllık bir çalışma süresi varsa, son güvenlik yamalarının uygulanmış olması olası değildir.
Giriş ekranında mesajları ve bilgileri göster (Show messages and infos on log-in screen)	Giriş ekranında hata mesajlarını ve bildirimleri göster. Bu seçenek etkinleştirilirse bu mesajlar kullanıcı kimlik bilgileriyle giriş yapmadan önce de gösterilir.

Syslog

Aşağıdaki syslog parametreleri ayarlanabilir:

Parametre	Syslog Ayarları
Depolama (Storage)	Günlük dosyalarının saklanacağı depolama aygıtı.
Azami dosya büyüklüğü (Max. filesize)	Döndürülecekleri zamana kadar günlük dosyalarının maksimum boyutu (kB cinsinden).
Yönlendirme adresi (Redirect address)	Günlük iletilerinin yönlendirileceği bir IP adresi belirtir. Windows için küçük bir sistem günlük sunucusu TFTP32'ye dahildir ve web sitemizden indirilebilir.

Genel olarak kutu, veri depolamak için kullanılabilen dahili bir flaş aygıtıyla birlikte gelir. Modelinize bağlı olarak bu, ek flaş veya USB disklerle genişletilebilir. Aşağıdaki depolama aygıtları mevcuttur:

Parametre	Depolama Ayarları
flash root	Dahili flaşın kök bölümü
flash data	Dahili flaşın veri bölümü
Genişletilmiş disk (Extended disk)	Genişletilmiş depolama disk
USB disk	Harici USB portuna bağlı bir depolama disk

LED'ler

Aşağıdaki LED parametreleri ayarlanabilir:

Parametre	LED Ayarları
LED	Cihazınızın ön panelindeki tüm durum LED'lerinin davranışını özelleştirebilirsiniz. Genellikle iki bankaya (üst/alt) ayrılırlar. Geçiş modunu yapılandırabilirsiniz, böylece LED'ler iki ayrı yapılandırılmış LED şeması arasında periyodik olarak dönüşür.



Önyükleyici (Bootloader)

Aşağıdaki önyükleyici parametreleri ayarlanabilir:

Parametre	Depolama Ayarları
Şifre (Password)	Önyükleyiciyi açmak için kullanılan parola. Boşsa, yönetici parolası kullanılacaktır.

Otomatik Çalıştırma (Autorun)

Bu özellik, harici bir depolama aygıtı takılır takılmaz bir kabuk betiğini otomatik olarak başlatmak veya bir yazılım/yapılandırma güncellemesi gerçekleştirmek için kullanılabilir. Kimlik doğrulaması için, FAT16/32 biçimli bir aygıtın kök dizininde `autorun.key` adlı bir dosya bulunmalıdır. Bu dosya o sayfadan indirilebilir ve `autorun` parolasının SHA256 hash anahtarını tutar. Dosya, kimlik doğrulaması sırasında satır satır işlenecek birden fazla hash tutabilir ve bu, farklı yönetici parolalarına sahip daha fazla sistem kurmak için kullanılabilir.

Boş parolaya sahip yeni cihazlar için karma anahtarı

`e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855` kullanılabilir.

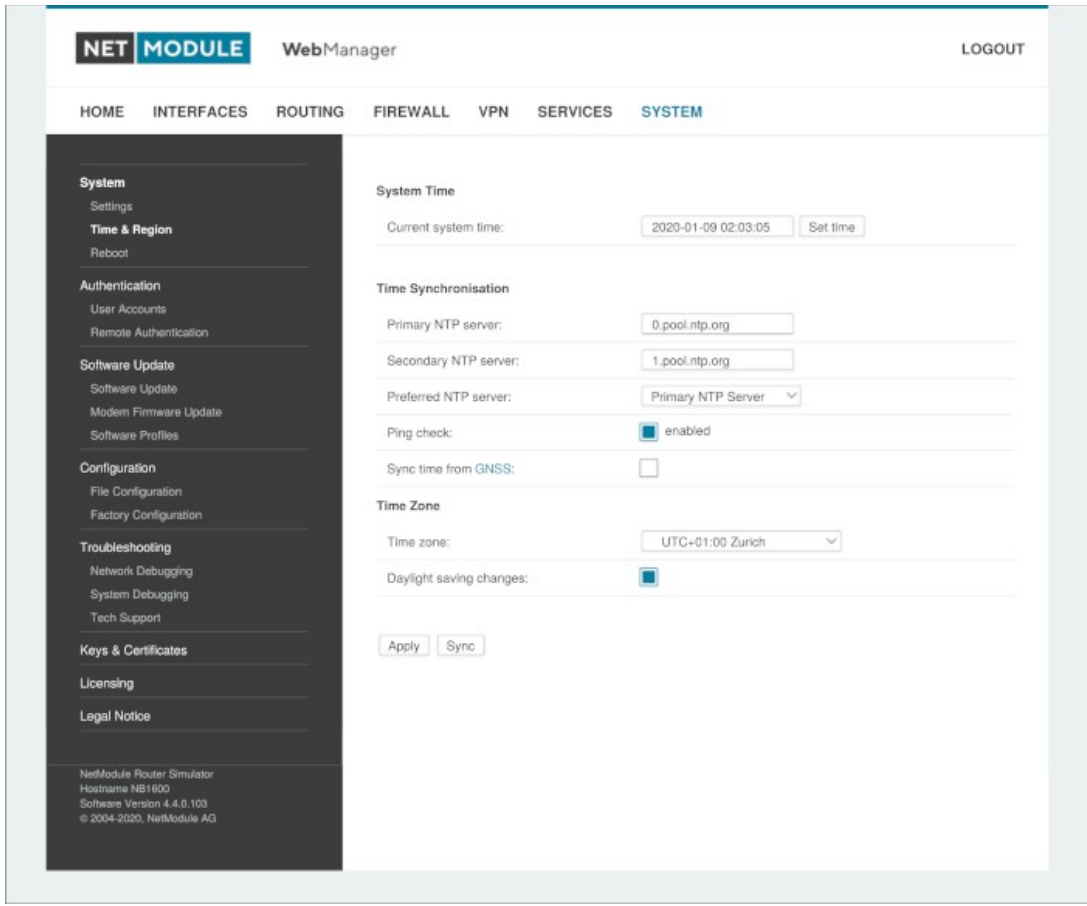
Karma anahtarlar, bir Linux sisteminde veya bir İnternet karma anahtar üreticinde `echo -n "<password>" | sha256sum` komutunu çalıştırarak üretilebilir ("sha-256 karma hesaplayıcı"yı arayın).

Kimlik doğrulama başarılı olduktan sonra, sistem kök dizinde aşağıdaki eylemleri gerçekleştirebilecek diğer dosyaları tarar:

1. Bir betiği çalıştırmak için: `autorun.sh`
2. Bir yapılandırma güncellemesi için: `cfg-<SERIALNO>.zip` (örn. `cfg-00112B000815.zip`) veya mevcut değilse `cfg.zip`
3. Bir yazılım güncellemesi için: `sw-update.img`

Zaman ve Bölge (Time & Region)

Bu sayfa sistem saatini ayarlamak ve saat dilimini yapılandırmak için kullanılabilir. Belirli saat diliminiz için yaz saati değişikliklerini daha da etkinleştirebilirsiniz. NetModule AG yönlendiricileri, Ağ Zaman Protokolü (Network Time Protocol, NTP) veya GNSS aracılığıyla bir veya daha fazla sunucu kullanarak sistem saatlerini senkronize edebilir. Etkinleştirilirse, zaman senkronizasyonu genellikle bir WAN bağlantısı kurulduktan sonra ancak herhangi bir VPN bağlantısı başlatılmadan önce tetiklenir. Daha fazla zaman senkronizasyonu döngüleri arka planda planlanır. Çoğu yönlendiricide pil destekli saat (RTC) yoktur. Bu durumda sistem saati önyükleme sırasında son geçerlilik saatine, örneğin güç kapatılmadan önce ayarlanır.



Ekran 6.66.: Bölgesel Ayarlar

Parametre	Zaman Senkronizasyonu
NTP Sunucu (NTP server)	Birincil NTP sunucusunun adresi
NTP Sunucu 2 (NTP server 2)	İsteğe bağlı olarak ikinci bir NTP sunucusunun adresi
Ping kontrolü (Ping check)	İlk zaman güncellemesi çalıştırılırken NTP sunucularının kullanılabilir olup olmadığını kontrol etmek için bir ICMP ping'i kullanır
GNSS'den zaman senkronizasyonu (Sync time from GNSS)	İlk GNSS cihazından zamanı türet (etkinleştirilmişse)

Parametre	Zaman Bölgesi
Zaman bölgesi (Time Zone)	Yerel saat dilimini ayarlayın.
Yaz saati uygulaması değişiklikleri (Daylight saving changes)	Yaz saati uygulamasını etkinleştirin/devre dışı bırakın.

Sanallaştırma (Virtualization)

Sanallaştırma teknikleri, ana bilgisayar sisteminin üstünde birden fazla izole edilmiş misafir çalıştırmak için kullanılabilir. Netmodule yönlendiricileri işletim sistemi düzeyinde sanallaştırma kullanır: Bir sistem işletim sistemi düzeyinde sanallaştırılır ve kapsayıcılar adı verilen birden fazla izole edilmiş kullanıcı alanı örneği etkinleştirilir. Misafir ortamlarını uygulamak için aynı işletim sistemi çekirdeği kullanılır, misafir ortamında çalışan uygulamalar bunu bağımsız bir sistem olarak görür.



Genel ayarlar:

Parametre	Sanallaştırma
Yönetimsel durum (Administrative status)	Sanallaştırmanın etkin olup olmadığını tanımlar

Sanal bir misafiri yapılandırmak için aşağıdaki parametreler kullanılabilir:

Parametre	Misafir Ayarları
Tip (Type)	Hangi sanallaştırma tekniğinin kullanıldığını tanımlar
Açıklama (Description)	Misafir hakkında açıklayıcı bilgiler
Depolama (Storage)	Misafirin kök dosya sisteminin bulunacağı depolama aygıtını belirtir

Bir kök dosya sistemi (root-file-system) kurmak için, bir görüntüyü yüklemek ve kurulumu tetiklemek üzere bir URL ayarlayabilirsiniz:

Parametre	Kurulum
URL	Görüntünün yükleneceği URL. Görüntünün, CPU mimarimizle uyumlu bir kök FS'nin dosyalarını içeren XZ sıkıştırılmış TAR arşivi olarak sağlanması gerekir (. İşlem için 'http://' veya 'https://', 'ftp://' veya 'tftp://' gibi farklı protokoller kullanılabilir. Görüntüyü önceden yönlendiriciye yüklediyseniz, dosyanın yerel yolunu izleyen 'file://' de kullanabilirsiniz. Talep üzerine çeşitli özel Linux dağıtım görüntüleri (Debian gibi) sağlayabiliriz.
Kurulum (Install)	Bu tetikleyici ayarlanırsa, görüntü indirme işlemi uygulama sırasında başlayacaktır. Mevcut herhangi bir kök dosya sistemi üzerine yazılacaktır. Bu parametre yapılandırmada saklanmayacaktır. Kurulum devam ettikten sonra değer sıfırlanacak ve yeni bir görüntü kurulacaksa tekrar ayarlanması gerekecektir.

Misafir ile iletişim, misafire yönlendirilebilen veya bir LAN arayüzü ile köprülenebilen ağ arayüzleri tanımlanarak sağlanabilir:

Parametre	Misafir Ağı
Misafir arayüzü (Guest interface)	Misafir arayüzünün adı
Mod (Mode)	Bu arayüz için ağ modu (yönlendirilmiş veya köprülenmiş)
Adres (Address)	Misafir arayüzünün IP adresi
Ağ maskesi (Netmask)	Misafir arayüzünün ağ maskesi
Ağ geçidi (Gateway)	Konuk içinde kullanılan ve aynı zamanda ana bilgisayar arayüzünde ayarlanan ağ geçidi
Köprü arayüzü (Bridge interface)	Misafir arayüzünün bağlanacağı arayüz

Misafir cihazları parametresi, misafir sistemine sağlanabilecek cihazların (örneğin bluetooth, CAN) bir listesini gösterir.

Parametre	Misafir Cihazları
Cihazları etkinleştir (Enable devices)	Misafir için cihazı etkinleştirin veya devre dışı bırakın



Bir misafirin kaynaklarını sınırlamak için aşağıdaki ayarlar uygulanabilir:

Parametre	Misafir Limitleri
CPU	Misafir için kullanılan CPU sayısı
Bellek (Memory)	Misafir için kullanılabilir bellek miktarı

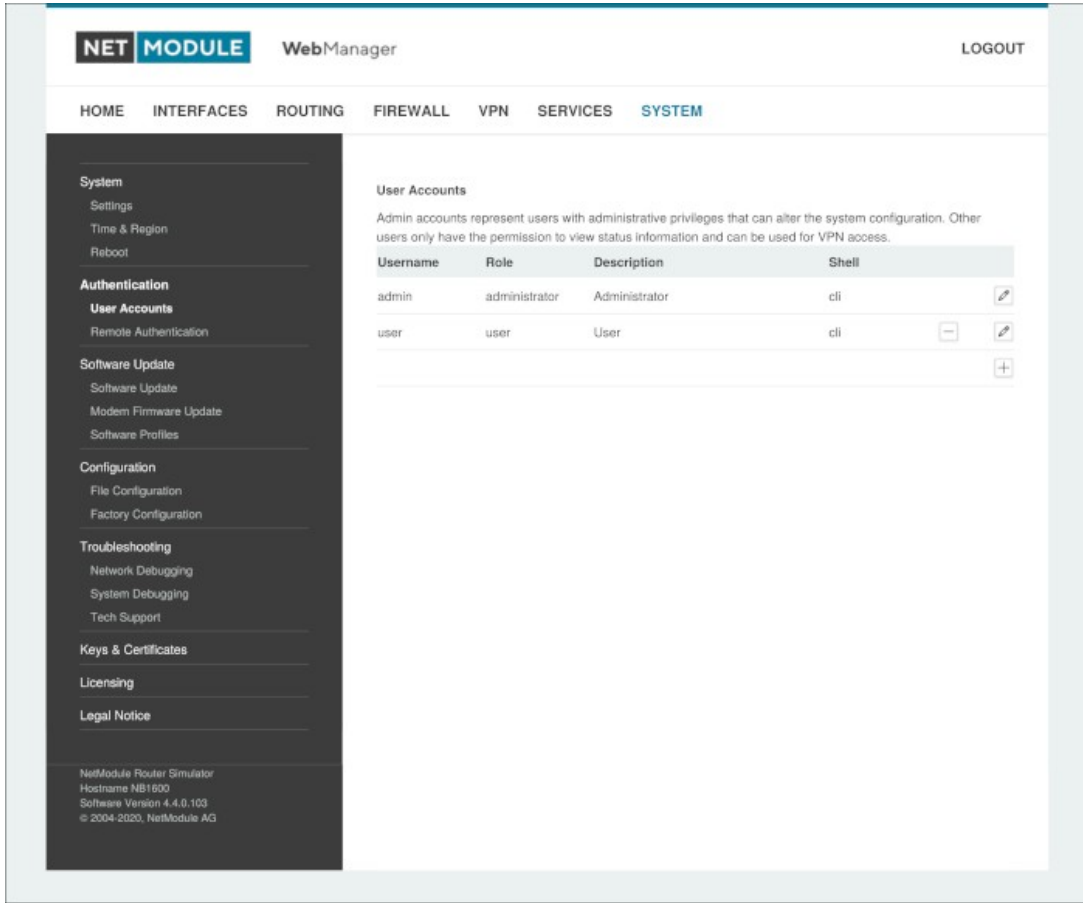
Yeniden Başlatma (Reboot)

Bu sayfa periyodik otomatik yeniden başlatmayı ayarlamak için kullanılabilir, ayrıca hemen verilecek manuel yeniden başlatmayı tetiklemek için de kullanılabilir.

6.8.2. Kimlik Doğrulama (Authentication)

Kullanıcı Hesapları (User Accounts)

Bu sayfayı kullanarak sistemdeki kullanıcı hesaplarını yönetebilirsiniz.



Ekran 6.67.: Kullanıcı Hesapları

Yönetici kullanıcısı, sistemin varsayılan yöneticisini temsil eden yerleşik bir güç kullanıcısıdır. Yönetici parolasının, bir sistem kabuğuna girebilen kök kullanıcıya da uygulanacağını lütfen unutmayın. Yönetici ayrıcalıklarına sahip başka yönetici hesapları eklenebilir, bunlar ayrıca sistem yapılandırmasını değiştirebilir veya yönetim sistemi görevlerini gerçekleştirebilir. Diğer kullanıcılar yalnızca durum bilgilerini görüntüleme iznine sahiptir. Ayrıca VPN erişimi için de kullanılabilirler.

Web Yöneticisi, 5'e kadar eşzamanlı kullanıcıyı destekler. Etkin olmayan kullanıcılar 30 dakika boyunca hareketsiz kaldıktan sonra atılır. Oturum açma başarılı olursa, diğer uzak ana bilgisayarlardan gelen tüm yinelenen kullanıcılar oturumdan çıkarılır. Uzak ana bilgisayarlar, 10 başarısız oturum açma girişiminden sonra 5 dakika boyunca engellenir.

Parametre	Kullanıcı Hesapları Yönetimi
Kullanıcı adı (Username)	Kullanıcının adı
Açıklama (Description)	Kullanıcı hakkında kısa açıklama
Rol (Role)	Yönetici (admin) veya kullanıcı (user)
Shell	Kullanıcının CLI'yi mi yoksa bir SHELL'i mi alacağını belirtir

Parametre	Kullanıcı Hesapları Yönetimi
Şifreyi şifrelenmemiş olarak sakla (Store password unencrypted)	Bu seçenek seçilirse kullanıcı parolası cihazda şifrelenmemiş olarak saklanır (önerilmez)
Eski şifre (Old password)	Kullanıcının eski şifresi
Yeni şifre (New password)	Kullanıcının yeni şifresi
Yeni şifreyi doğrula (Confirm new password)	Kullanıcının onaylanmış yeni şifresi

Lütfen ek yönetici kullanıcıları eklerken varsayılan yöneticinin şifresini girmeniz gerektiğini unutmayın.



Şifreleri Saklama

Normalde bir kullanıcının şifresi kriptografik olarak saklanır; bu, cihazlarda şifreleri işlemenin önerilen yoludur. Ancak ne yazık ki SNMP uygulaması parolanın cihazda şifrelenmemiş olarak saklanmasını zorunlu hale getirir.

Kullanıcılarınıza kısıtlayıcı bir şekilde erişim hakları verdiğinizden emin olun.

Uzaktan Kimlik Doğrulama (Remote Authentication)

Uzak kullanıcıları doğrulamak için bir RADIUS sunucusu kullanılabilir. Bu, Web Yöneticisi, WLAN ağı ve uzaktan kimlik doğrulamayı destekleyen ve içeren diğer hizmetler için geçerlidir.

NET MODULE WebManager LOGOUT

HOME INTERFACES ROUTING FIREWALL VPN SERVICES **SYSTEM**

System
Settings
Time & Region
Reboot

Authentication
User Accounts
Remote Authentication

Software Update
Software Update
Modem Firmware Update
Software Profiles

Configuration
File Configuration
Factory Configuration

Troubleshooting
Network Debugging
System Debugging
Tech Support

Keys & Certificates

Licensing

Legal Notice

NetModule Router Simulator
Hostname: NB3800
Software Version: 4.4.0.103
© 2004-2020, NetModule AG

Remote Authentication

Administrative Status: enabled
 disabled

Use for login:

Primary RADIUS Configuration

Server address: 192.168.1.200

Secret: *****

Authentication port: 1812

Accounting port: 1813

Secondary RADIUS Configuration

Server address:

Secret:

Authentication port: 1812

Accounting port: 1813

Apply

Ekran 6.68.: Uzaktan Kimlik Doğrulama



Aşağıdaki şekilde yapılandırılabilir:

Parametre	Uzaktan Kimlik Doğrulama
Yönetimsel durum (Administrative status)	Kimlik doğrulama için uzak bir sunucunun kullanılıp kullanılmayacağını tanımlar
RADIUS sunucu (RADIUS server)	RADIUS sunucu adresi
RADIUS sırrı (RADIUS secret)	RADIUS sunucusuna karşı kimlik doğrulaması için kullanılan sır
Kimlik doğrulama portu (Authentication port)	Kimlik doğrulama için kullanılan port
Hesap portu (Accounting port)	Hesap işlemleri için kullanılan port
Giriş için kullan (Use for login)	Bu seçenek, uzaktan tanımlanmış kullanıcıların Web Yöneticisine erişmesine olanak tanır, aksi takdirde yalnızca açıkça yapılandırılmış hizmetler (ör. WLAN) tarafından kullanılır

6.8.3. Yazılım Güncelleme (Software Update)

Elle Yazılım Güncelleme (Manual Software Update)

Bu menü sistemin manuel yazılım güncellemesini çalıştırmak için kullanılabilir.

Parametre	Elle Yazılım Güncelleme
Güncelleme işleme (Update operation)	Kullanılan güncelleme işlemi yöntemi. Görüntüyü yükleyebilir, bir URL'den indirebilir veya sunucumuzdaki en son sürümü kullanabilirsiniz
URL	Yazılım güncelleme görüntüsünün indirileceği sunucu URL'si
Yönetim şifresi (Administrator password)	4.2.x'ten önceki sürümlere geri dönüş için yönetici parolası



Dikkat

Yazılım ("SW") 4.2 sürümünden başlayarak varsayılan olarak parolaları parola karmaları kullanarak kaydetmemeye ayarladık. Kullanıcılar için parolaları depolamak etkinleştirilebilir, ancak yeni uygulamalar için önerilmez.

Daha eski SW sürümleri parolaların cihazda şifrelenmiş olarak depolanmasını gerektirir. 4.2 ve sonraki sürümlerde artık bunlara sahip olmadığımız için 4.1.x ve daha düşük bir sürüme geçmek istiyorsanız yönetici parolasını sağlamanız gerekecektir. Aynı parola ifadesi önyükleyici girişi için de kullanılacaktır.

Cihazda parolası depolanmamış tüm kullanıcılar, yeni parolalar uygulanana kadar düşürme işleminden sonra giriş yapamayacaktır.

Tekdüzen Kaynak Bulucu (Uniform Resource Locator, URL) aşağıdaki biçime sahip olabilir:

```
http://<username>:<password>@<host>:<port>/<path>  
https://<username>:<password>@<host>:<port>/<path>  
ftp://<username>:<password>@<host>:<port>/<path>  
sftp://<username>:<password>@<host>:<port>/<path>  
tftp://<host>/<path>  
file:///<path>
```

Bir yazılım güncellemesi yayınlandığında, geçerli yapılandırma (anahtarlar/sertifikalar gibi dosyalar dahil) yedeklenir. Dosya sistemindeki diğer değişiklikler silinir. Yapılandırma genellikle geriye dönük uyumludur. Aynı sürüm satırındaki önceki bir yazılıma geri dönüş yaparken de ileriye dönük uyumluluk uygularız; bu, aslında ayarların ve özelliklerin kaybına yol açabilecek bilinmeyen yapılandırma yönergelerini ayıklayarak gerçekleştirilir. Bu nedenle, çalışan yapılandırmanın bir kopyasını saklamak her zaman iyi bir fikirdir.



Dikkat

Önceki bir sürüm hattında (ör. 3.7.0'dan 3.6.0'a) büyük bir düşürme yapmanız durumunda, lütfen yalnızca bunların tam olarak ileriye dönük uyumlu olma eğiliminde olması nedeniyle her zaman o dalın en son sürümünü (ör. 3.6.0.X) kullandığınızdan emin olun. Ayrıca, bazı donanım özelliklerinin çalışmayabileceğini (ör. o sürümde uygulanmamışsa) unutmayın. Şüphenez varsa lütfen destek ekibimize danışın.



Bir yazılım görüntüsü Web Yöneticisi aracılığıyla yüklenebilir veya belirli bir URL'den alınabilir. Paketten çıkarılacak ve güncelleme başarıyla tamamlanırsa etkinleştirilen yedek bir bölüme dağıtılacaktır. Tüm prosedüre tüm yeşil LED'lerin yanıp sönmeye eşlik eder, sonraki sistem yeniden başlatması yavaşça yanıp sönen bir Durum LED'i ile belirtilir. Yedeklenen yapılandırma önyükleme sırasında uygulanır ve Durum LED'i bu işlem sırasında daha hızlı yanıp söner. Yapılandırmanıza bağlı olarak bu biraz zaman alabilir.

Otomatik Yazılım Güncelleme (Automatic Software Update)

Bu menü sistemin otomatik yazılım güncellemesini çalıştırmak için kullanılabilir.

Parametre	Otomatik Yazılım Güncelleme
Durum (Status)	Otomatik yazılım güncellemesini etkinleştir/devre dışı bırak
Günün zamanı (Time of day)	Her gün bu saatte yönlendirici güncelleme kontrolü yapacaktır
İşlem (Operation)	Sunucudan en son görüntüyü indirin veya yazılım güncelleme paketinin indirilmesi gereken URL'yi belirtin. Desteklenen protokoller TFTP, HTTP, HTTPS ve FTP'dir. protocol://server/path/file gibi bir URL sağlayın

Not: HTTPS URL'lerinin SSL sertifikaları yalnızca 6.8.8 altında CA kök sertifikalarının bir listesi sağlanırsa doğrulanacaktır.

Yeni yazılım yüklendikten sonra, önyükleme sırasında en son çalışan yapılandırma uygulanacaktır. Bu, Durum LED'inin daha hızlı yeşil yanıp sönmeyeyle belirtilir.

6.8.4. Modül Donanım Yazılımı Güncelleme (Module Firmware Update)

Bu menü belirli bir modülün donanım yazılımı güncellemesini gerçekleştirmek için kullanılabilir.

Parametre	Modül Donanım Yazılımı Güncelleme
Güncelleme işlemi (Update operation)	Kullanılan güncelleme işlemi yöntemi. Bir aygıt yazılımı paketini yükleyebilir veya belirli bir URL'den indirebilirsiniz.
Modül (Module)	Güncellenmesi gereken modül.
Depolama (Storage)	Güncelleme prosedürü için kullanılacak geçici depolama. Sınırlı miktarda flaşa sahip kutular için USB bölümünde düzgün bir şekilde ayarlanmış ve ext4 gibi uygun bir dosya sistemi barındıran bir USB çubuğu kullanmak mümkündür.
URL	Yazılım paketinin indirilmesi gereken sunucu URL'si (örn. protokol://sunucu/yol/dosya). Desteklenen protokoller TFTP, HTTP, HTTPS ve FTP'dir. Sınırlı miktarda flaşa sahip kutular için usb0://<yol-yazılım-paketi> de kullanabilirsiniz.

Bir firmware paketi (ZIP) genellikle bir flash yardımcı programı, bir bilgi dosyası ve karşılık gelen firmware dosyalarından oluşur. En son sürümü edinmek için lütfen <https://support.netmodule.com> adresini takip edin.

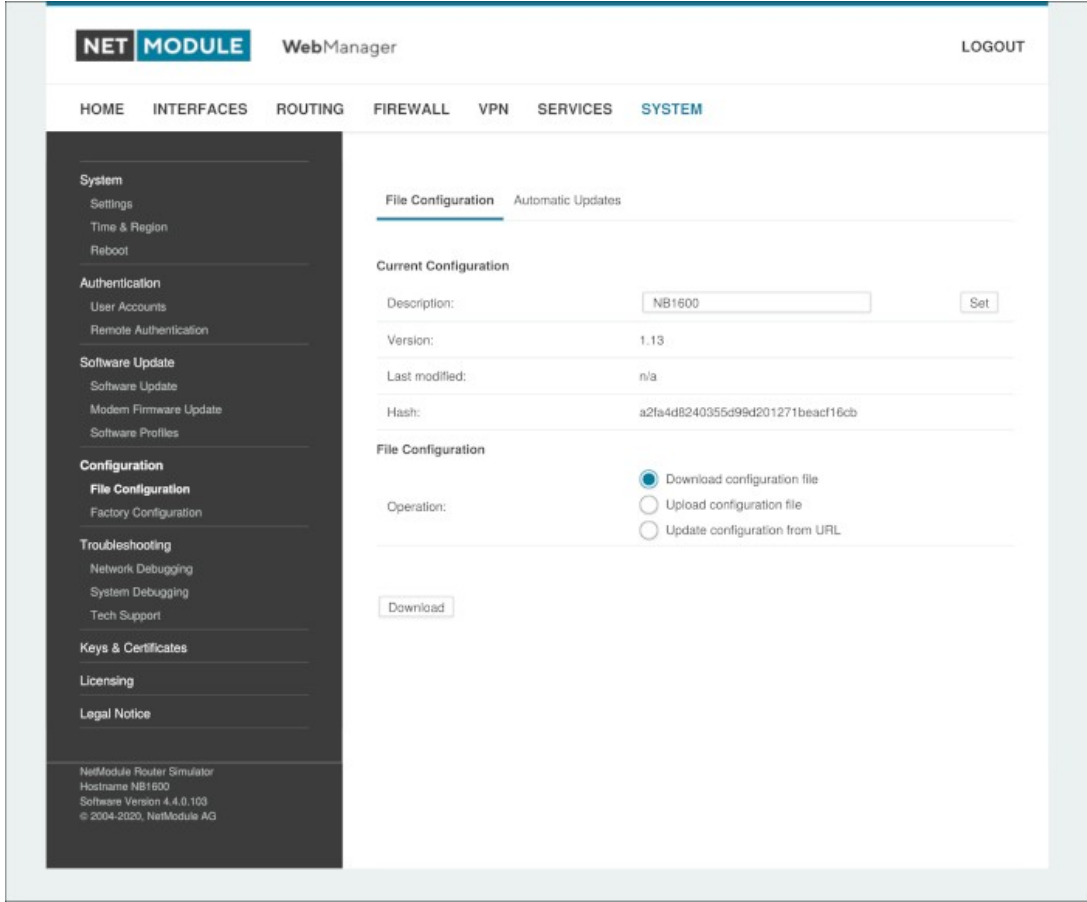
6.8.5. Yazılım Profilleri (Software Profiles)

Sistem, farklı yazılım sürümlerini tutabilen iki kök bölümden oluşur ve bu menü bunlar arasında geçiş yapmak için kullanılabilir. Bunu yaparak, daha yeni bir yazılım sürümünü test edebilir ve işler ters giderse kolayca geri dönebilirsiniz.

6.8.6. Yapılandırma

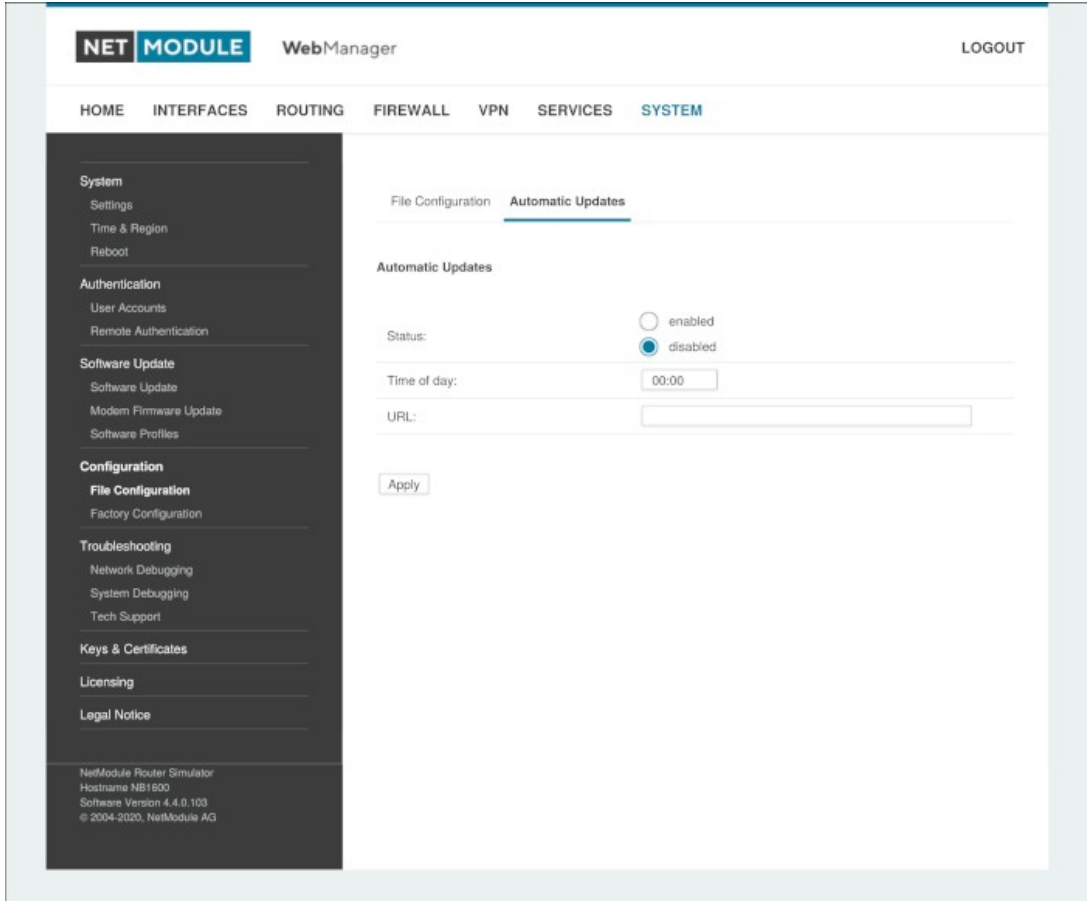
Web Yöneticisi üzerinden yapılandırma, daha büyük cihaz hacimleri için sıkıcı hale gelir. Bu nedenle yönlendirici, işleri otomatikleştirmek için otomatik ve manuel dosya tabanlı yapılandırma sunar. Sistemi başarıyla kurduğunuzda yapılandırmayı yedekleyebilir ve daha sonra sistemi bununla geri yükleyebilirsiniz. Kök dizine yapılandırma dosyasını ve diğer temel dosyaların (sertifikalar gibi) paketlenmiş bir sürümünü içeren tek bir yapılandırma dosyası (.cfg) veya tam bir paket (.zip) yükleyebilirsiniz.

Manuel Dosya Yapılandırması



Ekran 6.69.: Elle Dosya Yapılandırma

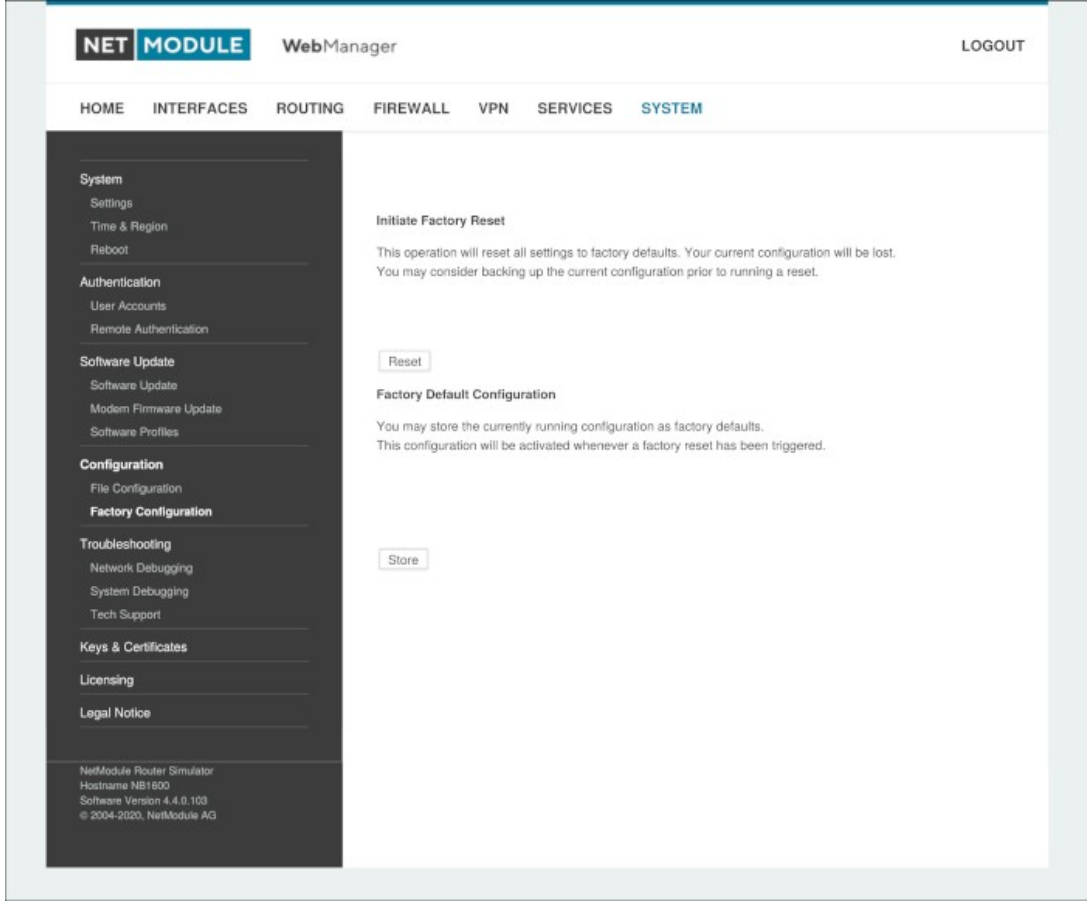
Bu bölüm, şu anda çalışan sistem yapılandırmasını (sertifikalar gibi temel dosyalar dahil) indirmek için kullanılabilir. Belirli bir yapılandırmayı geri yüklemek için daha önce indirilmiş bir yapılandırmayı yükleyebilirsiniz. Eksik yapılandırma yönergelerinin fabrika varsayılanlarına ayarlanması veya yok sayılması arasında seçim yapabilirsiniz, bu da potansiyel olarak var olan yapılandırma yönergelerinin sistemde tutulacağı anlamına gelir.

Otomatik Dosya Yapılandırma (Automatic File Configuration)

Ekran 6.70.: Otomatik Dosya Yapılandırma

Bu menü sistemin otomatik yapılandırma güncellemesini çalıştırmak için kullanılabilir. Aşağıdaki gibi yapılandırılır:

Parametre	Otomatik Dosya Yapılandırma
Durum (Status)	Otomatik yapılandırma güncellemesini etkinleştir/devre dışı bırak
Günün zamanı (Time of day)	Sistemin güncellemeleri kontrol etmesi gereken günün saati
İşlem (Operation)	Yapılandırma dosyasının alınacağı URL (desteklenen protokoller HTTP, HTTPS, TFTP, FTP'dir)

Fabrika Yapılandırması (Factory Configuration)

Ekran 6.71.: Fabrika Yapılandırması

Bu menü, cihazı fabrika varsayılanlarına sıfırlamak için kullanılabilir. Mevcut yapılandırmanız kaybolacaktır. Başarılı bir şekilde başlatılan fabrika sıfırlaması, tüm LED'lerin yanmış olmasıyla fark edilebilir. Fabrika sıfırlaması, ilk Ethernet arayüzünün IP adresini 192.168.1.1'e geri ayarlayacaktır. Varsayılan ağ parametrelerini kullanarak cihazla tekrar iletişim kurabileceksiniz. Şu anda çalışan yapılandırmayı, bir fabrika sıfırlaması başlatıldığında bile (örneğin servis personeliniz tarafından) etkin kalacak fabrika varsayılanları olarak kaydedebilirsiniz.

Lütfen bunun çalışan bir yapılandırmaya karşılık geldiğinden emin olun. Varsayılan ayarlara gerçek bir fabrika sıfırlaması, orijinal fabrika yapılandırmasını geri yükleyerek ve fabrika sıfırlamasını tekrar başlatarak gerçekleştirilebilir.



6.8.7. Sorun giderme (Troubleshooting)

Ağ Hata Ayıklama (Network Debugging)

Ağ hata ayıklama için ping, traceroute, tcpdump ve darkstat gibi çeşitli araçlar bulunmaktadır.

Parametre	Ayar
Ping	Ping yardımcı programı, uzak bir ana bilgisayara IP üzerinden ulaşıp ulaşılamadığını doğrulamak için kullanılabilir.
Traceroute	Traceroute yardımcı programı, rota paketlerinin izini uzak bir ana bilgisayara yazdırmak için kullanılabilir.
Tcpdump	tcpdump yardımcı programı, daha sonra Wireshark ile analiz edilebilecek bir arayüzün ağ yakalama (PCAP) görüntüsünü oluşturur.



Sistem Hata Ayıklama (System Debugging)

Burada *Debug log* seçeneğini seçerek sistem günlüğünü görüntüleyebilirsiniz veya önyükleme günlüğüyle ilgileniyorsanız *Boot log*'u seçin.

Kutuda neler olup bittiğini görmenin bir başka yolu da `root` olarak bir SSH veya Telnet oturumu açmak ve `tail - log` yazmaktır.

Ayrıca sistem günlüğü bir syslog sunucusuna yönlendirilebilir, bkz. Bölüm 6.8.1.

NET MODULE WebManager LOGOUT

HOME INTERFACES ROUTING FIREWALL VPN SERVICES **SYSTEM**

System Debugging

Log Viewer Debug Levels

Show all of system log Reset

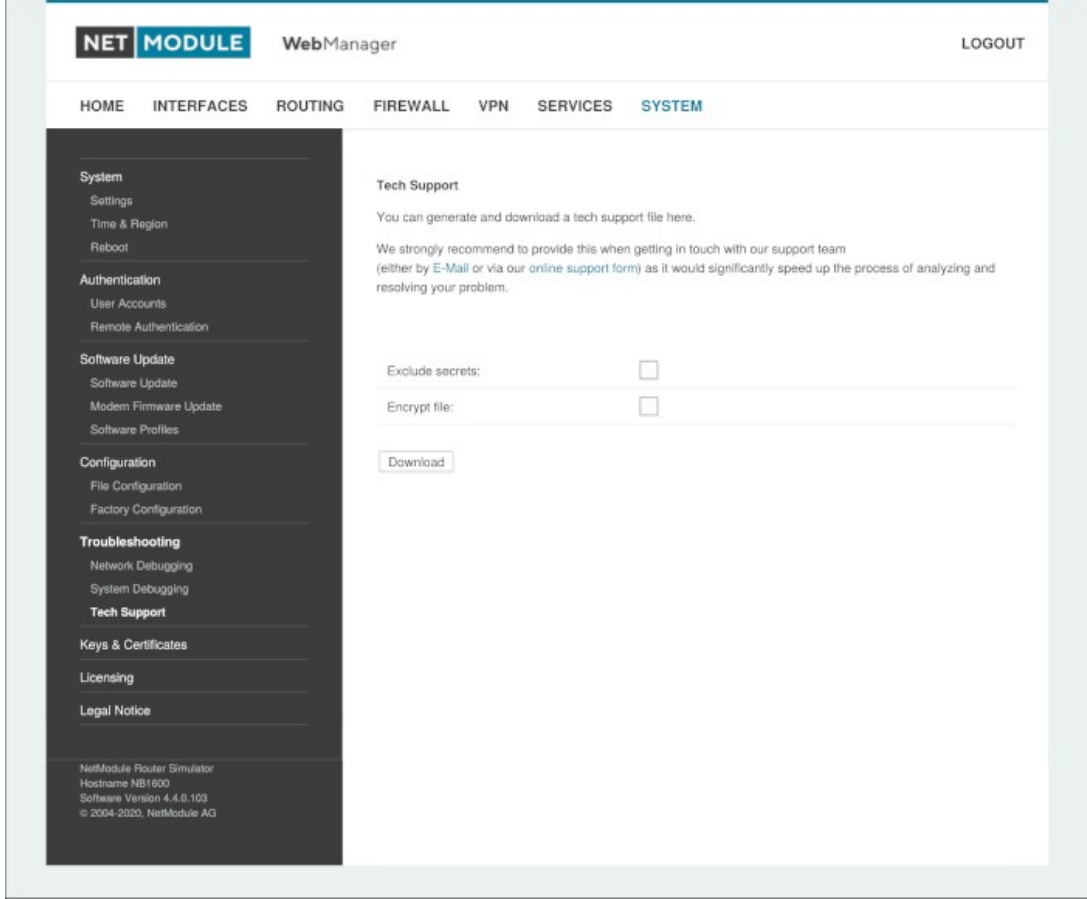
```
Jan 9 02:01:54 NB1600 dsemon.debug hostapd: wlan0: WPA rekeying GTK
Jan 9 02:02:13 NB1600 user.err link-manager(27880): wlanlink0: link is dialing too long (36s)
Jan 9 02:02:13 NB1600 user.notice link-manager(27880): wlanlink0: permanent link is suspended for 10s (set suspended [auto])
Jan 9 02:02:15 NB1600 user.err mobile-node(17795): Could not determine care-of address! (No route to home agent?)
Jan 9 02:02:15 NB1600 user.err mobile-node(17795): Could not determine care of address!
Jan 9 02:02:15 NB1600 user.err mobile-node(17795): TunnelController::sendRegistrationRequest() failed!
Jan 9 02:02:15 NB1600 user.err mobile-node(17795): Could not send registration request!
Jan 9 02:02:18 NB1600 user.notice link-manager(27880): wlanlink1: suspending link after 5 attempts
Jan 9 02:02:19 NB1600 user.notice link-manager(27880): wlanlink1: permanent link is suspended for 10s (set suspended [auto])
Jan 9 02:02:19 NB1600 user.notice link-manager(27880): wlanlink0: permanent link is unsuspending now (reset suspended [auto])
Jan 9 02:02:31 NB1600 user.notice link-manager(27880): wlanlink1: permanent link is unsuspending now (reset suspended [auto])
Jan 9 02:02:31 NB1600 user.notice link-manager(27880): wlanlink1: notify wlan0 setup 0 automatic
Jan 9 02:02:37 NB1600 user.err surveyor(27912): ipsec tunnel0 is down since 60s, reloading
Jan 9 02:02:45 NB1600 user.err mobile-node(17795): Could not determine care-of address! (No route to home agent?)
Jan 9 02:02:45 NB1600 user.err mobile-node(17795): Could not determine care of address!
Jan 9 02:02:45 NB1600 user.err mobile-node(17795): TunnelController::sendRegistrationRequest() failed!
Jan 9 02:02:45 NB1600 user.err mobile-node(17795): Could not send registration request!
Jan 9 02:02:54 NB1600 user.err link-manager(27880): wlanlink0: link is dialing too long (36s)
Jan 9 02:02:54 NB1600 user.notice link-manager(27880): wlanlink0: permanent link is suspended for 10s (set suspended [auto])
Jan 9 02:03:00 NB1600 user.warn config(25199): get values: key [network.lan.200.address] does not exist
Jan 9 02:03:00 NB1600 user.warn config(25199): get values: key [network.lan.200.netmask] does not exist
Jan 9 02:03:00 NB1600 user.warn config(25199): get values: key [network.lan.200.mode] does not exist
Jan 9 02:03:01 NB1600 user.notice link-manager(27880): wlanlink1: suspending link after 5 attempts
Jan 9 02:03:01 NB1600 user.notice link-manager(27880): wlanlink1: permanent link is suspended for 10s (set suspended [auto])
Jan 9 02:03:01 NB1600 user.notice link-manager(27880): wlanlink0: permanent link is unsuspending now (reset suspended [auto])
```

NetModule Router Simulator
Hostname NB1600
Software Version 4.4.0.103
© 2004-2020, NetModule AG

Ekran 6.72.: Log Görüntüleyici

Teknik Destek (Tech Support)

Burada bir teknik destek dosyası oluşturabilir ve indirebilirsiniz. Destek ekibimize e-posta veya çevrimiçi destek forumumuz aracılığıyla iletişime geçtiğinizde bu dosyayı sağlamanızı şiddetle öneririz, çünkü bu, sorununuzu analiz etme ve çözme sürecini önemli ölçüde hızlandıracaktır. Günlük dosyaları burada görüntülenebilir, indirilebilir ve sıfırlanabilir. Herhangi bir sorun olması durumunda lütfen bunları dikkatlice inceleyin. Olası yapılandırma sorunlarının daha fazla analizi için bu sayfada çeşitli araçlar bulunmaktadır.

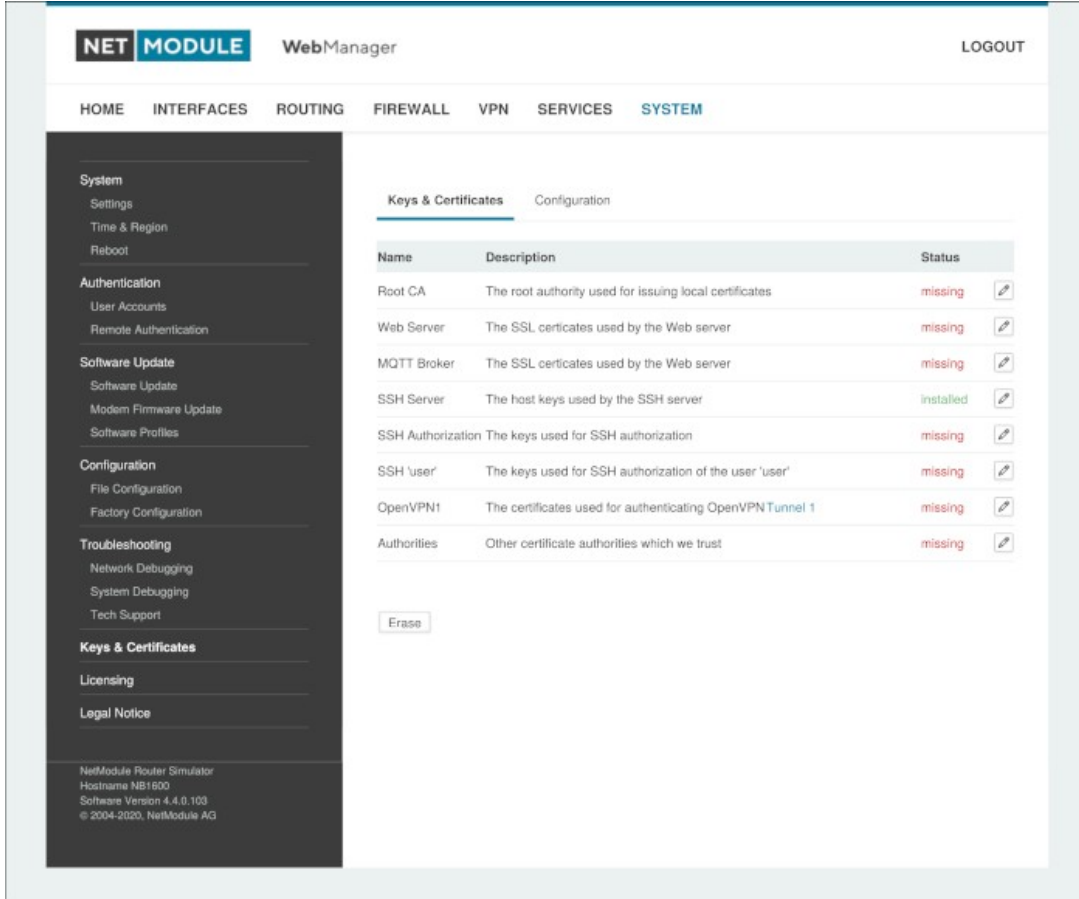


Ekran 6.73.: Teknik Destek Dosyası

Herhangi bir IP arayüzünü izlemek ve ana bilgisayarlar arasındaki bireysel paket akışlarını incelemek mümkündür. Bu, kutuya giriş yaparak ve tcpdump aracını kullanarak bir ağ paketi yakalama başlatarak gerçekleştirilebilir. Daha sonra ad çözümlemesini atlatmak için geçiş yapmanızı öneririz (örn. tcpdump -n -i lan0). Ayrıca Web Yöneticisi'ni kullanarak PCAP formatında bir döküm oluşturabilir, bilgisayarınıza indirebilir ve Wireshark ile daha fazla inceleme gerçekleştirebilirsiniz (www.wireshark.org adresinde mevcuttur).

6.8.8. Anahtarlar ve Sertifikalar (Keys and Certificates)

Anahtar ve sertifika sayfası, hizmetlerinizi (HTTP ve SSH sunucusu gibi) güvence altına almak için gerekli dosyaları oluşturmanıza olanak tanır, ayrıca sertifika tabanlı VPN tünelleri ve WLAN istemcileri için kimlik doğrulama ve şifreleme uygulamanıza da olanak tanır.



Ekran 6.74.: Anahtar ve Sertifikalar

Giriş sayfaları, yüklü anahtarlar ve sertifikalar hakkında genel bir bakış sunar. Aşağıdaki bölümler görünebilir:

Parametre	Açıklamalar
Root CA	Sertifikaları veren kök Sertifika Yetkilisi (CA), anahtarı diğer sistemlerdeki güvenilir üçüncü taraflarca sertifikalandırılmak için kullanılabilir
Web sunucu (Web server)	HTTP over SSL (HTTPS) çalıştırmak için gereken Web sunucusu sertifikaları.
MQTT Broker	TLS üzerinden şifrelenmiş bağlantı ile MQTT çalıştırmak için gereken MQTT Broker sertifikaları.
SSH Sunucu (SSH server)	SSH sunucusu için DSS/DSA anahtarları.
SSH kimlik doğrulama (SSH Authorization)	SSH yetkilendirmesi için kullanılan anahtarlar.
OpenVPN	OpenVPN tünellerini çalıştırmak için sunucu veya istemci anahtarları ve sertifikaları.
IPsec	IPsec tünellerini çalıştırmak için sunucu veya istemci anahtarları ve sertifikaları.

Tip	Açıklamalar
WLAN	Sertifika tabanlı WLAN kimlik doğrulamasını (örneğin WPA-EAP-TLS) uygulamak için anahtarlar ve sertifikalar.
ETH	Ethernet portlarında IEEE 802.1X üzerinden kimlik doğrulama için anahtarlar ve sertifikalar.
Otoriteler (Authorities)	SSL istemci bağlantıları kurarken güvendiğimiz diğer sertifika otoriteleri.

Tablo 6.196.: Sertifikalar Kısmı

Her sertifika bölümü için aşağıdaki işlemleri yapmak mümkündür:

İşlem	Açıklamalar
Yerel olarak üret (generate locally)	Anahtarı ve sertifikayı kutuda yerel olarak oluşturun (daha fazla seçenek için 6.8.8'e bakın)
Dosyaları yükleyin (upload files)	Anahtar ve sertifika yüklenecek. PKCS12, PKCS7, PEM/DER formatındaki dosyaları ve OpenSSH veya Dropbear formatındaki RSA/DSS anahtarlarını destekliyoruz.
SCEP aracılığıyla kaydolun (enroll via SCEP)	Anahtarı ve sertifikayı SCEP aracılığıyla kaydedin (daha fazla seçenek için 6.8.8'e bakın)
Sertifikayı indir (download certificate)	Anahtarı ve sertifikayı ZIP formatında indirin (dosyalar PEM formatında kodlanacaktır)
İmza isteği oluştur (create signing request)	Anahtarı yerel olarak oluşturun ve başka bir yetkili tarafından imzalanmış bir sertifikayı almak için bir imzalama isteği oluşturun
Sertifika sil (erase certificate)	Bu bölümle ilişkili tüm anahtarları ve sertifikaları silin

Tablo 6.197.: Sertifika İşlemleri

Yapılandırma

NET MODULE WebManager LOGOUT

HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM

System
Settings
Time & Region
Reboot

Authentication
User Accounts
Remote Authentication

Software Update
Software Update
Modem Firmware Update
Software Profiles

Configuration
File Configuration
Factory Configuration

Troubleshooting
Network Debugging
System Debugging
Tech Support

Keys & Certificates

Licensing

Legal Notice

NetModule Router Simulator
Hostname NB1600
Software Version 4.4.0.103
© 2004-2020, NetModule AG

Keys & Certificates Configuration

Organization (O) NetModule

Department (OU) Networking

Location (L) Switzerland

State (ST) Switzerland

Country (C) Switzerland

Common Name (CN) NB1600

E-Mail router@support.netmodule.com

Expiry period: 7300 days

Key size: 2048 bits

DH primes: 2048 bits

Signature: sha256

Cipher: aes256

Passphrase: *****

SCEP Configuration

SCEP Status: enabled disabled

Apply

Ekran 6.75.: Sertifika Yapılandırma

Bu sayfa, anahtarlar ve sertifikalar üzerinde çalışırken uygulanacak bazı genel yapılandırma seçenekleri sağlar. Anahtarlar, sertifikalar ve imzalama istekleri yerel olarak üretilirse, aşağıdaki ayarlar dikkate alınacaktır:

Parametre	Sertifika Yapılandırma
Organizasyon (Organisation (O))	Sertifika sahibinin kuruluşu
Departman (Department (OU))	Sertifika yayıncısının ait olduğu kuruluş biriminin adı
Konum (Location (L))	Sertifika sahibinin konumu
Eyalet (State (ST))	Sertifika sahibinin bulunduğu eyalet/şehir
Ülke (Country (C))	Sertifika sahibinin ülkesi (genellikle bir TLD kısaltması)
Bilinen adı (Common Name (CN))	Sertifika sahibinin genel adı, esas olarak bir ana bilgisayarı tanımlamak için kullanılır
E-posta (E-mail)	Sertifika sahibinin e-posta adresi
Son kullanma tarihi (Expiry period)	Sertifikanın bundan sonra geçerli olacağı gün sayısı
Anahtar büyüklüğü (Key size)	Özel anahtarın bit cinsinden uzunluğu
DH asal sayıları (DH primes)	Özel Diffie-Hellman asal sayıları için bit sayısı
İmza (Signature)	Sertifikaları imzalarken kullanılan imza algoritması
Şifre (Passphrase)	Özel bir anahtara erişmek/açmak için kullanılan parola. Bu parola, ilk kez oturum açtığınızda rastgele bir dizeye başlatılır. (bkz. 6.1.1)



Lütfen yerel rastgele sayı üreticinin (RNG) çoğu uygulama için oldukça iyi bir rastgelelik sağladığı gerçeğinin farkında olun. Daha güçlü şifreleme zorunluysa, anahtarları harici bir RNG cihazında oluşturmanızı veya tüm sertifikaları tamamen uzak bir sertifika sunucusunda yönetmenizi öneririz. Bununla birlikte, yerel bir sertifika yetkilisi kullanmak tüm gerekli sertifikaları verebilir ve yönetebilir ve ayrıca bir sertifika iptal listesi (CRL) çalıştırabilir.

Anahtarları içe aktarırken, sertifika ve anahtar dosyası PEM/DER veya PKCS7 biçiminde ayrı ayrı kodlanmış olarak yüklenebilir. Tüm dosyalar (CA sertifikası, sertifika ve özel anahtar) ayrıca PKCS12 kapsayıcı biçimi kullanılarak tek seferde yüklenebilir. RSA/DSS anahtarları OpenSSH veya Dropbear biçimlerinden dönüştürülebilir. Özel anahtarı açmak için parolayı belirtmek mümkündür. Lütfen sistemin sertifikayı yüklerken genellikle sistem genelindeki sertifika parolasını bir anahtara uygulayacağını unutmayın. Bu nedenle, genel parolayı değiştirmek, tüm yerel anahtarların yenisiyle donatılmasıyla sonuçlanacaktır.

SCEP Yapılandırması (SCEP Configuration)

Sertifikalar Basit Sertifika Kayıt Protokolü (Simple Certificate Enrollment Protocol, SCEP) kullanılarak kaydediliyorsa aşağıdaki ayarlar yapılandırılabilir:

Parametre	SCEP Yapılandırma
SCEP durumu (SCEP status)	SCEP'in etkin olup olmadığını belirtir
URL	SCEP URL'si genellikle http://<host>/<path>/pkiclient.exe biçimindedir
CA parmak izi (CA fingerprint)	Uzak otoriteyi tanımlamak için kullanılan sertifikanın parmak izi. Boş bırakılırsa, herhangi bir CA'ya güvenilecektir.
Parmak izi algoritması (Fingerprint algorithm)	CA'yı (MD5 veya SHA1) tanımlamak için parmak izi algoritması
Yoklama aralığı (Poll interval)	Bir sertifika isteği için saniye cinsinden yoklama aralığı
İstek zaman aşımı (Request timeout)	Bir sertifika isteği için saniye cinsinden maksimum sorgulama süresi
ID tipi (ID type)	IP, E-posta veya DNS olabilir
Şifre (Password)	SCEP sunucusunun şifresi

Sertifikaları kaydederken, CA sertifikası başlangıçta `get ca` işlemi kullanılarak belirtilen SCEP URL'sinden alınacaktır. Yapılandırma sayfasında gösterilecektir ve doğru yetkiliye ait olduğu doğrulanmalıdır. Aksi takdirde, CA reddedilmelidir. Bu kısım, güven zincirini oluşturduğu için SCEP kullanırken önemlidir.

Bir sertifika kayıt isteği zaman aşımına uğrarsa, kesintiye uğrayan kayıt isteğini yeniden tetiklemek mümkündür ve daha önce oluşturulan anahtar kullanılarak devam ettirilecektir. Bir istek reddedilmişse, önce sertifikayı silmeniz ve ardından kayıt sürecini baştan başlatmanız gerekir.



Yetkililer (Authorities)

SSL istemci bağlantıları için (SDK işlevleri tarafından veya yapılandırma/yazılım görüntüleri indirilirken kullanılan) güvenilir kabul edilen CA sertifikalarının bir listesini yükleyebilirsiniz.

Mozilla Firefox ile belirli bir siteden CA sertifikasını almak için aşağıdaki adımlar gerekecektir:

- Tarayıcıyı ilgili HTTPS web sitesine yönlendirin
- Adres çubuğundaki asma kilide tıklayın
- Daha Fazla Bilgi ve Sertifikayı Görüntüle düğmesine tıklayın
- Ayrıntılar sekmesini seçin ve Dışa Aktar düğmesine basın
- Dosya için bir yol seçin (ör. website.pem)

Kendi kendine imzalanmış yetkililerden gelen sertifikalar ayrıca şu şekilde çalıştırılarak da alınabilir:

```
echo quit | \  
openssl s_client -showcerts -connect <host>:443 | \  
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > other.crt
```

PEM kodlu X.509 sertifika dosyaları basit bir düzenleyici kullanılarak düzenlenebilir ve birleştirilebilir (gerekirse) ve ardından kutuya yüklenebilir. Kurulduktan sonra, bu CA sertifikalarından herhangi biriyle doğrulama başarısız olursa bir SSL istemci bağlantısı sonlandırılır.

6.8.9. Lisanslama (Licensing)

NetModule AG yönlendiricilerinin belirli özellikleri sistemde geçerli bir lisansın bulunmasını gerektirir, bazıları da takılı modüllere bağlıdır. Mevcut bileşenler için geçerli bir lisans almak için lütfen bizimle iletişime geçin ve daha sonra yönlendiriciye yüklenebilecek seri numaranıza dayalı bir lisans dosyası sağlayacağız.

Feature	Availability	Licensing Status
FMS2IP	no	unlicensed
GPS	yes	licensed
GSM	yes	licensed
ITXPT	no	unlicensed
LTE	yes	licensed
SERVER	yes	licensed
TX_ADV	yes	licensed
UMTS	yes	licensed
VIRT	no	licensed
VOICE	yes	licensed
WLAN	yes	licensed

Ekran 6.76.: Lisanslama



6.8.10. Yasal Uyarı

**Dikkat**

Ücretsiz ve Açık Kaynaklı Yazılımlar hakkında 3. bölümü inceleyin

Telif Hakkı (C) 2025, NetModule AG. Tüm hakları saklıdır.



6.9. ÇIKIŞ (LOGOUT)

Lütfen Web Yöneticisi'nden çıkış yapmak için bu menüyü kullanın.



7. Komut Satırı Arayüzü (Command Line Interface)

Komut Satırı Arayüzü (CLI), yönlendiriciye genel bir kontrol arayüzü sunar ve yapılandırma parametrelerini almak/ayarlamak, güncellemeleri uygulamak, hizmetleri yeniden başlatmak veya diğer sistem görevlerini gerçekleştirmek için kullanılabilir. Yönetici kullanıcısı olarak oturum açıldığında veya `cli` -i çalıştırıldığında etkileşimli modda otomatik olarak başlatılır. Ancak, sistem kabuğundan çağrılırken aynı sözdizimi kullanılabilir. Kullanılabilir komutların listesi `cli` -l çalıştırılarak görüntülenebilir. CLI, TAB tamamlamayı destekler, yani herhangi bir anda TAB tuşuna basılarak girilen sözcükleri veya parçaları genişletir. Bu, komutlar için geçerlidir ancak bazı argümanlar için de geçerlidir ve genellikle kabukta çalışmak için kullanışlı bir yol sunar. Lütfen her CLI oturumunun belirli bir süre (varsayılan olarak 10 dakika) geçtikten sonra otomatik olarak oturum kapatacağını unutmayın. `no-auto-logout` komutuyla kapatılabilir.



7.1. Genel Kullanım

CLI'yi etkileşimli moda çalıştırırken, girilen her komut RETURN tuşuyla yürütülecektir. Girilen karakterler arasındaki geçerli noktayı taşımak için Sol ve Sağ tuşlarını veya girilen komutların geçmişini aramak için Yukarı ve Aşağı tuşlarını kullanabilirsiniz. Exit yazıp CTRL-c'ye iki kez veya boş bir komut satırında CTRL-d'ye basmak CLI'den çıkmanızı sağlar.

Tuş	Eylem
CTRL-a	Geçerli satırın başına git
CTRL-e	Satırın sonuna git
CTRL-f	Bir karakter ileri git
CTRL-b	Bir karakter geri git
ALT-f	Bir sonraki kelimenin sonuna doğru ilerle
ALT-b	Geçerli veya önceki kelimenin başına geri dön
CTRL-l	Ekranı temizle, geçerli satırı ekranın en üstünde bırak; verilen bir argümanla, ekranı temizlemeden geçerli satırı yenile
CTRL-p	Önceki komutu geçmiş listesinden getir, listede geriye doğru hareket et
CTRL-n	Geçmiş listesinden bir sonraki komutu getir, listede ilerle
ALT-<	Tarihçedeki ilk satıra git
ALT->	Giriş geçmişinin sonuna git
CTRL-r	Geçerli satırdan başlayarak geriye doğru arama yapın ve geçmişte yukarı doğru ilerleyin
CTRL-s	Oturumu dondur
CTRL-q	Dondurulmuş oturumu yeniden etkinleştir
CTRL-d	Noktadaki karakteri sil veya satırın başındaysa CLI'den çık
CTRL-t	Karakterini satırın sonuna doğru sürükleyin, ardından bu, noktadan önceki iki karakteri yer değiştirir
ALT-t	Noktadan önceki kelimeyi noktadan sonraki kelimenin ötesine sürükleyin, noktayı o kelimenin üzerine de taşıyın. Nokta satırın sonundaysa, bu satırdaki son iki kelimeyi yer değiştirir.
CTRL-k	Metni noktadan satır sonuna kadar sil
CTRL-y	Silinen metnin üst kısmını tamponun şu noktasına çekin

Boşluk içeren argümanlarla komut girerken tırnak işareti ("") kullanılmasının gerekebileceğini lütfen unutmayın.



7.2. Yardım

Help komutu, argüman olmadan çağrıldığında kullanılabilir komutların listesini almak için kullanılabilir, aksi takdirde belirtilen komutun kullanımını yazdırır.

```
> help
```

Usage:

```
help [<command>]
```

Available commands:

get	Get config parameters
set	Set config parameters
done	Check done
update	Update system facilities
cert	Manage keys and certificates
status	Get status information
scan	Scan networks
send	Send message , mail , techsupport or ussd
restart	Restart service
debug	Debug system
reset	Reset system to factory defaults
reboot	Reboot system
shell	Run shell command
help	Print help for command
no-autologout	Turn off auto -logout
history	Show command history
exit	Exit

7.3. Yapılandırma Parametrelerinin Alınması

Yapılandırma değerlerini almak için get komutu kullanılabilir.

```
> get -h
```

Usage:

```
get [- hsvfc] <parameter > [< parameter >..]
```

Options:

-s	generate sourceable output
-v	validate config parameter
-f	get factory default rather than current value
-c	show configuration sections

7.4. Yapılandırma Parametrelerinin Yazılması

set komutu yapılandırma değerlerini ayarlamak için kullanılabilir.

```
> set -h
```

Usage:

```
set [-hv] <parameter>=<value > [<parameter>=<value>..]
```

Options:

-v	validate config parameter
----	---------------------------



7.5. Yapılandırmanın Tamamlandığını Kontrol Etme

done komutu, bir yapılandırma değişikliğinden sonra tüm değişiklik komut dosyalarının tamamlanıp tamamlanmadığını kontrol etmek için kullanılabilir.

```
> done -h
```

Usage:

```
done [-h]
```

7.6. Durum Bilgilerinin Alınması

status komutu sistemin çeşitli durum bilgilerini almak için kullanılabilir.

```
> status -h
```

Usage:

```
status [-hs]<section >
```

Options:

```
-s generate sourceable output
```

Available sections:

summary	Short status summary
info	System and config information
config	Current configuration
system	System information
configuration	Configuration information
license	License information
wwan	WWAN module status
wlan	WLAN module status
gnss	GNSS (GPS) module status
eth	Ethernet interface status
lan	LAN interface status
wan	WAN interface status
openvpn	OpenVPN connection status
ipsec	IPsec connection status
pptp	PPTP connection status
gre	GRE connection status
dialin	Dial -In connection status
mobileip	MobileIP status
dio	Digital IO status
audio	Audio module status
can	CAN module status
uart	UART module status
ibis	IBIS module status
redundancy	Redundancy status
sms	SMS status
firewall	Firewall status
qos	QoS status
neigh	Neighborhood status
location	Current Location



7.7. Ağları Tarama

scan komutu, kullanılabilir WWAN ve WLAN ağlarını taramak için kullanılabilir.

```
> scan -h
```

Usage:

```
scan [-hs] <interface>
```

Options:

```
-s generate sourceable output
```

7.8. E-posta veya SMS Gönderme

send komutu, belirtilen adrese veya telefon numarasına E-Posta/SMS yoluyla mesaj göndermek için kullanılabilir.

```
> send -h
```

Usage:

```
send [-h] <type><dest><msg>
```

Options:

```
<type> type of message to be sent (mail,sms,techsupport,ussd)
```

```
<dest> destination of message (mail-address,phone-number or index)
```

7.9. Sistem Güncelleme

update komutu çeşitli sistem güncellemelerini gerçekleştirmek için kullanılabilir.

```
> update -h
```

Usage:

```
update [-hfrsn]<software|config|license|sshkeys><URL>
```

Options:

```
-r reboot after update
```

```
-f force update
```

```
-n don't reset missing config values with factory defaults
```

```
-s show update status
```

Available update targets:

```
software Perform software update
```

```
firmware Perform module firmware update
```

```
config Update configuration
```

```
license Update licenses
```

```
sshkeys Install SSH authorized keys
```

Ayrıca sunucumuzdaki en son sürümü yüklemek için 'update software latest' komutunu da çalıştırabilirsiniz.



7.10. Anahtarları ve Sertifikaları Yönet

`cert` komutu anahtarları ve sertifikaları yönetmek için kullanılabilir.

```
> cert -h
```

Usage:

```
cert [-h] [-p phrase] <operation> <cert> [<url>]
```

Possible operations:

<code>install</code>	install a certificate from specified URL
<code>create</code>	create a certificate locally
<code>enroll</code>	enroll a certificate via SCEP
<code>erase</code>	erase an installed certificate
<code>view</code>	view an installed certificate

7.11. Servisleri Yeniden Başlatmak

`restart` komutu sistem servislerini yeniden başlatmak için kullanılabilir.

```
> restart -h
```

Usage:

```
restart [-h] <service>
```

Available services:

<code>configd</code>	Configuration daemon
<code>dnsmasq</code>	DNS/DHCP server
<code>dropbear</code>	SSH server
<code>firewall</code>	Firewall and NAT
<code>gpsd</code>	GPS daemon
<code>gre</code>	GRE connections
<code>ipsec</code>	IPsec connections
<code>lighttpd</code>	HTTP server
<code>link-manager</code>	WAN links
<code>network</code>	Networking
<code>openvpn</code>	OpenVPN connections
<code>pptp</code>	PPTP connections
<code>qos</code>	QoS daemon
<code>smsd</code>	SMS daemon
<code>snmpd</code>	SNMP daemon
<code>surveyor</code>	Supervision daemon
<code>syslog</code>	Syslog daemon
<code>telnet</code>	Telnet server
<code>usbipd</code>	USB/IP daemon
<code>voiced</code>	Voice daemon
<code>vrrpd</code>	VRRP daemon
<code>wlan</code>	WLAN interfaces
<code>wwan-manager</code>	WWAN manager



7.12. Hata Ayıklama

Hata ayıklama/günlük mesajlarını almak için debug komutu kullanılabilir.

```
> debug -h
```

Usage:

```
debug [-h] <target>
```

Available debug targets:

```
configd  
event-manager  
home-agent  
led-manager  
link-manager  
mobile-node  
qmid  
qosd  
scripts  
sdkhost  
ser2net  
smsd  
surveyor  
swupdate  
system  
voiced  
watchdog  
wwan-manager  
wwanmd
```

7.13. Sistemi Sıfırlama

reset komutu yönlendiriciyi fabrika ayarlarına sıfırlamak için kullanılabilir.

```
> reset -h
```

Usage:

```
reset [-h]
```

7.14. Sistemi Yeniden Başlatma

Yönlendiriciyi yeniden başlatmak için reboot komutu kullanılabilir.

```
> reboot -h
```

Usage:

```
reboot [-h]
```

7.15. Kabuk Komutlarını Çalıştırma

shell komutu, bir sistem kabuğunu çalıştırmak ve herhangi bir uygulamayı veya betiği çalıştırmak için kullanılabilir.

```
> shell -h
```



Usage:

```
shell [-h] [<cmd>]
```

7.16. Komut Geçmişi

`history` komutu, girilen komutların listesini kullanıcı bazında yazdıracaktır.

```
> history -h
```

Usage:

```
history [-c]
```

Komut geçmişi `history -c` ile temizlenebilir.

7.17. CLI-PHP

CLI uygulamasının HTTP ön ucu olan CLI-PHP, yönlendiriciyi uzaktan yapılandırmak ve kontrol etmek için kullanılabilir. Fabrika yapılandırmasında etkinleştirilmiştir, bu nedenle dağıtım amaçları için kullanılabilir, ancak yönetici hesabı kurulduğu anda devre dışı bırakılır. Hizmet daha sonra `cliphp.status` yapılandırma parametresi ayarlanarak açılıp kapatılabilir:

```
cliphp.status=0      Service is disabled
cliphp.status=1      Service is disabled
```

Bu bölüm Sürüm 2 için CLI-PHP arayüzünü açıklar. POST ve GET isteklerini kabul eder.



Dikkat

Örnekler yalnızca bu arayüzün kullanımını gösterim amacıyla gösterir. Üretken ortamlar için GET ve HTTP yerine POST ve HTTPS kullanılması önerilir. Bu arayüzü test etmek için GET isteklerini kullanırsanız tarayıcı geçmişinizin parolalar ve diğer hassas bilgiler dahil GET isteklerini depolayacağını lütfen unutmayın.

GET istekleri ile çalıştırıldığında genel kullanım şu şekilde tanımlanır:

Usage :

```
http(s)://cli.php?<key1>=<value1>&<key2>=<value2>..<keyN>=<valueN>
```

Available keys:

```
output      Output format (html,plain)
usr         Username to be used for authentication
pwd        Password to be used for authentication
command     Command to be executed
arg0..arg31 Arguments passed to commands
```

Notes:

The commands correspond to CLI commands as seen by '`cli -l`', the arguments (`arg0..arg31`) will be directly passed to `cli`.

Thus, an URL containing the following sequence:

```
command=get&arg0=admin.password&arg1=admin.debug
```

will lead to `cli` being called as:

```
cli get "admin.password" "admin.debug"
```



It supports whitespaces but please be aware that any special characters in the URL must be specified according to RFC1738 (usually done by common clients such as wget, lynx, curl).

Response:

The returned response will always contain a status line in the format:

```
<return >: <msg>
```

with return values of OK if succeeded and ERROR if failed. Any output from the commands will be appended.

Examples:

```
OK: status command successful
```

```
ERROR: authentication failed
```

status - Durum bilgilerini görüntüle**Key usage:**

```
command=status [&arg0=<section>]
```

Notes:

Available sections can be retrieved by running

```
command=status&arg0=-h .
```

Please note that the status summary can be displayed without authentication.

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=-h
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
status&arg0=summary
```

```
http://192.168.1.1/cli.php?version=2&output=html&command=status
```

get - Yapılandırma parametresini al**Key usage:**

```
command=get&arg0=<config-key> [&arg1=<config-key>..]
```

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
get&arg0=config.version
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=
get&arg0=openvpn.status&arg1=snmp.status&arg2=ipsec.status
```



set - Yapılandırma parametresini ayarla

Key usage:

```
command=set&arg0=<config-key>&arg1=<config-value> [&arg2=<config-key>&arg3=<config-value>..]
```

Notes:

In contrast to the other commands , this command requires a set of tuples because of the reserved '=' char , i.e.

[arg0=key0 , arg1=val0], [arg2=key1, arg3=val1], [arg4=key2, arg5=val2], etc

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=set&arg0=snmp.status&arg1=1
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=set&arg0=snmp.status&arg1=0&arg2=openvpn.status&arg3=1
```

restart - Bir sistem hizmetini yeniden başlat

Key usage:

```
command=restart&arg0=<service >
```

Notes:

Available services can be retrieved by running 'command=restart&arg0=-h'

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=restart&arg0=-h
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=restart&arg0=link-manager
```

reboot - Sistemin yeniden başlatılmasını tetikler

Key usage:

```
command=reboot
```

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=reboot
```

reset - Fabrika ayarlarına sıfırlamayı çalıştır

Key usage :

```
command=reset
```

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=reset
```



update – Sistemi Güncelle

Key usage:

```
command=update&arg0=<facility>&arg1=<URL>
```

Notes:

Available facilities can be retrieved by running 'command=update &arg0=-h'

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=software&arg1=tftp://192.168.1.254/latest
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=config&arg1=tftp://192.168.1.254/user-config.zip
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=license&arg1=http://192.168.1.254/xxx.lic
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=update&arg0=firmware&arg1=wwan0&arg2=tftp://192.168.1.254/firmware
```

send – SMS Gönder

Key usage:

```
command=send&arg0=sms&arg1=<number>&arg2=<text>
```

Notes:

The phone number has to be specified in international format such as +123456789 including a leading plus sign (which can be encoded with %2B). The SMS daemon must be properly configured prior to using that function.

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=sms&arg1=%2B123456789&arg2=test
```

send – E-posta Gönder

Key usage :

```
command=send&arg0=mail&arg1=<address>&arg2=<text>
```

Notes:

The address has to be a valid E-Mail address such as abc@abc.com (the at-sign can be encoded with %40). The E-Mail client must be properly configured prior to using that function.

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=mail&arg1=abc%40abc.com&arg2=test
```

send – TechSupport Gönder

Key usage :

```
command=send&arg0=techsupport&arg1=stdout
```

```
command=send&arg0=techsupport&arg1=<address>&arg2=<subject>
```

Notes:

The address has to be a valid E-Mail address such as abc@abc.com (the at-sign can be encoded with %40). The E-Mail client must be properly configured prior to using that function.

In case of stdout, the downloaded techsupport file will be called 'download'.

**Examples:**

```
http://192.168.1.1/cli.php?version=2&output=mime&usr=admin&pwd=admin01&command=send&arg0=techsupport&arg1=stdout
```

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=techsupport&arg1=abc%40abc.com&arg2=subject
```

send - USSD Kodu Gönder**Key usage:**

```
command=send&arg0=ussd&arg1=<card>&arg2=<code >
```

Notes:

The argument card specifies the card module index (e.g. 0 for wwan0). The USSD code can consist of digits, plus signs, asterisks (can be encoded with `\%2A`) and dashes (can be encoded with `\%23`).

Examples :

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=ussd&arg1=0&arg2=%2A100%23
```

A. Ek

A.1. Kısaltmalar

Kısaltma	Açıklama
ANY	Genel olarak mevcut bölüm tarafından sunulan tüm seçenekleri içerir
APN	Erişim Noktası Adı (Access Point Name)
ASU	Keyfi Güç Birimi (Arbitrary Strength Unit)
CID	Hücre Kimliği, her Baz Alıcı-Verici İstasyonunu (BTS) tanımlamak için kullanılan genellikle benzersiz bir sayıdır.
CLI	Yönlendiriciyi sorgulamak veya sistem görevlerini gerçekleştirmek için kullanılan genel arayüz (Komut Satırı Arayüzü, Command Line Interface, CLI)
DHCP	Dinamik Ana Bilgisayar Yapılandırma Protokolü (Dynamic Host Configuration Protocol)
DNS	Alan Adı Sistemi (Domain Name Server)
ETHx	Ethernet arayüzlerini belirtir (tekli veya anahtarlanmış olabilir)
FQDN	Tam nitelikli alan adı (Fully Qualified Domain Name)
GHz	Gigahertz
GNSSx	Küresel Konumlandırma Uydu Sistemi modülünü belirtir (Global Navigation Satellite System)
GUI	Grafiksel Kullanıcı Arayüzü
HTTP	Köprü Metni Aktarma Protokolü (HyperText Transfer Protocol)
ICCID	Entegre Devre Kartı Tanımlayıcısı (Integrated Circuit Card Identifier)
IMEI	Uluslararası Mobil Cihaz Kimliği (International Mobile Station Equipment Identity)
IMSI	Uluslararası Mobil Abone Kimliği (International Mobile Subscriber Identity)
INx	Sayısal G/Ç giriş portunu belirtir (DIx)
LAC	Konum Alanı Kodu (Location Area Code)
LAC	Sinyallemeyi iyileştirmek için bir araya getirilen bir dizi baz istasyonunun tanımlayıcısı
LAI	Konum Alanı Kimliği (Location Area Identification)
LAI	Ülke, ağ sağlayıcısı ve konum alanını küresel olarak benzersiz şekilde tanımlar
LANx	Local Area Network (LAN) arayüzleri – genellikle Ethernet tabanlı (köprüler dahil)
MAC	Ortam Erişim Denetimi (Media Access Control)
Mbps	Megabit/saniye
MCC	Mobil Ülke Kodu (Mobile Country Code)
MCS	Modülasyon Kodlama Şeması (Modulation Coding Scheme)
MEID	Mobil Cihaz Tanımlayıcısı (Mobile Equipment Identifier)
MHz	Megahertz
MNC	Mobil Ağ Kodu (Mobile Network Code)
Mobilex	Bir WWAN modemini tanımlar



Kısaltma	Açıklama
MOBILEIPx	Mobil IP tünel arayüzüne atıfta bulunur
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OUTx	Dijital bir G/Ç çıkış portu (DOx) belirtir
PPTPx	Bir PPTP tünel arayüzü belirtir
PSK	Pre-Shared Key
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indication
SDK	Uygulamaları programlamak için Betik Geliştirme Kiti (Script Development Kit)
SERIALx	Bir seri portu tanımlar
SIMx	Ön panelde görüldüğü gibi SIM yuvasını belirtir
SIM	Subscriber Identity Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Bir modülde birden fazla WLAN ağını tanımlamak için kullanılabilir
STP	Spanning Tree Protocol
TAPx	Bir OpenVPN tünel arayüzünü belirtir (TAP'a dayalı)
TUNx	Bir OpenVPN tünel arayüzünü belirtir (TUN'a dayalı)
USSD	Unstructured Supplementary Service Data
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Sistemde aktif olan tüm Geniş Alan Ağı (Wide Area Network, WAN) arayüzlerini içerir
WDS	Wireless Distribution System
WLANx	Erişim noktası olarak yapılandırıldığında ek LAN arayüzü olarak temsil edilecek bir Kablosuz LAN arayüzünü ifade eder
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WWANx	Kablosuz Geniş Alan Ağı (2G/3G/4G) bağlantısını ifade eder

Tablo A.1.: Kısaltmalar



Genel olarak, dahili arayüzler küçük harfle yazılır ve farklı bir adlandırmaya sahip olabilir. İndeksleri sıfırdan başlarken, kullanıcı tarafından görülen arayüzler birden başlayarak büyük harflerle yazılır.

A.2. Sistem Olayları (System Events)

ID	Olay	Açıklama
101	wan-up	WAN bağlantısı kuruldu
102	wan-down	WAN bağlantısı kesildi
201	dio-in1-on	DIO IN1 açık
202	dio-in1-off	DIO IN1 kapalı
203	dio-in2-on	DIO IN2 açık
204	dio-in2-off	DIO IN2 kapalı
205	dio-out1-on	DIO OUT1 açık
206	dio-out1-off	DIO OUT1 kapalı
207	dio-out2-on	DIO OUT2 açık
208	dio-out2-off	DIO OUT2 kapalı
209	poe-on	POE açık
210	poe-off	POE kapalı
301	gps-up	GPS sinyali mevcut
302	gps-down	GPS sinyali mevcut değil
401	openvpn-up	OpenVPN bağlantısı kuruldu
402	openvpn-down	OpenVPN bağlantısı kesildi
403	ipsec-up	IPsec bağlantısı kuruldu
404	ipsec-down	IPsec bağlantısı kesildi
406	pptp-up	PPTP bağlantısı kuruldu
407	pptp-down	PPTP bağlantısı kesildi
408	dialin-up	Dial-In bağlantısı kuruldu
409	dialin-down	Dial-In bağlantısı kesildi
410	mobileip-up	MobileIP bağlantısı kuruldu
411	mobileip-down	MobileIP bağlantısı kesildi
412	gre-up	GRE bağlantısı kuruldu
413	gre-down	GRE bağlantısı kesildi
414	l2tp-up	L2TP bağlantısı kuruldu
415	l2tp-down	L2TP bağlantısı kesildi
501	system-login-failed	Giriş başarısız oldu
502	system-login-succeeded	Giriş başarılı oldu
503	system-logout	Kullanıcı oturumu kapattı
504	system-rebooting	Sistem yeniden başlatıldı
505	system-startup	Sistem başlatıldı



ID	Olay	Açıklama
506	test	Test etkinliği
507	sdk-startup	SDK başlatıldı
508	system-time-updated	Sistem saati güncellendi
509	system-poweroff	Sistem kapatma tetiklendi
510	system-error	Sistem hata durumunda
511	system-no-error	Sistem hata durumundan çıktı
512	cliphp	cliphp ile sdk betiğini başlatın
601	sms-sent	Kısa mesaj gönderildi
602	sms-notsent	Kısa mesaj gönderilmedi
603	sms-received	Kısa mesaj alındı
604	sms-report-received	Kısa mesaj ileti raporu alındı
701	call-incoming	Gelen çağrı
702	call-outgoing	Giden çağrı
801	ddns-update-succeeded	Dinamik DNS güncellemesi başarılı
802	ddns-update-failed	Dinamik DNS güncellemesi başarısız
901	usb-storage-added	USB depolama aygıtı eklendi
902	usb-storage-removed	USB depolama aygıtı kaldırıldı
903	usb-eth-added	USB Ethernet aygıtı eklendi
904	usb-eth-removed	USB Ethernet aygıtı kaldırıldı
905	usb-serial-added	USB seri aygıtı eklendi
906	usb-serial-removed	USB seri aygıtı kaldırıldı
1001	redundancy-master	Yönlendirici artık ana yönlendiricidir
1002	redundancy-backup	Yönlendirici artık yedek yönlendiricidir

Tablo A.2.: Sistem Olayları



A.3. Fabrika Yapılandırması

Herhangi bir yapılandırma parametresi için varsayılan değerler içeren fabrika yapılandırması yönlendiricideki `/etc/config/factory-config.cfg` dosyasından türetilebilir. Ayrıca belirli bir varsayılan değer elde etmek için `cli get -f <parametre>` komutunu çağırabilirsiniz.



A.4. SNMP VENDOR MIB

NetModule SNMP VENDOR MIB'i buradan edinebilirsiniz:

<https://share.netmodule.com/public/system-software//4.8.0.104/NETMODULE-VENDOR-MIB-4.8.0.104.mib>

A.5. SDK Örnekleri

Dosya	Betik Açıklaması
best-operator.are	Başlangıçta operatörleri tarayacak ve en iyi sinyale sahip olanı seçecektir
candump.are	CAN mesajlarının alınmasını sağlar.
config-summary.are	Şu anda çalışan yapılandırmanın bir özetini gösterir.
dio.are	Dijital çıkış portu ayarlamak için kullanılabilir.
dio-monitor.are	DIO portlarını izler ve belirtilen telefon numarasına bir SMS gönderir.
dio-server.are	DIO portlarını kontrol etmek için kullanılabilen bir TCP sunucusu uygular.
dynamic-operator.are	Mobile2'yi tarar ve Mobil 1'de uygun SIM'i arar
email-to-sms.are	E-postaları alıp SMS olarak ileten basit bir SMTP sunucusu uygular.
etherwake.are	Uyuyan bir bilgisayarı uyandırmak için kullanılabilir (WakeOnLan)
gps-broadcast.are	GPS NMEA akışını UDP sunucusuna gönderir (cihaz kimliği dahil).
gps-monitor.are	GPS konumu (enlem, boylam) belirtilen aralıkta iken WLAN'ı etkinleştirir.
gps-udp-client.are	GPS NMEA akışını uzak bir UDP sunucusuna gönderir.
gps-udp-client-compat.are	GPS NMEA akışını (seri/sağlama toplamı dahil) UDP sunucusuna gönderir.
led.are	LED ayarlamak için kullanılabilir
modbus-rtu-master.are	Seri porttan gelen mesajları okumak için kullanılabilir
modbus-rtu-slave.are	Modbus slave sunucusu uygular
modbus-tcp-rtu-gateway.are	Modbus TCP RTU ağ geçidi uygular
mount-media.are	USB depolama çubuğunu monte etmek için kullanılabilir
opcua-browse.are	Uzak bir OPC-UA sunucusundaki düğümleri tarayacaktır
opcua-json.are	OPC-UA sunucusunun herhangi bir sıcaklık düğümünü yoklar ve bunları JSON kodlu olarak uzak bir sunucuya gönderir
opcua-read.are	OPC-UA sunucusundaki düğüm değerini okur
opcua-write.are	OPC-UA sunucusundaki bir düğüme yeni bir değer yazar
ping-supervision.are	Belirtilen bir ana bilgisayarı denetler
read-config.are	Bir yapılandırma parametresini okumak için kullanılabilir
remote-mail.are	Uzak bir IMAP/POP3/SMTP sunucusundan e-postaları okur ve gönderir
scan-mobile.are	Mobil LAI'yi mevcut ağlara göre değiştirmek için kullanılabilir
scan-wlan.are	WLAN istemci ağını kullanılabilirliğe göre değiştirmek için kullanılabilir
send-mail.are	Belirtilen adrese bir E-Posta gönderir
send-sms.are	Belirtilen telefon numarasına bir SMS gönder

Dosya	Betik Açıklaması
send-techsupport.are	Teknik destek dosyası oluşturur ve belirtilen e-posta adresine gönderir
serial-read.are	Seri porttan mesajları okumak için kullanılabilir
serial-readwrite.are	Seri porta yazar ve seri porttan okur
serial-tcp-broadcast.are	Seri porta gelen mesajları okur ve TCP'den bilgisayarlara iletir (ve tersi)
serial-tcsetattr.are	Seri portun niteliklerini ayarlamak/almak için kullanılabilir
serial-udp-server.are	Seri porta gelen mesajları okur ve UDP'den bilgisayarlara iletir (ve tersi)
serial-write.are	Seri porta bir mesaj yazmak için kullanılabilir
set-ipsec-route.are	WWAN/WLAN ağına bağlı olarak IPsec sunucusuna giden yolu ayarlar
sms-confirm.are	Bir mesaj gönderir ve teslimatını onaylar
sms-control.are	SMS ile alınan komutları yürütür
sms-delete-inbox.are	SMS gelen kutusunu temizlemek için kullanılabilir
sms-read-inbox.are	SMS gelen kutusunu okumak için kullanılabilir
sms-to-email.are	Gelen SMS mesajlarını belirli bir E-posta adresine iletir
sms-to-serial.are	Alınan bir SMS'i seri porta yazmak için kullanılabilir
snmp-agent.are	SNMP aracısının MIB girişlerini genişletir
snmp-cmd.are	SNMP set/get komutlarını verir
snmp-trap.are	SNMP tuzakları göndermek için kullanılabilir
status.are	Tüm durum değişkenlerini görüntülemek için kullanılabilir
syslog.are	Basit bir syslog mesajı atın
tcpclient.are	Bir TCP sunucusuna bir mesaj gönderir
tcpserver.are	Mesajları alabilen bir TCP sunucusunu uygular
techsupport.are	Teknik destek dosyasını uzak bir FTP sunucusuna aktarır
transfer.are	En son GNSS konumlarını uzak bir FTP dosyasında depolar
transfer-file.are	Bu betik uzak bir dosyayı arşivler
udpclient.are	Uzak bir UDP sunucusuna bir mesaj gönderir
udp-msg-server.are	Mesajları alabilen ve SMS/E-posta olarak iletebilen bir UDP sunucusu
udpserver.are	Mesajları alabilen bir UDP sunucusu uygular
update-config.are	Bir yapılandırma güncellemesi gerçekleştirmek için kullanılabilir
voice-dispatcher-audio.are	Bir ses dağıtıcısı uygular
webpage.are	Web Yöneticisi'nde görüntülenebilen bir sayfa oluşturur
write-config.are	Bir yapılandırma parametresini ayarlamak için kullanılabilir

Tablo A.3.: SDK Örnekleri