

9160 G2

Kablosuz Ağ Geçidi

Kullanım Kılavuzu

2 Kasım 2009

P/N 8000350.A



*ISO 9001 Sertifikalı
Kalite Yönetim Sistemi*



© Telif Hakkı 2009 Psion Teklogix Inc.

2100 Meadowvale Boulevard, Mississauga, Ontario, Kanada L5N 7J9

<http://www.psionteklogix.com>

Bu belge ve içerdiği tüm bilgiler, Psion Teklogix Inc.'nin mülkiyetinde olup son derece gizli bir şekilde hazırlanmıştır ve Psion Teklogix'in kendi ürünlerinin ve hizmetlerinin satışlarını artırma amacı dışında tamamen ya da kısmen yeniden üretilmesi veya kopyalanması kesinlikle yasaktır. Ayrıca bu belge; tasarım, üretim, taşeronluk veya Psion Teklogix Inc.'nin çıkarlarına zarar verecek herhangi bir amaca temel olarak kullanılamaz.

Feragat

Bu dokümanın eksiksiz, doğru ve güncel olması için her türlü çaba sarf edilmiştir. Ayrıca burada yer alan bilgilerde belirli aralıklarla değişiklikler yapılır; bu değişiklikler, yayının yeni baskılarına eklenir.

Psion Teklogix Inc. bu belgede tanımlanan ürünlerde ve/veya programlarda önceden haber vermeksizin geliştirme ve/veya değişiklik yapma hakkını saklı tutar ve baskı hatası gibi belgede yer alan yanlış bilgilerden kaynaklanan dolaylı hasarlar dahil ancak bunlarla sınırlı olmamak kaydıyla hiçbir hasardan sorumlu değildir.

Windows® ve Windows logosu, Microsoft Corporation'ın ABD ve/veya diğer ülkelerdeki ticari markaları ya da tescilli ticari markalarıdır.

Tüm ticari markalar ve ticari adlar ilgili sahiplerinin mülkiyetindedir.

Fabrikaya İade Garantisi

Psion Teklogix Inc., on iki (12) aylık bir zaman zarfında bu ürün için şu adreste verilen Sınırlı Garanti ve Sorumluluğun Sınırlandırılması Bildirimine uygun şekilde iade garantisi sağlamaktadır:

www.psionteklogix.com/warranty

Psion Teklogix tarafından üretilmiş ürünlerin garantisi, herhangi bir Psion Teklogix servis kuruluşunun yetkilisi olmayan kişilerce kurcalanmış, değiştirilmiş ya da onarılmış hiçbir ürünü kapsamamaktadır. Tüm ayrıntılar için Psion Teklogix'in satışla ilgili hüküm ve koşullarına göz atın.



Önemli: *Psion Teklogix garantileri ürünün gönderim tarihinden itibaren geçerlidir.*

Hizmet ve Bilgi

Psion Teklogix, tüm dünyadaki müşterilerine kusursuz ve çok çeşitli ürün destek hizmetleri ve ürünlerle ilgili bilgiler sunar. Hizmetler, teknik desteği ve ürün tamirlerini kapsar. Yerel destek hizmeti sunan birimlerimizi bulmak için bkz. www.psionteklogix.com/service-and-support.htm

Mevcut ve üretimi durdurulan ürünlerimiz hakkında daha fazla bilgi için <http://teknet.psionteklogix.com> adresine gidin ve Teknet'e daha önce kayıt yaptırdıysanız oturum açın, yaptırmadıysanız "Not Registered?" (Kayıtlı değil misiniz?) seçeneğine tıklayın. Web sitemizde ürünlerle ilgili bilgiler içeren bir arşiv bölümü mevcuttur.



Elektrikli ve Elektronik Ekipman Atıkları (WEEE) Direktifi 2002/96/EC

Bu ürün ve aksesuarları Elektrikli ve Elektronik Ekipman Atıkları (WEEE) Direktifi 2002/96/EC'nin gerekliliklerini karşılamaktadır. Kullanım süresi sona eren Psion Teklogix ürününüz ya da aksesuarınız burada gösterilen etiketi taşıyorsa geri dönüşüm işleminin nasıl gerçekleştirileceği ile ilgili detayları öğrenmek için lütfen yerel ülke temsilcinizle iletişime geçin.

Uluslararası bayiliklerin listesi için lütfen şu adrese gidin:

www.psionteklogix.com/EnvironmentalCompliance

Belirli Zararlı Maddelerin Kullanımını Kısıtlama (RoHS) Direktifi 2002/95/EC

RoHS Nedir?

Avrupa Birlięi, zararlı maddelerin doğaya salınmasını engellemek için Avrupa'da satılan elektronik ve elektrikli ürünlerin hem tasarım hem de üretim aşamasında yüksek çevresel standartlara sahip olmasını zorunlu kılmıştır. “Belirli Zararlı Maddelerin Kullanımını Kısıtlama Direktifi (RoHS)” bir üründe bulunabilecek kurşun, kadmiyum, cıva ve altı değerlikli kromun yanı sıra alevlenme geciktiriciler PBB ve PBDE'nin maksimum izleme seviyelerini belirtir. AB üyesi ülkelerde 1 Temmuz 2006 tarihinden itibaren sadece bu yüksek çevresel standartları karşılayan ürünler "pazarda yerini alabilecek".



RoHS Logosu

RoHS ile uyumlu ürünleri işaretleme konusunda yasal bir gereklilik olmamasına rağmen Psion Teklogix Inc., direktifle uyumluluęunu řu řekilde belirtmektedir:

Ürünün arka tarafında ya da pil bölümündeki pilin altında (veya řarj cihazı ya da yerleřtirme istasyonu gibi ilgili aksesuarlarda) bulunan RoHS logosu, ürünün AB direktifi uyarınca RoHS ile uyumlu olduęunu belirtir. Ařaęıda belirtilenin dıřında, RoHS logosu bulunmayan bir Psion Teklogix ürünü, 1 Temmuz 2006 tarihinden önce AB pazarında yer almıřtır; bu yüzden direktiften muaf tutulur.



Not:

Fiziksel alan sınırlamaları veya muafiyet durumları nedeniyle aksesuarların ya da yardımcı donanımların hepsinde RoHS logosu bulunmayabilir.

İÇİNDEKİLER

Onaylar ve Güvenlik Özeti	xiii
-------------------------------------	------

Bölüm 1: Giriş

1.1 Bu Kılavuz Hakkında	3
1.2 Çevrimiçi Yardım Özellikleri, Desteklenen Tarayıcılar ve Sınırlamalar	6
1.3 Metin Kuralları	7
1.4 9160 G2 Kablosuz Ağ Geçidi'ne Genel Bakış	7
1.4.1 Telsizler	7
1.4.2 Erişim Noktası İşlevleri	9
1.4.3 Baz İstasyonu İşlevleri	9
1.4.4 Mini Denetleyici İşlevleri	9
1.5 Özellikler ve Avantajlar	10
1.5.1 IEEE Standartları Desteği ve Wi-Fi Uyumluluğu	10
1.5.2 Kablosuz Özellikleri	10
1.5.2.1 The Psion Teklogix 802.IQ Protokolü	11
1.5.3 Güvenlik Özellikleri	11
1.5.4 Kullanıma Hazır Konuk Arabirimi	12
1.5.5 Kümeleme ve Otomatik Yönetme	12
1.5.6 Ağ	13
1.5.7 SNMP Desteği	13
1.5.8 Bakım	14
1.6 Sırada Ne Var?	14

Bölüm 2: Kurulum Gereksinimleri

2.1 Doğru Konumu Seçme	17
2.1.1 Çevre	17
2.1.2 Bakım	18
2.1.3 Telsizler	18
2.1.4 Güç ve Anten Kabloları	18

2.1.4.1	Güç	18
2.1.4.2	Antenler	19
2.2	Harici Cihazlara Bağlanma	20
2.2.1	Bağlantı noktaları	20
2.2.2	LAN Kurulumu: Genel Bakış	21
2.2.3	LAN Kurulumu: Ethernet	21
2.2.3.1	Ethernet Kablosu	22
2.2.3.2	100Base-FX Fiber Optik Ethernet Bağlantı Noktası	22
2.2.4	Durum Göstergeleri (LED'ler)	22
2.2.5	Video Ekranı Terminaline Bağlanma	23
2.3	Yapılandırmayı Web Tarayıcıyla Değiştirme	23

Bölüm 3: Başlatma Öncesi Kontrol Listesi

3.1	9160 G2 Kablosuz Ağ Geçidi	27
3.1.1	9160 G2 Kablosuz Ağ Geçidi'nin Varsayılan Ayarları	27
3.1.2	Erişim Noktasının Sağlamadığı Şeyler	30
3.2	Yönetici Bilgisayarı	30
3.3	Kablosuz İstemci Bilgisayarları	32
3.4	9160 G2 Kablosuz Ağ Geçidi Üzerinde Dinamik ve Statik IP Adreslemeyi Anlama	32
3.4.1	Erişim Noktası, Başlangıçta Nasıl IP Adresi Alır?	33
3.4.2	Dinamik IP Adresleme	33
3.4.3	Statik IP Adresleme	33
3.4.4	IP Adresi Kurtarma	34

Bölüm 4: Kurulum ve Başlatma İçin Hızlı Adımlar

4.1	9160 G2 Kablosuz Ağ Geçidinin Kutusundan Çıkarılması	37
4.1.1	9160 G2 Kablosuz Ağ Geçidi Donanım ve Bağlantı Noktaları	37
4.1.2	9160 G2 Kablosuz Ağ Geçidi'nin İçindekiler	37
4.2	Erişim Noktasını Ağa ve Güce Bağlama	38
4.2.1	Konuk Ağı İçin Bağlantı Kurma Hakkında	40
4.2.1.1	Konuk VLAN İçin Donanım Bağlantıları	40
4.3	Erişim Noktasındaki Güç	40
4.4	Yönetim Web Sayfalarında Oturum Açma	40
4.4.1	Erişim Noktalarının Temel Ayarlarını Görüntüleme	41

4.5	"Temel Ayarları" Yapılandırma ve Kablosuz Ağı Başlatma	42
4.5.1	Varsayılan Yapılandırma	42
4.6	Sırada Ne Var?	42
4.6.1	Erişim Noktasının LAN'a Bağlı Olduğundan Emin Olma	42
4.6.2	Kablosuz İstemcilerle LAN Bağlantısını Test Etme	43
4.6.3	Gelişmiş Ayarları Kullanarak Erişim Noktasını Güvenli Hale Getirme ve İnce Ayar Yapma	43

Bölüm 5: Temel Ayarları Yapılandırma

5.1	Temel Ayarlara Gitme	47
5.2	Erişim Noktasını İnceleme / Açıklama	48
5.3	Ağ Ayarlarını Sağlama	49
5.4	Temel Ayarları Güncelleme	50
5.5	Bağımsız Bir Erişim Noktasının Temel Ayarları	50
5.6	Bir Bakışta Ağınızı Tanıma: Gösterge Simgelerini Anlama	50
5.7	Farklı Renk ve Stillerle Kullanıcı Arabirimini Görüntüleme	50

Bölüm 6: Erişim Noktalarını ve Kümeleri Yönetme

6.1	Genel Bakış	55
6.2	Erişim Noktası Yönetimine Gitme	55
6.3	Kümelemeyi Anlama	56
6.3.1	Küme Nedir?	56
6.3.2	Bir Küme Kaç AP Destekleyebilir?	56
6.3.3	Hangi Tür AP'ler Birlikte Kümelenebilir?	56
6.3.4	Koordinatör AP'nin Diğer Küme Üyeleriyle İlişkisi Nedir?	57
6.3.5	Hangi Ayarlar Küme Yapılandırmasının Bir Parçası Olarak Paylaşılır, Hangileri Paylaşılmaz?	57
6.3.5.1	Küme Yapılandırmasında Paylaşılan Ayarlar	57
6.3.5.2	Kümeyle Paylaşılmayan Ayarlar	58
6.3.6	Küme Oluşturma	58
6.3.7	Küme Büyüklüğü ve Üyelik	58
6.3.8	Küme İçi Güvenliği	58
6.4	Erişim Noktası Ayarlarını Anlama	59
6.4.1	Konum Açıklamasını Değiştirme	60
6.4.2	Küme Adını Ayarlama	60

6.5	Kümeleme Başlatma	60
6.6	Kümelemeyi Durdurma	61
6.7	Belirli Bir AP'nin Yapılandırma Bilgileri ve Bağımsız AP'leri Yönetme	61
6.7.1	Bir URL'deki IP Adresini Kullanarak AP'ye Gitme	62
6.8	Oturum İzleme	62
6.8.1	Oturum İzleme Bölümüne Gitme	62
6.8.2	Oturum İzleme Bilgilerini Anlama	62
6.8.3	Erişim Noktası Oturum Bilgilerini Görüntüleme	64
6.8.4	Oturum Bilgilerini Sıralama	64
6.8.5	Oturum Bilgilerini Yenileme	64

Bölüm 7: Kullanıcı Hesaplarını Yönetme

7.1	Genel Bakış	67
7.2	Kullanıcı Yönetimine Gitme	67
7.2.1	Kullanıcı Hesaplarını Görüntüleme	68
7.2.2	Kullanıcı Ekleme	68
7.2.3	Kullanıcı Hesaplarını Düzenleme	69
7.2.4	Kullanıcı Hesaplarını Etkinleştirme ve Devre Dışı Bırakma	70
7.2.5	Bir Kullanıcı Hesabını Etkinleştirme	70
7.2.6	Bir Kullanıcı Hesabını Devre Dışı Bırakma	71
7.2.7	Bir Kullanıcı Hesabını Kaldırma	71
7.3	Kullanıcı Veritabanını Yedekleme ve Geri Yükleme	71
7.3.1	Kullanıcı Veritabanını Yedekleme	71
7.3.2	Veritabanını Yedekleme Dosyasından Geri Yükleme	71

Bölüm 8: Kanal Yönetimi

8.1	Kanal Yönetimine Gitme	75
8.2	Kanal Yönetimini Anlama	75
8.2.1	Çalışma Şekli Hakkında Kısa Bilgi	75
8.2.2	Merak Edenler İçin: Çakışan Kanallar Hakkında Daha Fazla Bilgi	76
8.2.3	Örnek: Bir Ağın Kanal Yönetiminden Önceki ve Sonraki Durumu	76
8.3	Kanal Yönetimi Ayarlarını Yapılandırma ve Görüntüleme	77
8.3.1	Otomatik Kanal Atamayı Başlatma/Durdurma	78
8.3.2	Geçerli Kanal Atamalarını Görüntüleme ve Kilit Koyma	78

8.3.2.1	Geçerli Kanal Ayarlarını Güncelleme (Manuel)	79
8.3.3	Son Önerilen Değişiklik Grubunu Görüntüleme	79
8.3.4	Gelişmiş Ayarları Yapılandırma (Kanal Planlarını Özelleştirme/ Programlama)	80
8.3.4.1	Gelişmiş Ayarları Güncelleme	81

Bölüm 9: Komşu Kablosuz Ağlar

9.1	Komşu Kablosuz Ağlar Ekranına Gitme	85
9.2	Komşu Kablosuz Ağlarla İlgili Bilgileri Anlama	85
9.3	Komşu Kablosuz Ağları Görüntüleme	86
9.4	Bir Küme Üyesinin Ayrıntılarını Görüntüleme	88

Bölüm 10: Güvenliği Yapılandırma

10.1	Kablosuz Ağlardaki Güvenlik Sorunlarını Anlama	93
10.1.1	Hangi Güvenlik Modunu Kullanmalıyım?	93
10.1.2	Güvenlik Modlarının Anahtar Yönetimi, Kimlik Doğrulama ve Şifreleme Algoritmaları Açısından Karşılaştırılması	94
10.1.2.1	Şifresiz Mod (Güvenli Değil) Ne Zaman Kullanılmalı?	94
10.1.2.2	Statik WEP Ne Zaman Kullanılmalı?	95
10.1.2.3	IEEE 802.1x Ne Zaman Kullanılmalı?	96
10.1.2.4	Kişisel WPA Ne Zaman Kullanılmalı?	97
10.1.2.5	Kurumsal WPA Ne Zaman Kullanılmalı?	98
10.1.3	SSID Yayınını Engellemek Güvenliği Artırır mı?	99
10.1.4	İstasyon Ayırma Ağı Nasıl Korur?	100
10.2	Güvenlik Ayarlarını Yapılandırma	100
10.2.1	SSID Yayını, İstasyon Ayırma ve Güvenlik Modu	101
10.2.2	Güvenlik Modları	102
10.2.2.1	Yok (Düz metin)	102
10.2.2.2	Statik WEP	103
10.2.2.3	IEEE 802.1x	108
10.2.2.4	WPA Kişisel	111
10.2.2.5	WPA Kurumsal	113
10.3	Ayarları Güncelleme	118

Bölüm 11: Bakım ve İzleme

11.1	Arabirimler	121
11.1.1	Ethernet (Kablolu) Ayarları	122
11.1.2	Kablosuz Ayarları	122
11.2	Olay Günlükleri	122
11.2.1	SürekliliğiEtkinleştirme ya da Devre Dışı Bırakma	123
11.2.2	Önem Derecesi	124
11.2.3	Derinlik	124
11.2.4	Çekirdek Mesajlar İçin Günlük Aktarma Sunucusu	125
11.2.4.1	Uzaktan Günlük Oluşturmayı Anlama	125
11.2.4.2	Günlük Aktarma Sunucusunu Kurma	125
11.2.4.3	Durum, Olaylar Sayfasında Günlük Aktarma Sunucusunu Etkinleştirme/Devre Dışı Bırakma	126
11.2.5	Olaylar Günlüğü	127
11.3	Alma/Verme İstatistikleri	127
11.4	İlişkili Kablosuz İstemciler	129
11.4.1	Bağlantı Bütünlüğünü İzleme	130
11.5	Komşu Erişim Noktaları	130

Bölüm 12: Ethernet (Kablolu) Arabirimi

12.1	Ethernet (Kablolu) Ayarlarına Gitme	137
12.1.1	DNS Ana Bilgisayar Adı	138
12.1.2	Konuk Erişimi	138
12.1.2.1	Dahili Bir LAN ve Konuk Ağı Yapılandırma	138
12.1.2.2	Konuk Erişimini Etkinleştirme ya da Devre Dışı Bırakma	139
12.1.2.3	Sanal Konuk Ağı Belirleme	139
12.1.3	Sanal Kablosuz Ağlar	140
12.1.4	Dahili Arabirim Ayarları	141
12.1.5	Guest Interface Settings (Konuk Arabirimi Ayarları)	143
12.1.6	Ayarları Güncelleme	143

Bölüm 13: Kablosuz Arabirimini Ayarlama

13.1	Kablosuz Ayarlarına Gitme	147
13.2	802.11d Düzenleyici Etki Alanı Desteğini Yapılandırma	148
13.3	802.11h Düzenleyici Etki Alanı Kontrolü	148

13.4	Telsiz Arabirimini Yapılandırma	149
13.5	"Dahili" Kablosuz LAN Ayarlarını Yapılandırma	150
13.6	"Konuk" Ağı Kablosuz Ayarlarını Yapılandırma	151
13.7	Kablosuz Ayarlarını Güncelleme	152

Bölüm 14: Konuk Erişimini Ayarlama

14.1	Konuk Arabirimini Anlama	155
14.2	Konuk Arabirimini Yapılandırma	155
14.2.1	Sanal Bir LAN'da Konuk Ağı Yapılandırma	156
14.2.2	Karşılama Ekranını (Giriş Portalı) Yapılandırma	157
14.3	Konuk Ağını İstemci Olarak Kullanma	157
14.4	Dağıtım Örneği	158

Bölüm 15: VLAN'ları Yapılandırma

15.1	Sanal Kablosuz Ağ Ayarlarına Gitme	161
15.2	VLAN'ları Yapılandırma	161
15.3	Ayarları Güncelleme	163

Bölüm 16: 802.11 Telsiz Ayarlarını Yapılandırma

16.1	Telsiz Ayarlarını Anlama	167
16.2	Telsiz Ayarlarına Gitme	167
16.3	Telsiz Ayarlarını Yapılandırma	169
16.4	Ayarları Güncelleme	173

Bölüm 17: MAC Adresi Filtreleme

17.1	MAC Filtreleme Ayarlarına Gitme	177
17.2	MAC Filtreleme Ayarlarını Kullanma	178
17.3	Ayarları Güncelleme	178

Bölüm 18: Yük Dengeleme

18.1	Yük Dengelemeyi Anlama	181
18.1.1	Yük Dengesizliğini Tanımlama: Kapasitesinden Fazla ya da Az Çalışan Erişim Noktaları	181
18.1.2	Kullanım Sınırlamaları ve İstemci İlişkilerini Belirleme	181
18.1.3	Yük Dengeleme ve Hizmet Kalitesi (QoS)	182
18.2	Yük Dengeleme Ayarlarına Gitme	182

18.3	Yük Dengelemeyi Yapılandırma	183
18.4	Ayarları Güncelleme	184

Bölüm 19: Hizmet Kalitesi (QoS)

19.1	QoS'i Anlama	187
19.1.1	QoS ve Yük Dengeleme	187
19.1.2	802.11e ve WMM Standartları Desteği	187
19.1.3	QoS Kuyrukları ve Trafik Akışını Koordine Etme Parametreleri	188
19.1.3.1	QoS Kuyrukları ve Paketlerdeki Hizmet Türleri (ToS)	188
19.1.3.2	Veri Çerçevelerinin EDCF Kontrolü ve Çerçeveler Arası Karar Verme Aralığı	190
19.1.3.3	Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi	191
19.1.3.4	Daha İyi Performans İçin Paket Artırma	191
19.1.3.5	İstemci İstasyonları İçin Aktarım Olanığı (TXOP) Aralığı	192
19.1.4	802.1p ve DSCP Etiketleri	192
19.1.4.1	VLAN Önceliği	193
19.1.4.2	DSCP Önceliği	194
19.2	QoS Kuyruklarını Yapılandırma	194
19.2.1	AP EDCA Parametrelerini Yapılandırma	196
19.2.2	Wi-Fi Multimedyaı Etkinleştirme/Devre Dışı Bırakma	198
19.2.3	İstasyon EDCA Parametrelerini Yapılandırma	198
19.3	Ayarları Güncelleme	200

Bölüm 20: Kablosuz Dağıtım Sistemi

20.1	Kablosuz Dağıtım Sistemini Anlama	203
20.1.1	WDS'yi Uzak Kablolı LAN'ları Birleştirmek İçin Kullanma	203
20.1.2	WDS İle Ağ Kapsamını Kablolı Kapsama Alanının Ötesine Taşıma	204
20.1.3	Yedekleme Bağlantıları Oluşturmak İçin WDS'yi Kullanma	205
20.2	WDS Bağlantılarıyla İlgili Güvenlik Hususları	205
20.2.1	Statik WEP Veri Şifrelemeyi Anlama	206
20.2.2	WPA (PSK) Veri Şifrelemeyi Anlama	206
20.3	WDS Ayarlarını Yapılandırma	207
20.3.1	WDS Bağlantısı Yapılandırma Örneği	209
20.4	Ayarları Güncelleme	210

Bölüm 21: SNMP'yi Yapılandırma

21.1	SNMP Ayarlarını Anlama.....	213
21.2	SNMP Ayarlarına Gitme	214
21.3	SNMP Ayarlarını Yapılandırma	215
21.3.1	SNMP Tuzaklarını Yapılandırma	217
21.3.2	SNMP Ayarlarını Güncelleme	218

Bölüm 22: 9160 G2'nin Baz İstasyonu Olarak Kullanılması

22.1	Genel Bakış	221
22.2	Telsiz Protokolleri	222
22.2.1	Ayarlanabilir Sorgulama/Çatışma Protokolü	222
22.3	Dar Bant Menüleri	222
22.3.1	Dar Bant Telsiz Yapılandırma Ayarları	222
22.3.1.1	RA1001A Telsiz Parametreleri	224
22.3.2	Bağlantı Seçenekleri.....	225
22.3.3	Bağlantı Seçenekleri: Baz İstasyonu Modu	225
22.3.3.1	Sorgulama Protokolü Parametreleri.....	227
22.3.3.2	Telsiz Parametreleri	229
22.3.4	Bağlantı Seçenekleri: RRM Modu	231
22.4	Bağlantı Menüleri.....	231
22.4.1	Baz İstasyonu Yapılandırma Ayarları.....	233
22.4.2	RRM Grupları Yapılandırma Ayarları	234
22.4.2.1	RRM Grupları	236
22.4.2.2	Sorgulama Protokolü Parametreleri.....	237
22.4.2.3	Telsiz Parametreleri	239
22.4.2.4	Grup Parametreleri	240
22.4.2.5	Uzak Telsiz Modülleri.....	241
22.4.3	Telsiz Bağlantısı Özellikleri Yapılandırma Ayarları.....	241
22.4.3.1	Telsiz Bağlantısı Özellikleri	243
22.4.3.2	Otomatik Telsiz Adresleri	244
22.4.3.3	Otomatik Terminal Numarası.....	245
22.4.4	Ana Bilgisayarlar Menüsü.....	246
22.4.4.1	9010 Yapılandırma	249

Bölüm 23: Mini Denetleyici Yapılandırması

23.1	Genel Bakış.....	253
23.2	Mini Denetleyici Yapılandırma Menüsü.....	254
23.3	Hosts (Ana Bilgisayarlar) Menüsü	254
23.4	Ana Bilgisayar Menüsü Seçenekleri	258
23.4.1	3274 Emülasyonu	258
23.4.1.1	Emulation Options (Emülasyon Seçenekleri).....	258
23.4.1.2	TESS Options (TESS Seçenekleri)	259
23.4.1.3	Telnet Protokol Seçenekleri	269
23.4.1.4	İşlev Tuşu Eşlemeleri	273
23.4.2	5250 Emülasyonu	274
23.4.2.1	Emulation Options (Emülasyon Seçenekleri).....	274
23.4.2.2	TESS Options (TESS Seçenekleri)	275
23.4.2.3	Telnet Protokol Seçenekleri	285
23.4.2.4	İşlev Tuşu Eşlemeleri	288
23.4.3	ANSI Emülasyonu	289
23.4.3.1	Emulation Options (Emülasyon Seçenekleri).....	289
23.4.3.2	Telnet Protokol Seçenekleri	293
23.4.3.3	Otomatik Telnet/Otomatik Oturum Açma	295
23.4.3.4	İşlev Tuşu Eşlemeleri	299

Bölüm 24: 802.IQ Ayarları

24.1	802.IQ Özellikleri	303
24.1.1	802.IQ v1/v2 Genel Özellikleri.....	303
24.1.2	802.IQ v1 Özellikleri.....	306
24.1.3	802.IQ v2 Özellikleri Menüsü	307
24.2	802.IQ Ayarlarını Güncelleme	307

Bölüm 25: Ağ Zaman Protokolü Sunucusu

25.1	Zaman Ayarlarına Gitme.....	311
25.2	Ağ Zaman Protokolü (NTP) Sunucusunu Etkinleştirme veya Devre Dışı Bırakma.....	312
25.3	Ayarları Güncelleme.....	312

Bölüm 26: Yapılandırmayı Yedekleme ve Geri Yükleme

26.1	AP'nin Yapılandırma Ayarlarına Götme	315
26.2	Fabrika Varsayılanları Yapılandırmasına Sıfırlama	316
26.3	Geçerli Yapılandırmayı Yedekleme Dosyasına Kaydetme	316
26.4	Yapılandırmayı Önceden Kaydedilen Bir Dosyadan Geri Yükleme	316
26.5	Erişim Noktasını Yeniden Başlatma	317
26.6	Ürün Yazılımını Yükseltme	317
26.6.1	Güncelleme	319
26.6.2	Ürün Yazılımını Yükseltmesini Doğrulama	319

Bölüm 27: Özellikler

27.1	Fiziksel Özelliklerle İlgili Açıklamalar	323
27.2	Çevresel Gereksinimler	323
27.3	AC Güç Gereksinimleri	323
27.4	Ethernet Üzerinden Güç Gereksinimleri	323
27.5	İşlemci ve Bellek	324
27.6	Ağ Arabirimleri	324
27.7	Telsizler	324

Ek A: Bağlantı Noktası İşlev Şemaları ve Kablo Şekilleri

A.1	Konsol Bağlantı Noktası	A-1
A.2	Seri Kablo Açıklamaları	A-1
A.3	RJ-45 Konektör İşlev Şemaları (10BaseT/100BaseT Ethernet)	A-3

Ek B: Kablosuz İstemcilerde/RADIUS Sunucusunda Güvenlik Ayarları

B.1	Ağ Altyapısı; Dahili ya da Harici Kimlik Doğrulama Sunucusu Arasında Seçim Yapma	B-8
B.1.1	Dahili Kimlik Doğrulama Sunucusunu (EAP-PEAP) Kullanma	B-8
B.1.2	EAP-TLS Sertifikalı ya da EAP-PEAP'li Harici RADIUS Sunucusu Kullanma	B-8
B.2	Kablosuz İstemci Yazılımının Güncel Olduğundan Emin Olma	B-9
B.3	Microsoft Windows Kablosuz İstemci Güvenlik Ayarlarına Erişme	B-9
B.4	İstemciyi Güvenli Olmayan (Güvenlik Ayarının "None" (Yok) Olduğu) Bir Ağa Erişmesi İçin Yapılandırma	B-11

B.5	İstemcide Statik WEP Güvenliği Yapılandırma	B-12
B.6	İstemcide IEEE 802.1x Güvenliği Yapılandırma	B-15
B.6.1	EAP/PEAP Kullanan IEEE 802.1x İstemci	B-15
B.6.2	EAP/TLS Sertifikası Kullanan IEEE 802.1x İstemci	B-18
B.7	İstemcide WPA/WPA2 Kurumsal (RADIUS) Güvenliği Yapılandırma	B-22
B.7.1	EAP/PEAP Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci	B-22
B.7.2	EAP-TLS Sertifikası Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci	B-26
B.8	İstemcide WPA/WPA2 Kişisel (PSK) Güvenliği Yapılandırma	B-30
B.9	9160 G2'yi Tanıması İçin Harici Bir RADIUS Sunucusu Yapılandırma	B-33
B.10	İstemci İçin TLS-EAP Sertifikası Edinme	B-37
B.11	VLAN etiketleri için RADIUS Sunucusu Yapılandırma	B-43
B.11.1	RADIUS Sunucusu Yapılandırma	B-43

Ek C: Sorun Giderme

C.1	Kablosuz Dağıtım Sistemi (WDS) Sorunları ve Çözümleri	C-47
C.2	Küme Kurtarma	C-48
C.2.1	Erişim Noktasını Yeniden Başlatma ya da Sıfırlama	C-48

Ek D: Sözlük

Dizin	1
-------------	---

ONAYLAR VE GÜVENLİK ÖZETİ

UYGUNLUK BEYANI

Ürün:	9160 G2 Kablosuz Ağ Geçidi - RA2050, RA2060 & RA1001A
Uygulanan Konsey Direktifleri:	EMC Direktifi: 2004/108/EC Düşük Voltaj Direktifi: 2006/95/EC RoHS Direktifi: 2002/95/EC R&TTE Direktifi: 1999/5/EEC
Uygunluk Beyan Edilen Standartlar:	EN 55022: B Sınıfı EN 61000-3-2; EN 61000-3-3 EN 55024 ETSI EN 300 113-1: V1.6.1 (2006-08) EN 301 893: 2003-08 V1.2.3 EN 300 328: 2004-11 V1.6.1 EN 301 489-1/17: 2004-11 V1.5.1/ 2002-08 V1.2.1 ETSI EN 301 489-5 V1.3.1 (2002-08) EN 60950-1
Üretici:	PSION TEKLOGIX INC. 2100 Meadowvale Blvd. Mississauga, Ontario; Kanada L5N 7J9
Üretim Yılı:	2006
Üreticinin Avrupa Topluluğu'ndaki Adresi:	PSION TEKLOGIX Bourne End Business Centre Cores End Road, Bourne End, SL8 5AR Birleşik Krallık
Donanım Türü:	Bilgi Teknolojileri Donanımı
Donanım Sınıfı:	Ticari ve Hafif Sanayi

FCC Bildirimi

FCC UYGUNLUK BEYANI (DoC)

Başvuranın Adı ve Adresi:	PSION TEKLOGIX 2100 Meadowvale Blvd. Mississauga, Ontario, Kanada L5N 7J9 Tel: (905) 813-9900
ABD Temsilcisi'nin Adı ve Adresi:	Psion Teklogix Corp. 1810 Airport Exchange Blvd., Suite 500 Erlanger, Kentucky, 41018, ABD Tel: (859) 372-4329
Donanım Türü / Kullanım Alanı:	Bilgisayar Cihazları
Marka / Model No.:	9160 G2 Kablosuz Ağ Geçidi
Üretim Yılı:	2005
Uygunluk Beyan Edilen Standartlar:	Psion Teklogix tarafından sunulan 9160 G2 Kablosuz Ağ Geçidi test edilmiş ve FCC BÖLÜM 15, ALT BÖLÜM B - KASITSIZ RADYATÖRLER, B SINIFI EV VE OFİSTE KULLANIM İÇİN BİLGİSAYAR CİHAZLARI standardına uygun bulunmuştur.
Başvuran:	Psion Teklogix Inc. Mississauga, Ontario, Kanada
ABD'deki Yasal Temsilci:	Psion Teklogix Corp. Erlanger, Kentucky, ABD

9160 G2 Ağ Geçidi test edilmiş ve FCC Kuralları Bölüm 15 uyarınca B Sınıfı dijital cihaz teknik özellikleriyle uyumlu olduğu belirlenmiştir. Çalışması aşağıdaki iki koşula bağlıdır:

1. Bu cihaz zararlı parazite neden olmamalıdır
2. Bu cihaz, istenmeden çalışmasına yol açan parazitler dahil, alınan her türlü paraziti kabul etmelidir.

Bu sınırlar, bir yerleşim alanında kurulum sırasında oluşabilecek zararlı parazite karşı makul koruma sağlama amacıyla belirlenmiştir. Bu donanım, kablosuz iletişim frekansı enerjisi üretir, kullanır, yayabilir ve talimatlara uygun olarak kurulmadığında ya da kullanılmadığında, telsiz iletişimde zararlı parazitlere neden olabilir. Ancak belirli bir kurulumda parazit oluşmayacağı garanti edilmez. Bu donanım, radyo ve televizyon yayınının alınmasını olumsuz etkileyen parazite neden olursa (bu durum, donanım açılıp kapatılarak belirlenebilir) kullanıcının aşağıdaki önlemlerden birini veya birkaçını deneyerek paraziti gidermeye çalışması önerilir:

- Alıcı antenin yönünü ya da yerini değiştirme.
- Donanım veya cihazların arasındaki mesafeyi artırma.
- Donanımı alıcının prizinden başka bir prize takma.
- Bayiden veya deneyimli bir radyo/TV teknisyeninden destek istenmesi.



Önemli: *Üründe Psion Teklogix tarafından açıkça onaylanmadan yapılan değişiklik ya da düzenlemeler, kullanıcının donanımı kullanma yetkisini geçersiz kılabilir.*

RF Radyasyona Maruz Kalma Bildirimi

Bu cihazın antenlerinin FCC ve ANSI C95.1 RF maruz kalma sınırlarıyla uyumlu olması için aşağıdaki koşullarla uyumlu olması gerekir:

- Tüm erişim noktası antenleri, verilen kabloyu kullanan kişilerden en az 25 cm (9,8 inç) uzakta çalışmalı, herhangi bir antenin ya da vericinin yanında bulunmamalı veya çalıştırılmamalıdır.
- Gabriel çanak anten (P/N 9002006) en az 63,2 cm (24,9 inç) mesafe gerektirir.



Not: Çalıştırma çeşitliliği için kullanılan ikili antenler eş konumlu sayılmaz.

Industry Canada (IC) Department Of Communications Açıklaması

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

“To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.”

Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada. “Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence.”

Güvenlik Onayları

CSA, NRTL/C ve CB.

CE İşareti

Bu ürün ile onaylı Birleşik Krallık ve Avrupa'daki yan donanımları; bir yerleşim alanında, ticari ortamlarda veya hafif sanayi ortamlarında kullanıldığında CE işaretinin tüm gerekliliklerini karşılar.

R&TTE Direktifi 1999/5/EC

Bu donanım, AB Direktifi 1999/5/EC'nin (Beyan şu adreste mevcuttur: www.psionteklogix.com) başlıca gereklilikleriyle uyumludur.

Cet équipement est conforme aux principales caractéristiques définies dans la Directive européenne RTTE 1999/5/CE. (Déclaration disponible sur le site: www.psionteklogix.com).

Die Geräte erfüllen die grundlegenden Anforderungen der RTTE-Richtlinie (1999/5/EG). (Den Wortlaut der Richtlinie finden Sie unter: www.psionteklogix.com).

Questa apparecchiatura è conforme ai requisiti essenziali della Direttiva Europea R&TTE 1999/5/CE. (Dichiarazione disponibile sul sito: www.psionteklogix.com).

Este equipo cumple los requisitos principales de la Directiva 1995/5/CE de la UE, "Equipos de Terminales de Radio y Telecomunicaciones". (Declaración disponible en: www.psionteklogix.com).

Este equipamento cumpre os requisitos essenciais da Directiva 1999/5/CE do Parlamento Europeu e do Conselho (Directiva RTT). (Declaração disponível no endereço: www.psionteklogix.com).

O εξοπλισμός αυτός πληροί τις βασικές απαιτήσεις της κοινοτικής οδηγίας EU R&TTE 1999/5/EK. (Η δήλωση συμμόρφωσης διατίθεται στη διεύθυνση: www.psionteklogix.com)

Deze apparatuur voldoet aan de noodzakelijke vereisten van EU-richtlijn betreffende radioapparatuur en telecommunicatie-eindapparatuur 199/5/EG. (verklaring beschikbaar: www.psionteklogix.com).

Dette udstyr opfylder de Væsentlige krav i EU's direktiv 1999/5/EC om Radio- og teleterminaludstyr. (Erklæring findes på: www.psionteklogix.com).

Dette utstyret er i overensstemmelse med hovedkravene i R&TTE-direktivet (1999/5/EC) fra EU. (Erklæring finnes på: www.psionteklogix.com).

Utrustningen uppfyller kraven för EU-direktivet 1999/5/EC om ansluten teleutrustning och ömsesidigt erkännande av utrustningens överensstämmelse (R&TTE). (Förklaringen finns att läsa på: www.psionteklogix.com).

Tämä laite vastaa EU:n radio- ja telepäätelaitedirektiivin (EU R&TTE Directive 1999/5/EC) vaatimuksia. (Julkilausuma nähtävillä osoitteessa: www.psionteklogix.com).

Psion Teklogix tímto prohlašuje, že 9160 G2 Wireless Gateway je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1995/5/ES (NV č. 426/2000 Sb.) a Prohlášení o shodě je k dispozici na www.psionteklogix.com.

Toto zařízení lze provozovat v České republice na základě generální licence č. GL-12/R/2000.

Psion Teklogix týmto vyhlasuje, že 9160 G2 Wireless Gateway spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1995/5/ES (NV č. 443/2001 Z.z.) a Vyhlásenie o zhode je k dispozícii na www.psionteklogix.com.

Toto zariadenie je možné prevádzkovať v Slovenskej republike na základe Všeobecného povolenia č. VPR-01/2001.



Önemli Güvenlik Talimatları

Bu güvenlik bilgileri hem ürünü çalıştıran personeli hem de servis personeli koruma amaçlıdır.

- 9160 G2, yetkin bir Psion Teklogix personeli tarafından kurulmalıdır. 9160 G2'nin doğru bir şekilde kurulmaması üretici garantisini geçersiz kılacaktır.
- Şebeke elektriği kablosu (ayrı satılıyorsa), donanımın kullanılacağı ülkenin ulusal güvenlik düzenlemeleriyle uyumlu olmalıdır.
- Üretici tarafından önerilmeyen veya satılmayan aksesuarların kullanımı yangına, elektrik çarpmasına ya da kişisel yaralanmalara neden olabilir.
- Fişin ya da kablounun zarar görme riskini azaltmak için 9160 G2'yi prizden çıkarırken kablodan değil, fişten tutarak çekin.
- Kablounun; üzerine basılmayacak, takılmaya sebep olmayacak ya da hasar veya basınca maruz kalmayacak şekilde konumlandırıldığından emin olun.
- 9160 G2'yi hasar görmüş bir kabloyla veya fişle kullanmayın. Hasar görmüş bu donanımları derhal değiştirin.
- Sert bir darbe aldıysa, düştüyse veya başka bir şekilde hasar gördüyse 9160 G2'yi çalıştırmayın; cihaz böyle durumlarda, yetkin bir servis elemanı tarafından kontrol edilmelidir.
- 9160 G2'yi sökmeyin, cihaz yetkin servis elemanları tarafından tamir edilmelidir. Doğru bir şekilde yapılmayan yeniden monte işlemi elektrik çarpmasına ya da yangına neden olabilir.
- Elektrik çarpması riskini azaltmak için bakımdan veya temizlikten önce 9160 G2'yi prizden çıkarın.
- Kesinlikle gerekmedikçe uzatma kablosu kullanılmamalıdır. Uygun olmayan bir uzatma kablosunun kullanılması yangına veya elektrik çarpmasına neden olabilir. Uzatma kablosunun mutlaka kullanılması gerekiyorsa şunlardan emin olun:
 - Uzatma kablosunda fişin gireceği haznedeki giriş sayısının, boyutunun ve şeklinin adaptördekilerle aynı olduğundan.
 - Uzatma kablosunun düzgün bir şekilde yalıtıldığından, elektriksel açıdan iyi durumda olduğundan ve kablo boyutunun 16 AWG'den büyük olduğundan.
- 9160 G2 yalnızca iç mekanda kullanım için tasarlanmıştır, cihazı yağmur ya da kara maruz bırakmayın.

9160 G2 Kablosuz Ağ Geçidi Fiber Optik Seçeneği:

1. SINIF LED ÜRÜNÜDÜR
APPAREIL À LED DE CLASSE 1

Patlayıcı Ortamlarda Çalıştırmayın

Psion Teklogix donanımını patlayıcı gazların olduğu ortamlarda çalıştırmak patlamaya yol açabilir.

Kapakları Veya Muhafazaları Çıkarmayın

Yaralanmaları önlemek için donanımın kapakları ve muhafazaları sadece yetkin servis elemanları tarafından çıkarılmalıdır. Donanımı kapakları ve muhafazaları düzgün bir şekilde takılı değilken çalıştırmayın.

Antene Dokunmayın

Telsiz frekansı enerjisinin lokal ısınma etkisinin yol açacağı sıkıntıyı önlemek için 9160 G2 veri iletirken antene dokunmayın.

Dış Antene Bağlanma

Dışarıdaki anten yalnızca Psion Teklogix servis uzmanları tarafından kurulmalıdır.

Ethernet Üzerinden Güç (PoE) ve Dış Anten Kurulumu

Topraklama



Uyarı: *Dış anten ya da PoE bağlantısı kurmadan önce Topraklama İletkeni Bağlantısı yapılması gerekir.*

1. Güç kaynağı kablosundaki donanım topraklama iletkeninin yanı sıra, 9160 ile toprak arasına ek bir donanım topraklama iletkeni yerleştirilmelidir.
2. Ek donanım topraklama iletkeni, topraklı olmayan kol devre güç kaynağı iletkeninden daha küçük olabilir (nominal kesit alanı min. 0,75 milimetre kare ya da 18 AWG). Ek donanım topraklama iletkeni, 9160 Ethernet Üzerinden Güç (PoE) ya da dış anteni kullandığında toprak bağlantısını kesecek şekilde, birlikte verilen terminalden 9160'a ve toprağa bağlanmalıdır. Ek topraklama iletkeninin toprak bağlantısı, cihazın kullanıldığı ülkedeki bağlantı hattı sonlandırma kurallarına uygun olmalıdır. Ek donanım topraklama iletkeninin sonlandırılma işlemi; binaların çelik kısımlarına, metal elektrik kanalı sistemlerine ya da topraklanmış elektrikli donanıma sabit ve sağlam şekilde bağlanmış herhangi bir topraklı öğeye uygulanabilir.

3. Çıplak, üzeri kaplı ya da yalıtılmış topraklama iletkenleri kullanılabilir. Üzeri kaplı ya da yalıtılmış topraklama iletkenlerinde yeşil ya da yeşil zemin üzerinde bir veya daha fazla sarı çizgi olan dış kaplama bulunur.
4. Gök gürültülü havalarda kullanmaktan kaçının. Düşük de olsa şimşekten kaynaklanabilecek bir elektrik çarpması riski vardır.

1.1 Bu Kılavuz Hakkında.	3
1.2 Çevrimiçi Yardım Özellikleri, Desteklenen Tarayıcılar ve Sınırlamalar.	6
1.3 Metin Kuralları	7
1.4 9160 G2 Kablosuz Ağ Geçidi'ne Genel Bakış	7
1.4.1 Telsizler.	7
1.4.2 Erişim Noktası İşlevleri	9
1.4.3 Baz İstasyonu İşlevleri	9
1.4.4 Mini Denetleyici İşlevleri	9
1.5 Özellikler ve Avantajlar	10
1.5.1 IEEE Standartları Desteği ve Wi-Fi Uyumluluğu	10
1.5.2 Kablosuz Özellikleri	10
1.5.2.1 The Psion Teklogix 802.IQ Protokolü	11
1.5.3 Güvenlik Özellikleri	11
1.5.4 Kullanıma Hazır Konuk Arabirimi.	12
1.5.5 Kümeleme ve Otomatik Yönetme	12
1.5.6 Ağ.	13
1.5.7 SNMP Desteği	13
1.5.8 Bakım.	14
1.6 Sırada Ne Var?	14

1.1 Bu Kılavuz Hakkında

Bu kılavuz, kablosuz bir ağda bulunan bir ya da daha fazla 9160 G2 Kablosuz Ağ Geçidi cihazının kurulum, yapılandırma, yönetim ve bakım süreçlerini açıklamaktadır.

Bölüm 1: “Giriş”

Bu kılavuzla ve 9160 G2 Kablosuz Ağ Geçidi'nin özellikleriyle ilgili genel bilgiler sunar.

Bölüm 2: “Kurulum Gereksinimleri”

9160 G2 Kablosuz Ağ Geçidi'nin kurulumunu ve tanılamalar için 9160 G2'ye nasıl bağlanılacağını açıklar.

Bölüm 3: “Başlatma Öncesi Kontrol Listesi”

Gerekli donanım bileşenlerini, yazılımları, istemci yapılandırmalarını ve uyumluluk sorunlarını hızlıca kontrol etmeniz için bir kontrol listesi sunar.

Bölüm 4: “Kurulum ve Başlatma İçin Hızlı Adımlar”

9160 G2 Ağ Geçitlerinizi ve kablosuz ağınıza kurmak için adım adım talimatlar içerir.

Bölüm 5: “Temel Ayarları Yapılandırma”

Yönetici erişimi ayarlarının ve yeni erişim noktası ayarlarının yapılandırılmasıyla ilgili talimatlar sunar.

Bölüm 6: “Erişim Noktalarını ve Kümeleri Yönetme”

Erişim noktası kümelerini ve kümelerdeki belirli erişim noktalarında nasıl gezinileceğini anlatır.

Bölüm 7: “Kullanıcı Hesaplarını Yönetme”

İstemcinin erişim noktalarına erişiminin kontrolüyle ilgili kullanıcı yönetimi özelliklerini açıklar.

Bölüm 8: “Kanal Yönetimi”

9160 G2 Ağ Geçidi'nin karşılıklı paraziti ya da kendi kümesinin dışındaki diğer erişim noktalarıyla olan paraziti azaltmak için, kümelenmiş erişim noktaları tarafından kullanılan telsiz kanallarını otomatik olarak nasıl atadığını anlatır.

Bölüm 9: “Komşu Kablosuz Ağlar”

Komşu erişim noktalarıyla ilgili tanımlayıcı bilgiler, küme durumu ve istatistik bilgileri gibi ayrıntılı bilgiler sunar.

Bölüm 10: “Güvenliği Yapılandırma”

Kablosuz altyapınıza yalnızca istenilen kullanıcıların erişmesini sağlamak için bir dizi kimlik doğrulama ve şifreleme yöntemi sunar. Her bir güvenlik moduyla ilgili detaylı bilgiler sunulur.

Bölüm 11: “Bakım ve İzleme”

Her bir erişim noktasının bakımını ve izlenişini anlatır (küme yapılandırmaları dahil değildir).

Bölüm 12: “Ethernet (Kablolu) Arabirimi”

9160 G2 Kablosuz Ağ Geçidi'nde kablolu arabirim ayarlarının nasıl yapılandırılacağını anlatır.

Bölüm 13: “Kablosuz Arabiriminin Ayarlama”

9160 G2 Kablosuz Ağ Geçidi'nde kablosuz adres ve ilgili ayarların nasıl yapılandırılacağını anlatır.

Bölüm 14: “Konuk Erişiminin Ayarlama”

İzole bir ağa kontrollü konuk erişimi sağlamak için 9160 G2 Kablosuz Ağ Geçidi'ni yapılandırmanıza olanak sağlar.

Bölüm 15: “VLAN'ları Yapılandırma”

Sanal LAN'larda (VLAN'larda) birden fazla kablosuz ağın nasıl yapılandırılacağını açıklar.

Bölüm 16: “802.11 Telsiz Ayarlarını Yapılandırma”

9160 G2 Kablosuz Ağ Geçidi'nde telsiz ayarlarının nasıl yapılandırılacağını açıklar.

Bölüm 17: “MAC Adres Filtreleme”

İstemcinin kablosuz ağınıza erişimini kontrol etmek için MAC adresi filtrelemesini nasıl kullanacağınızı anlatır.

Bölüm 18: “Yük Dengeleme”

Kablosuz istemci bağlantılarını birden fazla erişim noktasına dengeli biçimde dağıtmanız için kablosuz aığınızda Yük Dengelemeyi nasıl yapacağınızı açıklar.

Bölüm 19: “Hizmet Kalitesi (QoS)”

Verimi ve ayrılan kablosuz trafiğin performansını artırmak için birden fazla kuyruktaki parametreleri yapılandırmak için gerekli talimatları sunar.

Bölüm 20: “Kablosuz Dağıtım Sistemi”

Birden fazla erişim noktasını birbirine bağlayarak kendi aralarında standart yollarla kablosuz olarak iletişim kurmalarını sağlayan ve 9160 G2 Kablosuz Ağ Geçidi'nde yer alan Kablosuz Dağıtım Sistemi'nin (WDS) nasıl yapılandırılacağını anlatır.

Bölüm 21: “SNMP'yi Yapılandırma”

9160 G2 Kablosuz Ağ Geçidi Kurumsal-Yönetici API'da SNMP ve ilgili ayarların nasıl yapılandırılacağını açıklar.

Bölüm 22: “9160 G2’nin Baz İstasyonu Olarak Kullanılması”

9160 G2 Kablosuz Ağ Geçidi'nin kablolu ya da kablosuz bir baz istasyonu veya Uzak Telsiz Modülü (RRM) olarak nasıl yapılandırılacağını açıklar. Bu bölümde, dar bant telsiz yapılandırma ayarları da anlatılır.

Bölüm 23: “Mini Denetleyici Yapılandırması”

9160 G2 Kablosuz Ağ Geçidi'nin mini denetleyici olarak kullanıldığında nasıl yapılandırılacağını anlatır.

Bölüm 24: “802.IQ Ayarları”

9160 G2 baz istasyonları ve mini denetleyiciler için 802.IQ özel kablosuz protokol ayarlarını açıklar.

Bölüm 25: “Ağ Zaman Protokolü Sunucusu”

Ağınızdaki bilgisayar saatlerini senkronize etmek üzere belirli bir Ağ Zaman Protokolü (NTP) sunucusu kullanmak için 9160 G2 Kablosuz Ağ Geçidi'nin nasıl yapılandırılacağını anlatır.

Bölüm 26: “Yapılandırmayı Yedekleme ve Geri Yükleme”

Bir erişim noktasını önceden kaydedilen yapılandırmaya geri döndürmek amacıyla ileride kullanılabilecek bir yapılandırma dosyasının nasıl yedekleneceğini gösterir.

Bölüm 27: “Özellikler”

9160 G2 Kablosuz Ağ Geçidi ve telsizlerinin fiziksel, çevresel ve çeşitli çalışma özelliklerini ayrıntılı biçimde açıklar.

Ek A: Bağlantı Noktası İşlev Şemaları ve Kablo Şekilleri

9160 G2'nin bağlantı noktaları ve kablolarıyla ilgili işlev şemalarını ve şekillerini içerir.

Ek B: Kablosuz İstemcilerde/RADIUS Sunucusunda Güvenlik Ayarları

İstemciye güvenlik ayarlarının her bir ağ (AP) bağlantısı tarafından kullanılan güvenlik moduyla eşleşmesi için nasıl yapılandırılacağını ayrıntılarıyla açıklar.

Ek C: Sorun Giderme

Birden fazla kümelenmiş erişim noktası tarafından sunulan ağlarda ağ yapılandırmalarını güncellerken karşılaşılabilecek olası sorunların nasıl çözüleceğini anlatır.

Ek D: Sözlük

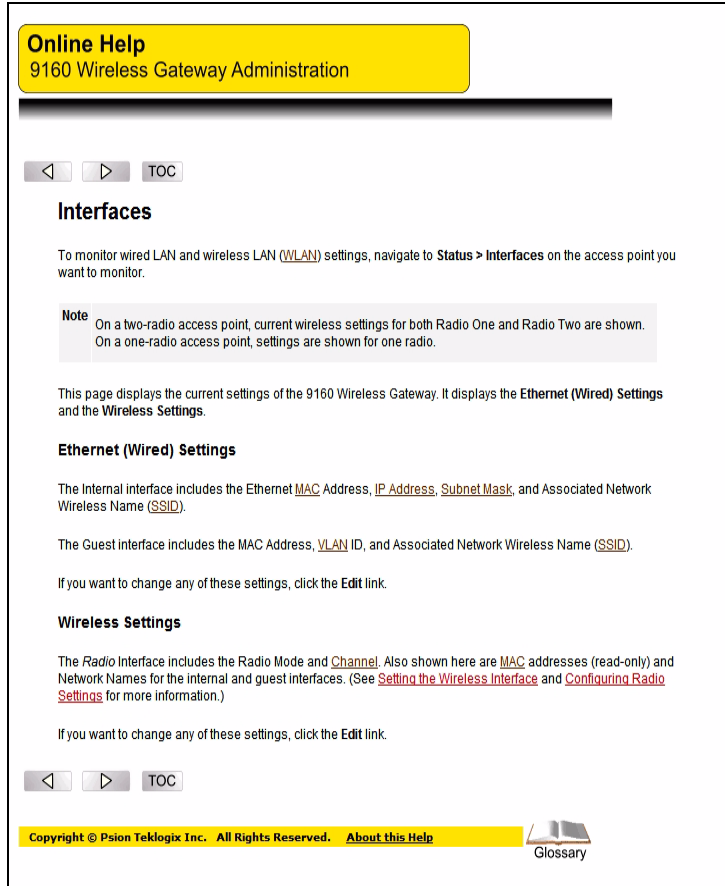
Kılavuzda kalın italik harflerle belirtilen terimlerin tanımlarını ve bu terimlerle ilgili ayrıntılı bilgileri içerir.

1.2 Çevrimiçi Yardım Özellikleri, Desteklenen Tarayıcılar ve Sınırlamalar

9160 G2 Kablosuz Ağ Geçidi için Çevrimiçi Yardım, kullanıcı arabirimindeki tüm alan ve özellikler hakkında bilgi sunar. Çevrimiçi Yardım, kullanım kılavuzundaki bilgilerin bir kısmını içerir.

Çevrimiçi Yardım'daki bilgiler, 9160 G2 Kablosuz Ağ Geçidi Yönetimi kullanıcı arabirimindeki sekmelere karşılık gelir. Bulunduğunuz sekmenin ayarları hakkında bilgi almak için sekmedeki **Help** (Yardım) düğmesine ya da kullanıcı arabirimindeki çevrimiçi yardım panelinin alt kısmında yer alan “More...” (Daha Fazla...) bağlantısına tıklayın.

Şekil 1.1 Çevrimiçi Yardım Ekranı



1.3 Metin Kuralları



Not: Notlar yardımcı ek bilgileri vurgular.



Önemli: *Bu açıklamalar özellikle önemli talimatları ya da bilgisayarın veya diğer donanımların çalışmasıyla ilgili kritik ek bilgileri içerir.*



Uyarı: *Bu açıklamalar yaralanmaları, donanım hasarlarını ya da veri kaybını önleyebilecek önemli bilgiler içerir.*



Alan ve açıklama bilgilerinin (genellikle tablolarda bulunur) yanındaki ok işareti Erişim Noktası (AP) üzerinde bulunan bir seçenek için tavsiye edilen ya da sunulan bir yapılandırma ayarını belirtir.

Kalın İtalik harflerle yazılmış terimler Ek D: “Sözlük” bölümünde tanımlanır ve ayrıntılı biçimde açıklanır. Kılavuzdaki tüm terimler kalın italik olarak vurgulanmamıştır. Sözlük, vurgulanmamış terimleri de içermektedir; bu nedenle bilmediğiniz kelime ya da ifadeleri sözlükte arayabilirsiniz.

1.4 9160 G2 Kablosuz Ağ Geçidi'ne Genel Bakış

9160 G2 Kablosuz Ağ Geçidi, kablosuz ve Ethernet cihazlarınız arasında sürekli ve yüksek hızlı erişim sağlar. Küçük ve orta ölçekli işletmelerin kablosuz ağları için gelişmiş, standart tabanlı bir çözümdür. 9160 G2 Kablosuz Ağ Geçidi, gelişmiş kablosuz ağ özellikleri sağlarken yönetim gerektirmeyen kablosuz yerel alan ağı (**WLAN**) kullanma olanağı sunar.

9160 G2 Kablosuz Ağ Geçidi; en iyi güvenlik özellikleri, yönetim kolaylığı ve sektör standartlarını sunarak ek yönetim ve güvenlik sunucusu yazılımlarına ihtiyaç duymayan bağımsız ve tamamen güvenli bir kablosuz ağı sunar.

9160 G2 Kablosuz Ağ Geçidi, çok çeşitli sistem yapılandırmalarını destekleyecek şekilde tasarlanmıştır. IEEE 802.11 Kablosuz LAN Standartlarını kullanan 9160 G2, kablosuz ve kablolu ağlar arasında görünmez bir köprü (erişim noktası) işlevi görebilir. Bu sayede kablosuz istemciler ağa erişebilir ve ağdaki 9160 G2'ler arasında sorunsuzca hareket edebilir. 9160 G2 mini denetleyici, baz istasyonu ve uzak telsiz modülü (RRM) olarak kullanılabilir ve mapRF sistemlerinin bir parçası olabilir.

1.4.1 Telsizler

9160 G2, tek ya da çift telsizle çalışmayı destekler. Kullanılabilen telsiz modülleri şunlardır: 802.11a/g telsiz, 802.11g telsiz ve RA1001A dar bant telsiz. Bu telsizlerin ayrıntılı teknik özellikleri için bkz. "Telsizler", sayfa 324.

Eriřim noktası, kurulu olan telsizlerin türüne baęlı olarak řu modlarda alıřabilir:

- IEEE **802.11b** modu.
- IEEE **802.11g** modu.
- IEEE **802.11a** modu.
- Atheros Turbo 5 GHz.
- Atheros Dynamic Turbo 5 GHz.
- Atheros Turbo 2,4 GHz.
- Atheros Dynamic Turbo 2,4 GHz.
- Uzun Menzil.
- Psion Teklogix Dar Bant Sorgulama Protokolü.



Önemli: *Psion Teklogix mobil bilgisayarlar, Atheros Turbo modlarını desteklemez. Gereksiz telsiz yükünü önlemek için Turbo modunun kullanılması önerilmez.*

9160 G2 Kablosuz Ağ Geçidi dört farklı telsiz yapılandırmasını destekler: 802.11g, 802.11g + 802.11ag, NB (dar bant) ve NB + 802.11ag.

Bu farklı seçenekler *Maintenance > Upgrade* (Bakım > Yükseltme) web sayfasında (bkz. Şekil 1.2, sayfa 9) gösterilen "Model" değeri tarafından belirlenir. Modeller řu şekilde tanımlanır:

- 9160 Kablosuz Ağ Geçidi = 802.11g.
- 9160 Kablosuz Ağ Geçidi (Çift Telsiz) = 802.11g + 802.11ag.
- 9160 Kablosuz Ağ Geçidi NB = NB.
- 9160 Kablosuz Ağ Geçidi NB (Çift Telsiz) = NB + 802.11ag.



Not: *"Yalnızca NB" durumunda, web sayfası tek bir 802.11 telsizinin yapılandırma sayfasını gösterebilir. Bu sayfayı görmezden gelebilirsiniz ancak bu var olmayan telsizi yapılandırmayı denerseniz bu durum 9160 G2'de herhangi bir soruna yol açmaz.*

Şekil 1.2 Ürün Yazılımı Yükseltme Sayfası

Upgrade firmware

Model	9160 Wireless Gateway NB (Dual Radio)
Platform	PTX9160G2
Firmware Version	E187k

New Firmware Image

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

1.4.2 Erişim Noktası İşlevleri

Bir erişim noktası, kablolu bir ağa bağlandığında 9160 G2 Kablosuz Ağ Geçidi, Psion Teklogix RF mobil bilgisayarlar veya kablosuz erişim noktası istemcileriyle bir Psion Teklogix Ağ Denetleyicisi ya da ana bilgisayar arasında iletişim bağlantısı kurar. Mobil bilgisayarlarla IEEE 802.11 RF veri bağlantısı üzerinden, ağ denetleyicisi ya da ana bilgisayarlarla kablo üzerinden iletişim kurar. 9160 G2, Ethernet bağlantısıyla ağa bağlanabilir.

1.4.3 Baz İstasyonu İşlevleri

9160 G2, baz istasyonu ya da Uzak Telsiz Modülü (RRM) olarak kullanıldığında özel Psion Teklogix telsiz protokollerini kullanarak yerel alan ağı ve kablosuz mobil bilgisayarlar arasında bir bağlantı oluşturur. 9160 G2 baz istasyonu (ya da RRM), yerel alan ağında TCP/IP üzerinden özel 9010 protokolünü kullanarak bir 9500 İletişim Sunucusuyla (ya da Psion Teklogix Yazılım Geliştirme Paketini kullanarak bir ana bilgisayarla) iletişim kurar. 9160 G2'yi baz istasyonu ya da RRM olarak yapılandırma hakkında bilgi için bkz. Bölüm 22: “9160 G2'nin Baz İstasyonu Olarak Kullanılması”.

1.4.4 Mini Denetleyici İşlevleri

9160 G2, mini bir denetleyici olarak kullanılmasına olanak veren bazı emülasyon özelliklerine sahiptir. 9160 G2 mini denetleyici olarak yapılandırıldığında Psion Teklogix mobil bilgisayarlar, 9500 İletişim Sunucusu yerine 9160 G2 aracılığıyla bir ANSI, 5250 ya da 3274 mobil bilgisayar gibi çalışabilir.

9160 G2 Ağ Geçidi'ni mini denetleyici olarak yapılandırmak için bkz. Bölüm 23: “Mini Denetleyici Yapılandırması”.

1.5 Özellikler ve Avantajlar

1.5.1 IEEE Standartları Desteği ve Wi-Fi Uyumluluğu

- IEEE **802.11a**, IEEE **802.11b**, IEEE **802.11g**, IEEE **802.11i** ve IEEE **802.3af** kablosuz ağ standartları için destek.
- IEEE **802.11a** ya da IEEE **802.11g** için 54 Mb/sn'ye kadar bant genişliği sunar (IEEE **802.11b** için 11 Mb/sn, Atheros **802.11a Turbo** için 108 Mb/sn).
- Sertifika için Wi-Fi uyumluluğu gereklidir.

1.5.2 Kablosuz Özellikleri

- Başlarken otomatik kanal seçimi.
- İletim gücünü ayarlama.
- Birden fazla erişim noktasını kablosuz olarak bağlamak için Kablosuz Dağıtım Sistemi (**WDS**). Ağınızı daha az kabloyla genişletir.
- Video, ses, IP üzerinden ses (VoIP) ve medya akışı gibi zaman açısından duyarlı kablosuz trafiğin daha fazla verim ve daha iyi performansla sahip olması için Hizmet Kalitesi (**QoS**). Hizmet Kalitemiz (QoS), Wi-Fi Multimedia (WMM) ile uyumludur.
- Yük dengeleme.
- Aynı erişim noktası üzerinde birden çok **SSID** (ağ adları) ve birden çok **BSSID** (temel hizmet seti kimlikleri) için dahili destek.
Biri dahili (birincil ve yönetim) ağ, diğeri konuk ağı için olmak üzere iki özel amaçlı BSSID desteklenmektedir. Genel amaçlı altı ek BSSID (Sanal Kablosuz Ağ ya da VWN olarak adlandırılır), VLAN'lar kullanılarak desteklenir.
- Ağdaki AP - AP parazitini azaltmak ve Wi-Fi bant aralığını en üst düzeye çıkarmak amacıyla telsiz kanalı atamalarını otomatik olarak koordine etmek için kanal yönetimi.
- Komşu erişim noktalarını algılama ("Rogue" AP algılama olarak da bilinir).
- **IEEE 802.11d** Düzenleyici Etki Alanı seçimi desteği (global kullanma için ülke kodları).
- TPC ve DFS hizmetlerini içeren **IEEE 802.11h** desteği.
IEEE 802.11h, 5 GHz bant için belirli düzenleyici etki alanlarının karşılanması için gerekli olan iki hizmeti sunan bir standarttır. Bu iki hizmet şunlardır: İletim Gücü Kontrolü (TPC) ve Dinamik Frekans Seçimi (DFS).
- Uzun Menzil (XR) desteği.

- SpectraLink Ses Önceliği (SVP).
SpectraLink Ses Önceliği (SVP), Wi-Fi kullanımı için bir Hizmet Kalitesi (QoS) yaklaşımıdır. SVP, IEEE 802.11b standardıyla uyumlu olan açık bir özelliktir. SVP, Kablosuz LAN'daki bekleme süresini en aza indirir ve veri paketleri yerine ses paketlerine öncelik vererek daha iyi ağ performansı elde edilmesinin olasılığını artırır.

1.5.2.1 The Psion Teklogix 802.IQ Protokolü

802.IQ, mobil bilgisayarların aynı anda hem TCP/IP hem de 802.IQ protokollerini destekleyen bir ağdaki kablosuz LAN'da çalışmasına olanak sağlayan bir Psion Teklogix özel protokolüdür. 802.IQ protokolünün 802.IQ v1 ve 802.IQ v2. olmak üzere iki sürümü vardır. 9160 G2 Kablosuz Ağ Geçidi aynı anda protokolün iki sürümünü de destekler (mobil bilgisayarlar yalnızca birini kullanmalıdır).

802.IQ v1 protokolü, TCP/IP yönlendirmeye göre 802.11 kablosuz ağda daha iyi performans sağlayan bir kablosuz LAN yönlendirme sistemidir. Mobil bilgisayarlar TCP/IP ya da 802.IQ v1 protokolünü kullanarak 9160 G2 erişim noktasıyla iletişim kurabilir. Bu özellik, iki şekilde çalışabilen bir sistemi mümkün kılar.

802.IQ v2 protokolü, paketleri UDP katmanı üzerinden aktaran 802.IQ v1 protokolünün geliştirilmiş bir sürümüdür. 802.IQ v1'in tüm işlevlerine sahip olmanın yanı sıra, RF üzerinden yazılım yükseltme, denetleyiciler ve mobil bilgisayarlar arasında üçüncü taraf erişim noktaları ekleme ve istenildiğinde MapRF sistemine entegre olma gibi ek özellikler sunar.

802.IQ ile ilgili daha fazla bilgi ve yapılandırma menüleri için bkz. Bölüm 24: “802.IQ Ayarları”.

1.5.3 Güvenlik Özellikleri

- SSID Yayınını Engelleme.
- SSID Yayınını Yok Sayma.
- Zayıf IV'den kaçınma.
- Kablosuza Eş Değer Gizlilik (**WEP**).
- Şu standartlar için Wi-Fi sertifikalıdır:
 - IEEE Standartları: 802.11b, 802.11g, 802.11d
 - Güvenlik:
 - WPA™ - Kişisel
 - WPA™ - Kurumsal
 - WPA2™ - Kişisel
 - WPA2™ - Kurumsal

- EAP Türleri:
 - EAP-TLS
 - EAP-TTLS/MSCHAPv2
 - PEAPv0/EAP-MSCHAPv2
 - PEAPv1/EAP-GTC
 - EAP-SIM
- Gelişmiş Şifreleme Standardı (**AES**).
- Yerel kimlik doğrulama sunucusuyla kullanıcı tabanlı erişim kontrolü.
- Yerel kullanıcı veritabanı ve kullanıcı yaşam döngüsü yönetimi.
- MAC adresi filtreleme.
- **WDS** üzerinden WPA/WPA2.
- Güvenli Yuva Kabuğu (SSH).
- Güvenli Yuva Katmanı (SSL).

1.5.4 Kullanıma Hazır Konuk Arabirimi

- Konuk Arabirimi için benzersiz ağ adı (**SSID**).
- Konukları onlara özel, isteğe göre uyarlanabilen web sayfasına yönlendiren bağlı portal.
- VLAN ve Ethernet seçenekleri.

1.5.5 Kümeleme ve Otomatik Yönetme

- AP'lerin kümeleme ve küme birleştirme aracılığıyla sağlanması ve otomatik yapılandırılması.

Yönetici yeni erişim noktalarının ağa eklenmeden önce nasıl yapılandırılacağını belirleyebilir. Yeni erişim noktaları eklendiğinde otomatik olarak kümeyle birleşebilir ve doğru yapılandırmayı güvenli bir şekilde indirebilir. Bu süreç elle müdahaleyi gerektirmez ancak yöneticinin kontrolü altındadır.

- Kümelenmiş erişim noktalarının ve küme yapılandırma ayarlarının tek evrensel görünümü.

Bir kümedeki tüm erişim noktalarının yapılandırması tek bir arabirimden yönetilebilir. Ortak parametrelerdeki değişiklikler kümenin tüm elemanlarına otomatik olarak yansıtılır.

- Otomatik yapılandırma senkronizasyonuna sahip kendi kendini yöneten erişim noktaları.

Bir kümedeki erişim noktaları küme yapılandırmasının tutarlı olup olmadığını periyodik olarak kontrol eder ve kümenin diğer elemanlarının varlığını ve kullanılabilirliğini denetler. Yönetici bu bilgiyi kullanıcı arabiriminden izleyebilir.

- Ek BT kurulumu gerekmeden 802.1x kullanarak gelişmiş yerel kimlik doğrulama.

Kümeler, kullanıcı kimlik doğrulama sunucularını ve erişim noktalarında depolanan veritabanlarını içerebilir. Böylece; bir **RADIUS** altyapısını yüklemeye, yapılandırmaya ve muhafaza etmeye gerek kalmaz. Ayrıca bir yönetici görevi olan güvenli kablosuz ağ kullanmayı kolaylaştırır.

1.5.6 Ağ

- Ağ yapılandırma bilgisini dinamik olarak elde etmek için Dinamik Ana Bilgisayar Yapılandırma Protokolü (**DHCP**) desteği.
- Sanal Yerel Alan Ağı (VLAN) desteği.
- Sanal Kablosuz Ağlar (Dinamik VLAN'lar).
- Yayılan Ağaç Protokolü (**STP**).
- **802.1p**.
- 100Base-FX fiber optik desteği.

1.5.7 SNMP Desteği

9160 G2 Kablosuz Ağ Geçidi, şu standart Basit Ağ Yönetimi Protokolü (**SNMP**) Yönetim Bilgi Tabanlarını (**MIB**'ler) içerir:

- Köprü MIB 802.1d (RFC 1493).
- SNMPv2 MIB (RFC 3418).
- IEEE Std 802.11 MIB (taban).
- Arabirim Grubu MIB (RFC 2233).
- Yeni IEEE 802.11k MIB'ye dayanan iki özel MIB (Kablosuz MIB ve Sistem MIB'si). Bu MIB'ler sırasıyla 9160 G2 Kablosuz Ağ Geçidi istemci ilişkisi listesi ve AP algılama tablosuyla ilgili bilgi sağlar. Özel Sistem MIB'si sistemi yeniden başlatma ve ürün yazılımı yükseltme gibi bakım işlevleri sağlar.

1.5.8 Bakım

- Oturum izleme, istemci ilişkileri, alma/verme istatistikleri ve olay günlüğü dahil, ağın durumu, takibi ve izlenme görüntüleri.
- Ağ trafik etkinliğinin seviyesinden bağımsız olarak istemci bağlantısını sürekli bir şekilde doğrulamak için bağlantı bütünlüğünü izleme.
- Yapılandırmayı sıfırlama seçeneği.
- Ürün yazılımı yükseltmesi.
- Erişim noktası yapılandırmasını yedekleme ve geri yükleme.
- Dahili RADIUS sunucusu için kullanıcı veritabanını yedekleme ve geri yükleme (IEEE 802.1x ve WPA/WPA2 Kurumsal (RADIUS) güvenlik modlarıyla kullanılabilir).

1.6 Sırada Ne Var?

Kablosuz ağa geçmeye hazır mısınız? 9160 G2 Kablosuz Ağ Geçidinizi kurduktan sonra (bkz. Bölüm 2: “Kurulum Gereksinimleri”) Bölüm 3: “Başlatma Öncesi Kontrol Listesi” bölümünü okuyun ve ardından Bölüm 4: “Kurulum ve Başlatma İçin Hızlı Adımlar” bölümündeki adımları izleyin.

KURULUM GEREKSİNİMLERİ

2

2.1 Doğru Konumu Seçme	17
2.1.1 Çevre	17
2.1.2 Bakım.	18
2.1.3 Telsizler.	18
2.1.4 Güç ve Anten Kabloları	18
2.1.4.1 Güç	18
2.1.4.2 Antenler	19
2.2 Harici Cihazlara Bağlanma.	20
2.2.1 Bağlantı noktaları.	20
2.2.2 LAN Kurulumu: Genel Bakış	21
2.2.3 LAN Kurulumu: Ethernet	21
2.2.3.1 Ethernet Kablosu	22
2.2.3.2 100Base-FX Fiber Optik Ethernet Bağlantı Noktası	22
2.2.4 Durum Göstergeleri (LED'ler)	22
2.2.5 Video Ekranı Terminaline Bağlanma.	23
2.3 Yapılandırmayı Web Tarayıcıyla Değiştirme.	23



Uyarı: 9160 G2, yetkin bir Psion Teklogix personeli tarafından kurulmalıdır.

2.1 Doğru Konumu Seçme

Psion Teklogix genellikle bir alan incelemesi yapar ve 9160 G2 için tercih edilen konumlarla ilgili önerilerde bulunur. Bu konumlar iyi bir telsiz kapsama alanı içeren, ana bilgisayarla ya da ağ denetleyiciyle olan mesafeyi en aza indiren ve çevresel gereksinimleri karşılayan yerlerdir.

2.1.1 Çevre

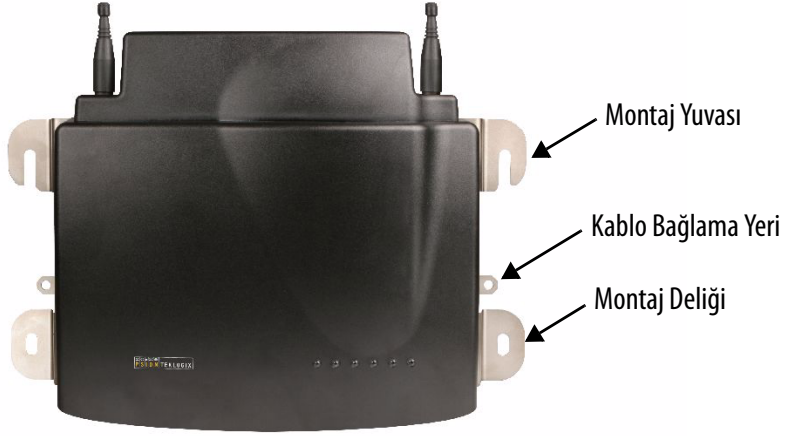
9160 G2, iyi havalandırılan bir alana yerleştirilmeli ve aşırı sıcaklık değişikliklerinden (örneğin doğrudan ısıtıcıdan, nakliye depolarının kapılarından ya da doğrudan güneşe maruz kalmadan dolayı gelen sıcaklık) korunmalıdır. Koruyucu bir kapak gerekliyse birimin düzgün biçimde çalışabilmesi için yeterli havalandırmanın sağlanması gerekir.

Çevresel gereklilikler hakkında daha ayrıntılı açıklamalar için bkz. Bölüm 27: “Özellikler”. Çevresel koşullar bu kılavuzda listelenen koşullar kadar zorlu olmadığında ekipmanın uzun vadeli istikrarının artacağını unutmayın.

9160 G2, araçların geçtiği yollardan, sudan ve tozdan uzak olacak şekilde konumlandırılmalıdır. 9160 G2 Şekil 2.1, sayfa 18'de gösterildiği gibi yalnızca dik konumda monte edilmelidir. Bu şekilde, 9160 G2 yanlışlıkla suya maruz kaldığında birimin içine su girme riski en aza iner.

9160 G2, arka kapaktaki dört vidayla dikey bir yüzeye monte edilir (vidaların türü, cihazın monte edileceği yüzeye göre değişiklik gösterir). Arka kapaktaki iki delik, kalan cıvatalar takılmadan önce birimin asılı durmasını sağlayarak kurulumu kolaylaştıran yuvalardır. Kurulum için SAE 1/4-20 cıvataları kullanılır.

Şekil 2.1 9160 G2 Kurulum Pozisyonu



2.1.2 Bakım

9160 G2'de dahili seçenek değiştirme özelliği yoktur ve birim fiziksel erişim gerektirmez. Tüm yapılandırmalar uzaktan gerçekleştirilir. (bkz "Temel Ayarlara Gitme", sayfa 47). Çevresel ve telsiz iletişimi hususları geçerlidir.

2.1.3 Telsizler

- Entegre antensiz 802.11g telsiz (standart).
- Entegre antensiz 802.11a/g telsiz (isteğe bağlı ikinci telsiz).
- RA1001A - Dar Bant (NB) Telsiz.

2.1.4 Güç ve Anten Kabloları

2.1.4.1 Güç

Bağlantının yanlışlıkla kopmasını ve 9160 G2'deki baskıyı önlemek için anten ve güç kabloları, birimden 30 cm uzakta olacak şekilde sabitlenmelidir. Kabloları 9160 G2'deki kablo bağlantı yerlerinden geçirerek sabitleyin (bkz. Şekil 2.1). 9160 G2'nin bir metre (3,1 ft) yakınında tek fazlı bir priz (100 - 240 V AC , minimum 1,0 A) olmalıdır. 9160 G2, bu güç aralığındaki girişleri otomatik olarak ayarlar. Güç kablosu çıkarılabilir ve bulunduğunuz yerde kullanılan güç türüne uygundur. 9160 G2 AC güç kaynağı, standart bir IEC320 konektörü aracılığıyla evrensel giriş sunar.

9160 G2 Kablosuz Ağ Geçidi, AC kablosu ihtiyacını ortadan kaldırmak için IEEE 802.3af standardıyla uyumludur ve Ethernet bağlantısı üzerinden kullanılabilir. Ayrıntılı bilgi için bkz. "Ethernet Üzerinden Güç Gereksinimleri", sayfa 323.



Uyarı: *Elektrik çarpmasını önlemek için güç kablosunun koruyucu topraklama iletkeni her zaman toprağa bağlı olmalıdır.*

2.1.4.2 Antenler

Her kurulum için gereken anten türü kapsama alanı gereksinimlerine ve kullanılan frekanslara göre değişiklik gösterir. En fazla dört anten kullanılabilir. Bu antenler ters dişli SMA "vidalı" çeşitlerin ya da yüksek verimli WDS antenlerin bir kombinasyonu olabilir. Psion Teklogix'de çeşitli çok yönlü antenler ve özel, yönlü antenler bulabilirsiniz. Alan incelemesinde genellikle hangi antenin uygun olduğu belirlenir. Daha fazla bilgi için Psion Teklogix servis elemanlarına danışın.



Uyarı: *9160 G2'yi asla uygun bir anten ya da yapay yük olmadan çalıştırmayın.*

Dış Antene Bağlama (P/N 1916641 Kiti)

Anten, yetkin bir servis elemanı tarafından yerel elektrikli cihaz kurulum kurallarına uygun biçimde kurulmalıdır. Anten, kullanıcı ve o bölgede çalışan diğer kişilerden en az 4,6 m (15 ft) yüksekte ve 3 m (10 ft) uzakta olacak şekilde konumlandırılmalıdır.

Dış antene bağlanan bir 9160 G2 için aşağıdaki notların hepsi geçerlidir:

1. Kurulum, cihazın kullanılacağı ülkedeki yetkililerce uygun bulunduğu takdirde, anten koaksiyel kablosunun koruyucu kısmı, bina tesisatındaki toprağa (9160 G2'den bağımsız olarak) bağlı olmalıdır.
2. Güç kaynağı kablosundaki donanım topraklama iletkeninin yanı sıra, 9160 G2 ile toprak arasına ek bir donanım topraklama iletkeni yerleştirilmelidir.
3. Ek donanım topraklama iletkeni, topraklı olmayan kol devre güç kaynağı iletkeninden daha küçük olabilir (nominal kesit alanı min. 0,75 milimetre kare ya da 18 AWG). Ek donanım topraklama iletkeni, güç kaynağının fişi çekildiğinde toprak bağlantısını kesecek şekilde, birlikte verilen terminalden 9160 G2'ye ve toprağa bağlanmalıdır. Ek topraklama iletkeninin toprak bağlantısı, cihazın kullanıldığı ülkedeki bağlantı hattı sonlandırma kurallarına uygun olmalıdır. Ek donanım topraklama iletkeninin sonlandırılma işlemi binaların çelik kısımlarına, metal elektrik kanalı sistemlerine ya da topraklanmış elektrikli donanıma sabit ve sağlam şekilde bağlanmış herhangi bir topraklı öğeye uygulanabilir.

4. Çıplak, üzeri kaplı ya da yalıtılmış topraklama iletkenleri kullanılabilir. Üzeri kaplı ya da yalıtılmış topraklama iletkenlerinde yeşil (yalnızca Kanada ve ABD) ya da yeşil-sarı (tüm ülkeler) dış kaplama bulunur.
5. Gök gürültülü havalarda kullanmaktan kaçının. Düşük de olsa şimşekten kaynaklanabilecek bir elektrik çarpması riski vardır.
6. Finlandiya, Norveç ve İsveç için: Ekipman, eşpotansiyel bağının uygulandığı ERİŞİMİN KISITLI OLDUĞU YERLERDE kullanılır. Kalıcı olarak bağlanan KORUYUCU TOPRAKLAMA İLETKENİ SERVİS ELEMANLARI tarafından takılmalıdır.



Uyarı: *RF güvenlik hususları gereği kullanıcıların antene yaklaşması yasaktır.*

Psion Teklogix, 9160 G2'nin antene bağlanması için gereken koaksiyel kabloyu sağlar. Antenin yeri belirlenirken, antenin kapsama alanı gereksinimleri 9160 G2'nin çevresel gereksinimleriyle birlikte göz önüne alınır.

Koaksiyel kablolar, kablo çengeli ve/veya koaksiyel kablo klipsleri kullanılarak yönlendirilmeli ve sabitlenmelidir. 9160 G2'nin anten bağlantısını kolayca kesmek için antenin yanında birkaç santimetre kablo payı bırakılmalıdır.

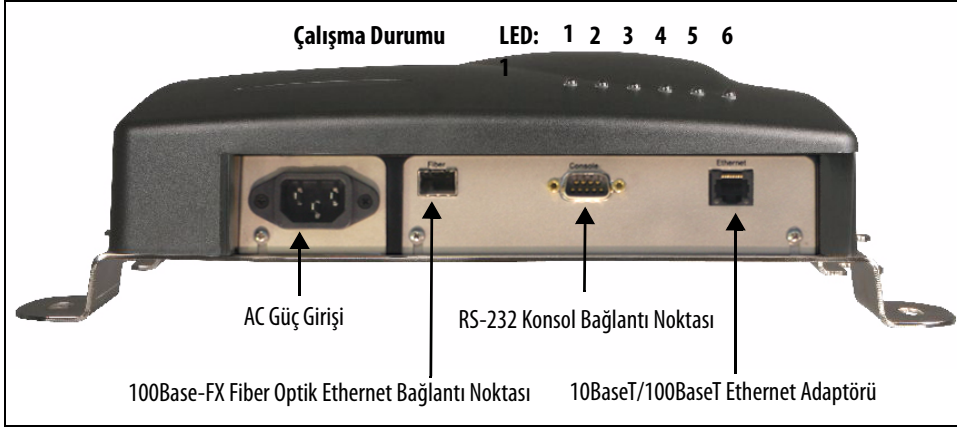
2.2 Harici Cihazlara Bağlanma

Bu bölümde, 9160 G2'yi ağ denetleyicileri, baz istasyonları, ana bilgisayarlar, bilgisayarlar ve video ekranı terminalleri gibi harici cihazlara bağlamaya ilgili genel talimatlar yer alır.

2.2.1 Bağlantı noktaları

Şekil 2.2, sayfa 21, 9160 G2'nin tabanında yer alan bağlantı noktalarını ve güç konektörlerini gösterir. Bağlantı noktası işlev şemaları Ek A: “Bağlantı Noktası İşlev Şemaları ve Kablo Şekilleri” bölümünde gösterilmiştir.

Şekil 2.2 9160 G2 Bağlantı Noktası ve LED Konumları



* Not: 9160 G2'nin önceki sürümlerinde fiber optik bağlantı noktası bulunmaz.

2.2.2 LAN Kurulumu: Genel Bakış

9160 G2 Ethernet bağlantısı sunduğu için mevcut bir LAN'a eklenebilir. Ağ yöneticileri, kendi ağlarını ve ağ yapılandırmalarını bildiklerinden LAN kurulumları genellikle ağ yöneticilerinin yardımıyla yapılır. 9160 G2 kurulduktan, bağlandıktan ve açıldıktan sonra sistem yöneticisi yapılandırmayı kontrol etmek ve 9160 G2'ye özel IP adresini atamak için cihaza erişebilir. Bu işlem ağ aracılığıyla yapılabilir (bkz. "Yapılandırmayı Web Tarayıcıyla Değiştirme", sayfa 23). Ağda yeni istemci ve kullanıcı ekleme gibi birbirini izleyen değişiklikler olduğunda 9160 G2'nin yapılandırmasının da değiştirilmesini gerekir.



Önemli: 9160 G2 ilk kez yapılandırılıp yeniden başlatıldığında, 9160 G2 IP adresini sunucudan almıyorsa DHCP devre dışı olmalıdır.

2.2.3 LAN Kurulumu: Ethernet

9160 G2, 100 Mb/sn Hızlı Ethernet LAN'larının ve 10 Mb/sn LAN'larının tam ve yarı iki yönlü çalışmasını destekleyen yüksek performanslı bir Erişim Noktasıdır. Cihaz, aşağıdakilerle birlikte gelir:

- 10BaseT/100BaseT kart (5. kategori çift bükümlü kablo, 10 ya da 100 Mb/sn hızla çalışan RJ-45 konektör). Bağlantı noktası işlev şemaları için bkz Ek A: "Bağlantı Noktası İşlev Şemaları ve Kablo Şekilleri".
- 100Base-FX fiber optik bağlantı noktası (ayrıntılar için bkz. Bölüm 2.2.3.2).



Not: 9160 G2, Ethernet 10BaseT, 100BaseT ve 100Base-FX'ten başka herhangi bir bağlantı türü desteklemez.

2.2.3.1 Ethernet Kablosu

9160 G2'de (10BaseT/100BaseT Ethernet kablosu) yineleyiciler arası izin verilen maksimum kablo uzunluğu 100 metredir.

2.2.3.2 100Base-FX Fiber Optik Ethernet Bağlantı Noktası

9160 G2 Kablosuz Ağ Geçidi, 100Base-FX fiber optik ağı desteği sunar. Kullanıcıların fiber optik Ethernet bağlantı noktasını kullanabilmeleri için 9160 G2 fiber genişletme yuvasına küçük takılabilir bir (SFP) 100Base-FX modülü kurmaları gerekir. SFP'ler yüksek hızlı aktarımlara olanak sağlayan kompakt optik modüler alıcı-vericilerdir.

Donanım kurulduğunda özellik etkinleşir: Bağlantı noktası için herhangi bir yapılandırma gerekmez. 9160 G2 yazılımı başlangıçta SFP modülünü otomatik olarak algılar ve standart 10/100BaseT bağlantı noktasının yerine onu kullanır.

Modül parmakla baskı yapılarak önce elektrik arabirimine takılır. SFP modülü cihaz açıkken çıkarılıp takılmayı desteklemez. Modülü yalnızca 9160 G2 kapalıyken çıkarıp takın.

9160 G2, başlarken SFP modülünün kurulu olup olmadığına bağlı olarak seri konsol bağlantı noktasındaki aşağıdaki iki mesajdan birini sunar:

ixp425_eth: 100BASE-FX SFP fiber modül algılandı

ixp425_eth: 100BASE-FX SFP fiber modül algılanmadı

9160 G2, fiber optik arabirimi kullanırken yalnızca 100 Mb/sn'de çalışmayı destekler.

9160 G2, hangi Ethernet bağlantı noktasının kullanıldığı fark etmeksizin aynı kablolu MAC adresini kullanır.

İki Ethernet bağlantı noktasının aynı anda kullanılması desteklenmez. PoE (10/100BaseT bağlantı noktası aracılığıyla) ve fiber optik arabirimin kullanılması desteklenir. Bu yapılandırmada, 10/100BaseT bağlantı noktası yalnızca güç için kullanılır.

2.2.4 Durum Göstergeleri (LED'ler)

Yüksek performanslı 9160 G2'nin muhafazasının ön kısmında, Şekil 2.2, sayfa 21'de gösterildiği gibi altı durum göstergesi vardır. Birimin ön kısmındaki numaralı ve renkli LED'ler her bağlantı noktasının çalışma durumunu gösterir (bkz. Tablo 2.1, sayfa 23).

Tablo 2.1 9160 G2 LED İşlevleri: Ön Muhafaza

LED numarası	Ad	İşlev	Renk
1	Ethernet bağlantısı	10BaseT/100BaseT için bağlantı göstergesi: ON (Açık) = iyi bağlantı; OFF (Kapalı) = bağlantı yok	sarı *
2	Ethernet etkinliği	Ethernet LAN etkinliği (Rx/Tx)	yeşil
3	1. 802.11 telsiz durumu	1. 802.11 telsiz etkinliği (Rx/Tx)	yeşil
4	2. 802.11 telsiz durumu	2. 802.11 telsiz etkinliği (Rx/Tx)	yeşil
5	NB telsiz durumu	NB telsiz etkinliği (Rx/Tx)	yeşil
6	Güç	LED Sabit Açık = Birim çalışıyor LED Kapalı = Birim çalışmıyor	yeşil

* LED 1 rengi belirli bir uzaklıktan bakıldığında LED'lerin yönünü gösterir.

2.2.5 Video Ekranı Terminaline Bağlanma

ANSI uyumlu bir video ekranı terminali (örn., DEC VT220 ya da üstü) ya da bilgisayar ile çalışan terminal emülasyonu tanılama amaçlı kullanılır.

Terminal, 9160 G2'deki RS-232 bağlantı noktasına bağlanır (bkz. Şekil 2.2.2, sayfa 21). Bu bağlantı noktası normalde 115.200 baud, 8 bit, 1 dur biti, 0 eşlikte çalışmaya ayarlanır. B Sınıfı bilgisayar cihazlarına yönelik FCC kuralları Bölüm 15 ile uyumluluk için cihaz yalnızca birlikte verilen kabloyla (P/N 19387) kullanılmalıdır.

2.3 Yapılandırmayı Web Tarayıcıyla Değiştirme

9160 G2 Flash belleği, MS Internet Explorer (4.0 ya da üstü) veya Firefox gibi standart bir HTML Web Tarayıcı kullanılarak ağ aracılığıyla uzaktan yeniden yapılandırılabilir. Parametreleri değiştirme ve genel yapılandırma ayarlarıyla ilgili talimatlar için bkz. Bölüm 4: “Kurulum ve Başlatma İçin Hızlı Adımlar”.

BAŞLATMA ÖNCESİ KONTROL LİSTESİ

3

3.1 9160 G2 Kablosuz Ağ Geçidi	27
3.1.1 9160 G2 Kablosuz Ağ Geçidi'nin Varsayılan Ayarları	27
3.1.2 Erişim Noktasının Sağlamadığı Şeyler.	30
3.2 Yönetici Bilgisayarı	30
3.3 Kablosuz İstemci Bilgisayarları	32
3.4 9160 G2 Kablosuz Ağ Geçidi Üzerinde Dinamik ve Statik IP Adreslemeyi Anlama . . .	32
3.4.1 Erişim Noktası, Başlangıçta Nasıl IP Adresi Alır?.	33
3.4.2 Dinamik IP Adresleme	33
3.4.3 Statik IP Adresleme	33
3.4.4 IP Adresi Kurtarma.	34

Yeni bir **Erişim Noktası** bağlayıp başlatmadan önce gerekli donanım bileşenlerini, yazılımları, istemci yapılandırmalarını ve uyumluluk sorunlarını hızlıca kontrol etmek için aşağıdaki bölümleri inceleyin. Yeni (ya da genişletilmiş) kablosuz ağınıza başarılı bir şekilde başlatmak ve test etmek için ihtiyaç duyduğunuz her şeyin hazır olduğundan emin olun.

3.1 9160 G2 Kablosuz Ağ Geçidi

9160 G2 Kablosuz Ağ Geçidi, ağındaki cihazlar için kullanılan bir kablosuz iletişim hub'ıdır. **IEEE 802.11a, 802.11b, 802.11g** ve **802.11a Turbo** modlarında, kablosuz ve Ethernet cihazlarınız arasında sürekli ve yüksek hızlı erişim sağlar.

9160 G2 Kablosuz Ağ Geçidi, Sanal LAN'ları kullanarak kablosuz ağa kontrollü konuk erişimi için erişim noktalarını yapılandırmanızı sağlayan, kullanıma hazır *Guest Interface* (Konuk Arabirimi) özelliğini sunar.

Konuk Arabirimi hakkında daha fazla bilgi için bkz. Bölüm 14: “Konuk Erişimİni Ayarlama” ve “Konuk Ağı İçin Bağlantı Kurma Hakkında”, sayfa 40.

3.1.1 9160 G2 Kablosuz Ağ Geçidi'nin Varsayılan Ayarları

Tablo 3.1 9160 G2'nin Varsayılan Ayarları

Seçenek	Varsayılan Ayarlar	İlgili Bilgiler
<i>System Name</i> (Sistem Adı)	PTX9160-Wireless-AP	“Ethernet (Kablolu) Arabirimi”, sayfa 135, “DNS Ana Bilgisayar Adı”, sayfa 138 bölümü.
<i>User Name</i> (Kullanıcı Adı)	admin Kullanıcı adı salt okunurdur. Değiştirilemez.	
<i>Password</i> (Şifre)	admin	“Temel Ayarları Yapılandırma”, sayfa 45, “Ağ Ayarlarını Sağlama”, sayfa 49 bölümü.

Tablo 3.1 9160 G2'nin Varsayılan Ayarları (Devamı)

Seçenek	Varsayılan Ayarlar	İlgili Bilgiler
<i>Network Name (Ağ Adı) (SSID)</i>	Dahili Arabirim için "TEKLOGIX" Konuk Arabirimi için "TEKLOGIX Guest"	"Temel Ayarları Yapılandırma", sayfa 45, "Erişim Noktasını İnceleme / Açıklama", sayfa 48 bölümü. "Kablosuz Arabiriminin Ayarlama", sayfa 145, "Dahili" Kablosuz LAN Ayarlarını Yapılandırma", sayfa 150 bölümü. "Kablosuz Arabiriminin Ayarlama", sayfa 145, "Konuk" Ağ Kablosuz Ayarlarını Yapılandırma", sayfa 151 bölümü.
<i>Network Time Protocol (Ağ Zaman Protokolü) (NTP)</i>	None (Yok)	"Ağ Zaman Protokolü Sunucusu", sayfa 309
<i>IP Address (IP Adresi)</i>	192.168.1.10 <i>Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)</i> sunucusu kullanmıyorsanız varsayılan IP adresi kullanılır. Yönetim Web sayfalarından yeni bir statik IP adresi atayabilirsiniz. Ağınızda bir DHCP sunucusu varsa IP adresi AP başlangıcı sırasında sunucu tarafından dinamik olarak atanır.	"9160 G2 Kablosuz Ağ Geçidi Üzerinde Dinamik ve Statik IP Adreslemeyi Anlama", sayfa 32
<i>Connection Type (Bağlantı Türü)</i>	<i>Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)</i> Dahili ağınızda bir DHCP sunucusu yoksa ve kullanmayı da düşünmüyorsanız erişim noktasını başlattıktan sonra yapmanız gereken ilk şey, Bağlantı Türünü "DHCP"den "Static IP"ye dönüştürmektir. Konuk ağın DHCP sunucusu olması gereklidir.	"9160 G2 Kablosuz Ağ Geçidi Üzerinde Dinamik ve Statik IP Adreslemeyi Anlama", sayfa 32 Bağlantı Türünü yeniden yapılandırma hakkında bilgi için bkz. "Dahili Arabirim Ayarları", sayfa 141.
<i>Subnet Mask (Alt Ağ Maskesi)</i>	None (Yok) Bu ayar, ağ kurulumunuz ve DHCP sunucu yapılandırmanız tarafından belirlenir.	"Ethernet (Kablolu) Arabirimi", sayfa 135

Tablo 3.1 9160 G2'nin Varsayılan Ayarları (Devamı)

Seçenek	Varsayılan Ayarlar	İlgili Bilgiler
<i>Radio (Telsiz)</i>	On (Açık)	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>IEEE 802.11 Mode (IEEE 802.11 Modu)</i>	802.11g ya da 802.11a+g	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>802.11g Channel (802.11g Kanalı)</i>	Auto (Otomatik)	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>Beacon Interval (Uyarı Aralığı)</i>	100	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>DTIM Period (DTIM Süreci)</i>	2	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>Fragmentation Threshold (Bölme Eşiği)</i>	2346	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>Regulatory Domain (Düzenleyici Etki Alanı)</i>	FCC	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>RTS Threshold (RTS Eşiği)</i>	2347	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>MAX Stations (Maksimum İstasyon Sayısı)</i>	2007	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>Transmit Power (Aktarım Gücü)</i>	%100	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>Rate Sets Supported (Mbps) (Desteklenen Hız Grupları [Mb/sn])</i>	<ul style="list-style-type: none">• IEEE 802.1a: 54; 48; 36; 24; 18; 12; 9; 6• IEEE 802.1g: 54; 48; 36; 24; 18; 12; 11; 9; 6; 5,5; 2; 1• IEEE 802.1b: 11; 5,5; 2; 1	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165
<i>Rate Sets (Mbps) (Hız Grupları [Mb/sn]) (Basic/Advertised) (Temel/Bildirilen)</i>	<ul style="list-style-type: none">• IEEE 802.1a: 24; 12; 6• IEEE 802.1g: 11; 5,5; 2; 1• IEEE 802.1b: 2; 1	"802.11 Telsiz Ayarlarını Yapılandırma", sayfa 165

Tablo 3.1 9160 G2'nin Varsayılan Ayarları (Devamı)

Seçenek	Varsayılan Ayarlar	İlgili Bilgiler
<i>Broadcast SSID</i> (SSID Yayını)	Allow (İzin Ver)	"Güvenlik Ayarlarını Yapılandırma", sayfa 100.
<i>Security Mode</i> (Güvenlik Modu)	None (plain-text) (Yok [düz metin])	"Güvenlik Ayarlarını Yapılandırma", sayfa 100.
<i>Authentication Type</i> (Kimlik Doğrulama Türü)	None (Yok)	
<i>MAC Filtering</i> (MAC Filtreleme)	Allow any station unless in list (Listede olmayan istasyonlara izin ver)	"MAC Adresİ Filtreleme", sayfa 175
<i>Guest Login and Management</i> (Konuk Olarak Oturum Açma ve Yönetim)	Disabled (Devre Dışı)	"Konuk Erişimini Ayarlama", sayfa 153
<i>Load Balancing</i> (Yük Dengeleme)	Disabled (Devre Dışı)	"Yük Dengeleme", sayfa 179
<i>WDS Settings</i> (WDS Ayarları)	None (Yok)	"Kablosuz Dağıtım Sistemi", sayfa 201

3.1.2 Erişim Noktasının Sağlamadığı Şeyler

9160 G2 Kablosuz Ağ Geçidi, Internet'e yönelik bir **Ağ Geçidi** olarak tasarlanmamıştır. Kablosuz LAN'ınızı (**WLAN**) diğer **LAN**'lara ya da Internet'e bağlamak için bir ağ geçidi cihazı gereklidir.

3.2 Yönetici Bilgisayarı

9160 G2 Kablosuz Ağ Geçidi cihazının yapılandırılması ve yönetilmesi web tabanlı bir kullanıcı arabirimi (UI) aracılığıyla gerçekleşir. Tablo 3.2, yönetici bilgisayarının minimum gereksinimlerini açıklamaktadır.

Tablo 3.2 Gerekli AP Yöneticisi Yazılımı ve Donanımı

Gerekli Bileşenler	Açıklama
<i>İlk Erişim Noktasına Ethernet Bağlantısı</i>	<p>İlk erişim noktasını yapılandırmak için kullanılan bilgisayarın bir Ethernet kabloyla erişim noktasına (doğrudan ya da hub aracılığıyla) bağlı olması gerekir.</p> <p>Daha fazla bilgi için bkz. "Erişim Noktasını Ağa ve Güce Bağlama", sayfa 38, "Kurulum ve Başlatma İçin Hızlı Adımlar".</p>
<i>Ağa Kablosuz Bağlantı</i>	<p>Yeni kablosuz ağındaki ilk erişim noktasını ilk kez yapılandırdıktan ve başlattıktan sonra ileriki yapılandırma değişikliklerini "Dahili" ağa kablosuz bağlanarak Yönetici web sayfalarından yapabilirsiniz. Erişim noktasına kablosuz bağlanmak için yönetici cihazınızın şu kablosuz istemcilerinkine benzer Wi-Fi özelliklerinin olması gerekir:</p> <ul style="list-style-type: none">Erişim noktasını çalıştırmayı düşündüğünüz IEEE 802.11 modlarından birini ya da birkaçını destekleyen taşınabilir ya da dahili Wi-Fi istemci adaptörü. (IEEE 802.11a, 802.11b802.11a, 802.11g802.11b, 802.11a Turbo802.11g 802.11a Turbo modları desteklenir.)9160 G2 Kablosuz Ağ Geçidi ile ilişkilendirilmek üzere yapılandırılmış Microsoft® Windows® XP ya da Funk Odyssey gibi kablosuz istemci yazılımları. <p>Wi-Fi istemci kurulumuyla ilgili ayrıntılar için bkz. "Kablosuz İstemci Bilgisayarları", sayfa 32.</p>
<i>Web Tarayıcı / İşletim Sistemi</i>	<p>9160 G2 Kablosuz Ağ Geçidi cihazının yapılandırılması ve yönetimi, erişim noktasında bulunan bir web tabanlı kullanıcı arabirimi tarafından sağlanır. Erişim noktası Yönetim Web sayfalarına erişmek için aşağıdaki yer alan desteklenen web tarayıcılardan birini kullanmanızı öneririz:</p> <ul style="list-style-type: none">Microsoft Windows XP ya da Microsoft Windows 2000 işletim sistemlerinde Microsoft Internet Explorer sürüm 5.5 ya da 6.x (iki ana sürüm için de güncel düzeltme eki seviyesiyle birlikte)Redhat Linux sürüm 2.4 işletim sisteminde Netscape® Mozilla 1.7.x <p>Yönetim Web tarayıcısının yönetim arabirimindeki interaktif özellikleri desteklemesi için JavaScript'in etkinleştirilmesi gerekir. Ayrıca, ürün yazılımı yükseltme özelliğinin kullanılabilmesi için HTTP yüklemelerini desteklemesi gerekir.</p>
<i>Güvenlik Ayarları</i>	<p>Erişim noktasını yapılandırmak için kullanılan kablosuz istemcide güvenliğin devre dışı olması gerekir.</p>

3.3 Kablosuz İstemci Bilgisayarları

9160 G2 Kablosuz Ağ Geçidi, erişim noktasının çalıştığı 802.11 modu için uygun şekilde yapılandırılan Wi-Fi istemci adaptörüne sahip tüm istemcilere kablosuz erişim sağlar.

Birden çok istemcili işletim sistemleri desteklenir. İstemci; bir dizüstü bilgisayar, masaüstü bilgisayar, avuçiçi bilgisayar (PDA) veya Wi-Fi adaptörü ve desteklenen sürücülere sahip elde kullanılan, taşınabilir ya da sabit herhangi bir cihaz olabilir.

Erişim noktasına bağlanmak için kablosuz istemcilerin Tablo 3.3'te belirtilen yazılım ve donanımlara sahip olması gerekir.

Tablo 3.3 Gerekli AP İstemci Yazılımı ve Donanımı

Gerekli Bileşenler	Açıklama
<i>Wi-Fi İstemci Adaptörü</i>	<p>Erişim noktasını çalıştırmayı düşündüğünüz IEEE 802.11 modlarından birini ya da birkaçını destekleyen taşınabilir ya da dahili Wi-Fi istemci adaptörü. (IEEE 802.11a, 802.11b ve 802.11g desteklenir.)</p> <p>Wi-Fi istemci adaptörlerinin son derece farklı çeşitleri vardır. Adaptör, istemci cihazına takılan bir bilgisayar kartı; taşınabilir PCMCIA ya da PCI kartı (NIC türleri) veya bir kablo aracılığıyla istemciye bağladığınız USB ve Ethernet adaptörü gibi harici bir cihaz olabilir.</p> <p>Erişim noktası 802.11a/b/g modlarını destekler ancak hangi modu kullanacağınıza büyük olasılıkla ağ tasarlama aşamasında karar verirsiniz. Erişim noktalarınızın yapılandırıldığı 802.11 moduyla eşleşen yapılandırılmış adaptörlere sahip olmak, istemciler için başlıca gerekliliktir.</p>
<i>Kablosuz İstemci Yazılımı</i>	<p>9160 G2 Kablosuz Ağ Geçidi ile ilişkilendirilmek üzere yapılandırılmış Microsoft Windows Supplciant ya da Funk Odyssey gibi istemci yazılımları.</p>
<i>İstemci Güvenlik Ayarları</i>	<p>Erişim noktasını yapılandırmak için kullanılan istemcide güvenliğin devre dışı olması gerekir.</p> <p>Erişim noktasındaki Güvenlik modu düz metinden başka bir şeye ayarlanmışsa kablosuz istemcinin erişim noktası tarafından kullanılan kimlik doğrulama modu için bir profil ayarlaması ve geçerli bir kullanıcı adı, şifre, sertifika ya da benzer kullanıcı kimliği kanıtları sağlaması gerekir. Güvenlik modları şunlardır: Statik WEP, IEEE 802.11, RADIUS sunuculu WPA ve WPA2PSK.</p> <p>Erişim noktasında güvenliği yapılandırma hakkında bilgi için bkz. "Güvenliği Yapılandırma", sayfa 91.</p>

3.4 9160 G2 Kablosuz Ağ Geçidi Üzerinde Dinamik ve Statik IP Adreslemeyi Anlama

9160 G2 Kablosuz Ağ Geçidi cihazları, ilk erişim noktası için çok az kurulum işlemi gerektirecek; önceden yapılandırılmış bir *küme*ye art arda katılan ek erişim noktaları içinse herhangi bir yapılandırma gerektirmeyecek şekilde otomatik olarak yapılandırılmak üzere tasarlanmıştır.

3.4.1 Erişim Noktası, Başlangıçta Nasıl IP Adresi Alır?

Bir erişim noktası oluşturduğunuzda ilk önce bir ağ **DHCP** sunucusu arar. Bulduğunda, DHCP sunucusundan bir **IP Address (IP Adresi)** alır. Ağda herhangi bir DHCP sunucusu bulunmazsa siz yeni bir statik IP adresi atayana kadar (ve bir statik IP adresleme politikası belirleyene kadar) veya bir DHCP sunucusu çevrimiçi olana kadar AP, varsayılan **Statik IP Adresini** (192.168.1.10) kullanmaya devam eder.



Notlar: Hem Dahili hem de Konuk ağı yapılandırdıysanız ve ikisi için de dinamik adresleme politikası kullanmayı planlıyorsanız her ağda ayrı bir DHCP sunucusunun çalışması gerekir.

DHCP sunucusu Konuk ağı için zorunlu bir gerekliliktir.

3.4.2 Dinamik IP Adresleme

9160 G2 Kablosuz Ağ Geçidi cihazı, AP'nin oluşturulduğu ağda genellikle bir **DHCP** sunucusunun çalışmasını bekler. Çoğu ev ve küçük işletme ağı, bir ağ geçidi cihazı ya da merkezi sunucu aracılığıyla sağlanan DHCP hizmeti içerir. Ancak Dahili ağda herhangi bir DHCP sunucusu yoksa AP, ilk kez başlatıldığında varsayılan **Statik IP Adresini** kullanır.

Benzer şekilde, kablosuz istemciler ve yazıcı gibi diğer ağ cihazları, ağda bir DHCP sunucusu varsa IP adreslerini bu sunucudan alır. Ağda herhangi bir DHCP sunucusu yoksa kablosuz istemcinize ve diğer ağ cihazlarınıza manuel olarak statik IP adresi atamanız gerekir.

Konuk ağın DHCP sunucusu olması gereklidir.

3.4.3 Statik IP Adresleme

9160 G2 Kablosuz Ağ Geçidi cihazı şu varsayılan **Statik IP Adresi** ile birlikte gelir: 192.168.1.10. (Bkz. “9160 G2 Kablosuz Ağ Geçidi'nin Varsayılan Ayarları”, sayfa 27.) Ağda herhangi bir **DHCP** sunucusu bulunmazsa AP, ilk kez başlatıldığında bu statik IP adresini kullanır.

AP'yi başlattıktan sonra, erişim noktası Yönetim Web sayfalarını kullanarak 9160 G2 Kablosuz Ağ Geçidi cihazlarınızda statik IP adresleme politikası belirleyebilir ve Dahili ağdaki AP'lere statik IP adresleri atayabilirsiniz. ("Bağlantı Türü" alanı ve ilgili alanlar hakkındaki bilgilere bakın ["Dahili Arabirim Ayarları", sayfa 141]).



Önemli: *Dahili ağınızda bir DHCP sunucusu yoksa ve kullanmayı da düşünmüyorsanız erişim noktasını başlattıktan sonra yapmanız gereken ilk şey, Bağlantı Türünü "DHCP"den "Static IP"ye dönüştürmektir. AP'ye yeni bir Statik IP adresi atayabilir ya da varsayılan adresi kullanmaya devam edebilirsiniz. Yeni bir Statik IP adresi atamanızı öneririz. Böylece, ileride aynı ağa başka bir 9160 G2 Kablosuz Ağ Geçidi eklerseniz her AP'nin IP adresi farklı olur.*

3.4.4 IP Adresi Kurtarma

Erişim noktasıyla ilgili iletişim sorunları yaşıyorsanız AP yapılandırmasını fabrika ayarlarına sıfırlayarak **Statik IP Adresini** kurtarabilir (bkz. “Fabrika Varsayılanları Yapılandırmasına Sıfırlama” , sayfa 316) ya da AP'yi, **DHCP** içeren bir ağa bağlayarak dinamik olarak atanan bir adres alabilirsiniz.

KURULUM VE BAŞLATMA İÇİN HIZLI ADIMLAR

4

4.1 9160 G2 Kablosuz Ağ Geçidinin Kutusundan Çıkarılması	37
4.1.1 9160 G2 Kablosuz Ağ Geçidi Donanım ve Bağlantı Noktaları	37
4.1.2 9160 G2 Kablosuz Ağ Geçidi'nin İçindekiler	37
4.2 Erişim Noktasını Ağa ve Güce Bağlama	38
4.2.1 Konuk Ağı İçin Bağlantı Kurma Hakkında	40
4.2.1.1 Konuk VLAN İçin Donanım Bağlantıları	40
4.3 Erişim Noktasındaki Güç	40
4.4 Yönetim Web Sayfalarında Oturum Açma	40
4.4.1 Erişim Noktalarının Temel Ayarlarını Görüntüleme	41
4.5 "Temel Ayarları" Yapılandırma ve Kablosuz Ağı Başlatma	42
4.5.1 Varsayılan Yapılandırma	42
4.6 Sırada Ne Var?	42
4.6.1 Erişim Noktasının LAN'a Bağlı Olduğundan Emin Olma	42
4.6.2 Kablosuz İstemcilerle LAN Bağlantısını Test Etme	43
4.6.3 Gelişmiş Ayarları Kullanarak Erişim Noktasını Güvenli Hale Getirme ve İnce Ayar Yapma	43

Bir veya daha fazla 9160 G2 Kablosuz Ağ Geçidi cihazını kurmak ve kullanmaya başlamak aslında bir *kablosuz ağ* oluşturmak ve başlatmaktır. *Basic Settings* (Temel Ayarlar) Yönetim Web sayfası bu süreci kolaylaştırır. Burada 9160 G2 Kablosuz Ağ Geçidi cihazlarınızı ve sonrasında kablosuz ağını kurmak için adım adım talimatları içeren bir kılavuz bulunmaktadır. Henüz yapmadıysanız Bölüm 3: “Başlatma Öncesi Kontrol Listesi” hakkında bilgi edinin.

Bu bölümde şu konular anlatılır:

- 1. Adım: **9160 G2 Kablosuz Ağ Geçidinin Kutusundan Çıkarılması.**
- 2. Adım: **Erişim Noktasını Ağa ve Güce Bağlama.**
- 3. Adım: **Erişim Noktasındaki Güç.**
- 5. Adım: **Yönetim Web Sayfalarında Oturum Açma.**
- 6. Adım: **"Temel Ayarları" Yapılandırma ve Kablosuz Ağı Başlatma.**
- **Sırada Ne Var?**

4.1 9160 G2 Kablosuz Ağ Geçidinin Kutusundan Çıkarılması

9160 G2 Kablosuz Ağ Geçidini kutusundan çıkarın ve donanım bağlantı noktalarını, ilişkili kabloları ve aksesuarları inceleyin.

4.1.1 9160 G2 Kablosuz Ağ Geçidi Donanım ve Bağlantı Noktaları

9160 G2 Kablosuz Ağ Geçidi şunları içerir:

- Yerel Alan Ağına (LAN) Ethernet ağ kablosuyla bağlanmak için Ethernet bağlantı noktası.
- Güç bağlantı noktası ve güç adaptörü.
- Gücü açma/kapatma anahtarı.
- Ürünün hangi modelini edindiğinize bağlı olarak bir ya da iki adet telsiz.

4.1.2 9160 G2 Kablosuz Ağ Geçidi'nin İçindekiler

Bir **Erişim Noktası** (AP) olan 9160 G2 Kablosuz Ağ Geçidi, kablosuz hub olarak kullanılmak üzere tasarlanmış tek amaçlı bir bilgisayardır. Erişim noktasının içinde bir Wi-Fi telsiz sistemi ve mikro işlemci vardır. Erişim noktası, “9160 G2 Kablosuz Ağ Geçidi’ne Genel Bakış”, sayfa 7 bölümünde özetlenen yapılandırılabilir çalışma süresi özelliklerine sahip ürün yazılımı kullanılarak FlashROM’dan başlatılır.

Yeni özellikler ve geliştirmeler çıktıkça kablosuz ağını oluşturarak erişim noktalarına yeni özellikler ve performans iyileştirmeleri eklemek için ürün yazılımını yükseltebilirsiniz. (Bkz. “Ürün Yazılımını Yükseltme”, sayfa 317.)

4.2 Erişim Noktasını Ağa ve Güce Bağlama

Sonraki adım ağı ve güç bağlantılarını kurmaktır.

1. Erişim noktası ve bilgisayar arasında bir Ethernet bağlantısı oluşturmak için aşağıdakilerden birini yapın:

Ethernet kablosunun bir ucunu erişim noktasındaki ağ bağlantı noktasına, diğer ucunu da bilgisayarınızın bağlı olduğu hub'a bağlayın. (Bkz. Şekil 4.2, sayfa 39.)

Veya

Çapraz¹ kablunun bir ucunu erişim noktasındaki ağ bağlantı noktasına, diğer ucunu da bilgisayarınızdaki Ethernet bağlantı noktasına bağlayın. (Bkz. Şekil 2, sayfa 39.)



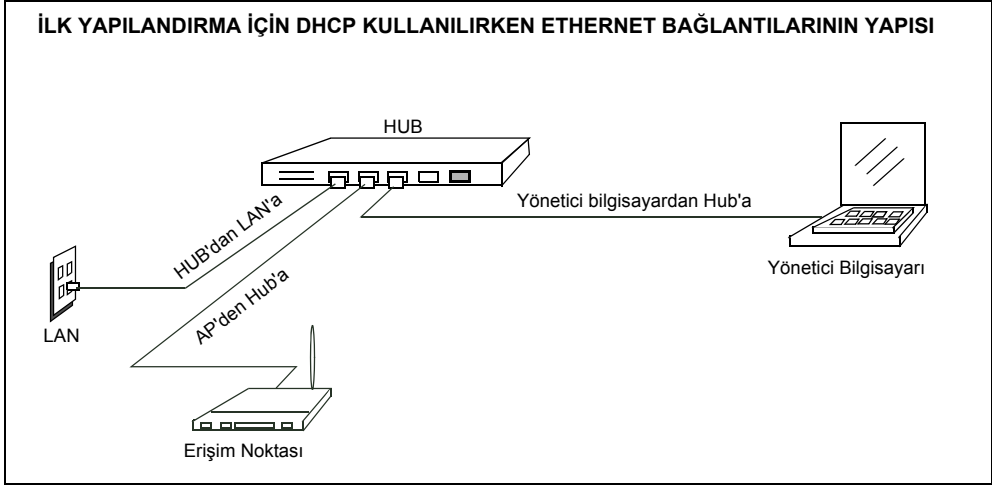
Notlar: Hub kullanıyorsanız cihazınızın erişim noktasından ağdaki diğer tüm cihazlara giden yayın sinyallerine izin vermesi gerekir. Standart bir hub kullanabilirsiniz. Ancak bazı anahtarlar yönlendirilen ya da alt ağ yayınlarına izin vermez. Yönlendirilen yayınlara izin vermek için anahtarı yapılandırmanız gerekebilir.

Doğrudan bir Ethernet bağlantısını ve DHCP olmayan bir sunucuyu ilk kez yapılandırırken bilgisayarınızı erişim noktasındaki varsayılan IP adresiyle aynı alt ağda bulunan statik bir IP'ye ayarladığınızdan emin olun. (Erişim noktasının varsayılan IP adresi şudur: 192.168.1.10.)

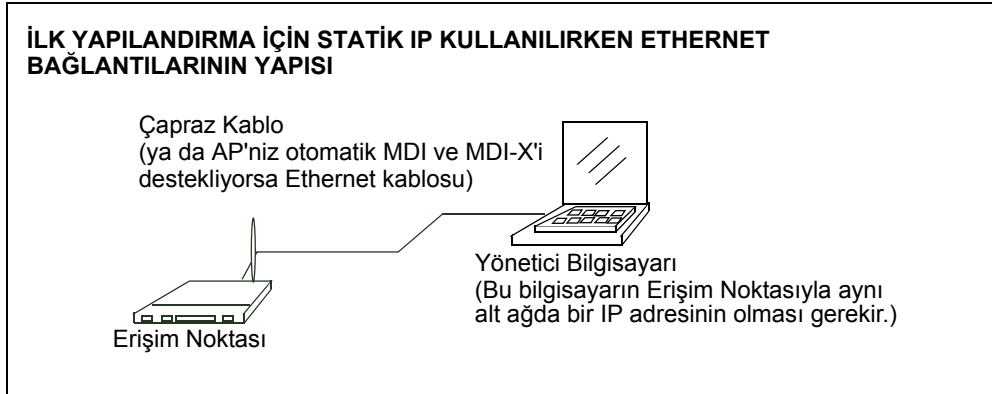
İlk yapılandırmada erişim noktası ile bilgisayar arasında çapraz kablo aracılığıyla doğrudan Ethernet (kablolu) bağlantısı kurduysanız erişim noktasının sonraki başlatması ve kullanımları için kablo sistemini yeniden yapılandırmanız gerekecektir. Böylece erişim noktası doğrudan bilgisayara değil (Şekil 4.2'de gösterildiği gibi hub ile ya da doğrudan) LAN'a bağlanacaktır.

¹Erişim noktası donanımı **MDI** ve **MDI-X** otomatik işlevlerini destekliyorsa bilgisayardan AP'ye doğrudan bağlantı için standart bir Ethernet kablosu kullanabilirsiniz. Çapraz kablo da kullanabilirsiniz ancak cihazınızda MDI ve MDI-X otomatik algılama bağlantı noktaları varsa çapraz kabloya gerek yoktur.

Şekil 4.1 DHCP Kullanılırken Ethernet Bağlantılarının Yapısı



Şekil 4.2 Statik IP Kullanılırken Ethernet Bağlantılarının Yapısı



2. Güç adaptörünü erişim noktasının arka kısmındaki güç bağlantı noktasına bağlayın ve güç kablosunun diğer ucunu prize (tercihen bir gerilim koruyucu ile) takın.

4.2.1 Konuk Ağı İçin Bağlantı Kurma Hakkında

9160 G2 Kablosuz Ağ Geçidi, ağa kontrollü konuk erişimi sağlamak için bir erişim noktası yapılandırmanıza olanak sağlayan kullanıma hazır bir Konuk Arabirimi sunar. Aynı erişim noktası, iki farklı kablosuz ağ (güvenli bir "Dahili" LAN ve herkese açık "Konuk" ağı) arasında köprü görevi görebilir. Bunu, Yönetim Kullanıcı Arabirimi aracılığıyla iki farklı Sanal LAN tanımlayarak yapabilirsiniz.

Yönetim Kullanıcı Arabiriminde Konuk arabirimi ayarlarını yapılandırma hakkında bilgi için bkz. Bölüm 14: “Konuk Erişimİni Ayarlama”.

4.2.1.1 Konuk VLAN İçin Donanım Bağlantıları

VLAN'lar kullanarak bir konuk ağı yapılandırmak istiyorsanız şunları yapın:

- Erişim noktasındaki bir ağ bağlantı noktasını VLAN ile uyumlu bir anahtara bağlayın.
- Bu anahtarda VLAN'lar tanımlayın.

4.3 Erişim Noktasındaki Güç

9160 G2 Kablosuz Ağ Geçidi cihazı fişe taktığınızda çalışmaya başlar.

4.4 Yönetim Web Sayfalarında Oturum Açma

9160 G2 Kablosuz Ağ Geçidi Yönetim Web sayfalarının IP adresine gittiğinizde sizden bir kullanıcı adı ve şifre girmeniz istenir.



Varsayılan kullanıcı adı ve şifre bilgileri şöyledir:

Tablo 4.1 Kullanıcı adı ve Şifre

Alan	Varsayılan Ayar
User name (Kullanıcı adı)	admin
Password (Şifre)	admin (Kullanıcı adı salt okunurdur, değiştirilemez.)

Kullanıcı adını ve şifreyi girdikten sonra **OK** (Tamam) seçeneğine tıklayın.

4.4.1 Erişim Noktalarının Temel Ayarlarını Görüntüleme

İlk kez oturum açtığınızda, 9160 G2 Kablosuz Ağ Geçidi yönetimi *Basic Settings* (Temel Ayarlar) sayfası görüntülenir. Bu ayarlar, erişim noktası kümesindeki tüm erişim noktaları ve otomatik yapılandırma ayarlandıysa kümeye daha sonra eklenen yeni erişim noktaları için geçerli olan global ayarlardır.

Şekil 4.3 Erişim Noktası Temel Ayarları

4.5 "Temel Ayarları" Yapılandırma ve Kablosuz Ağ Başlatma

Kablosuz ağınız için temel ayarlar tanımlayarak minimum yapılandırma bilgileri sağlayın. Bu ayarlar, Yönetim Web arabiriminin *Basic Settings* (Temel Ayarlar) sayfasında bulunur ve web sayfasında 1-3 adımlarına ayrılır.

Bu "Temel Ayarlar" ve uygun biçimde yapılandırılmaları hakkında ayrıntılı açıklamalar için bkz. Bölüm 5: "Temel Ayarları Yapılandırma". Bahsi geçen adımlar aşağıda özetlenmiştir:

1. Review Description of this Access Point (Bu Erişim Noktasının Açıklamasını İnceleyin).
IP adreslemeyle ilgili bilgiler sunar. Daha fazla bilgi için bkz. "Erişim Noktasını İnceleme / Açıklama", sayfa 48.
2. Provide Network Settings (Ağ Ayarlarını Sağlayın).
Kümelenen erişim noktaları için yeni bir yönetici şifresi sağlayın. Daha fazla bilgi için bkz. "Ağ Ayarlarını Sağlama", sayfa 49.
3. Settings (Ayarlar).
Kablosuz ağ bu yeni ayarlarla etkinleştirmek için **Update** (Güncelle) düğmesine basın. Daha fazla bilgi için bkz. "Temel Ayarları Güncelleme", sayfa 50.

4.5.1 Varsayılan Yapılandırma

Yukarıdaki adımları izleyip tüm varsayılanları kabul ettiğinizde erişim noktası "9160 G2 Kablosuz Ağ Geçidi'nin Varsayılan Ayarları", sayfa 27'de açıklanan varsayılan yapılandırmaya sahip olur.

4.6 Sırada Ne Var?

Bu adımın ardından erişim noktasının LAN'a bağlı olduğundan emin olun, birkaç kablosuz istemci ekleyin ve istemcileri ağa bağlayın. Kablosuz ağınızın temel noktalarını test ettikten sonra erişim noktasındaki gelişmiş yapılandırma özelliklerini değiştirerek daha fazla güvenlik ve ince ayar sağlayabilirsiniz.

4.6.1 Erişim Noktasının LAN'a Bağlı Olduğundan Emin Olma

Erişim noktasını ve yönetici bilgisayarını ağ hub'ına bağlayarak yapılandırdıysanız erişim noktanız zaten LAN'a bağlı demektir. Yapmanız gereken başka bir şey yoktur. Sonraki adım, birkaç kablosuz istemciyi test etmektir.

Erişim noktasını çapraz bir kablo aracılığıyla bilgisayarınızla erişim noktasını bağlayan doğrudan kablolu bir bağlantı kullanarak yapılandırdıysanız aşağıdakileri yapın:

1. Çapraz kabloyu bilgisayardan ve erişim noktasından çıkarın.
2. Erişim noktasından **LAN**'a standart bir Ethernet kablosu bağlayın.
3. Bilgisayarınızı Ethernet kablosu ya da kablosuz istemci kartı aracılığıyla LAN'a bağlayın.

4.6.2 Kablosuz İstemcilerle LAN Bağlantısını Test Etme

9160 G2 Kablosuz Ağ Geçidi cihazını birkaç kablosuz istemci cihazından algılamaya ve bu cihazlarla ilişkilendirmeye çalışarak test edin. (Bu istemcilerle ilgili gereksinimler hakkında bilgi için bkz. “Kablosuz İstemci Bilgisayarları”, sayfa 32, **Başlatma Öncesi Kontrol Listesi**.)

4.6.3 Gelişmiş Ayarları Kullanarak Erişim Noktasını Güvenli Hale Getirme ve İnce Ayar Yapma

Kablosuz ağınıza çalıştırdıktan ve erişim noktasını birkaç kablosuz istemciyle test ettikten sonra daha fazla güvenli katmanı ve kullanıcı ekleyebilir, bir Konuk arabirimi yapılandırabilir ve performans ayarlarında ince ayar yapabilirsiniz.

TEMEL AYARLARI YAPILANDIRMA

5

5.1 Temel Ayarlara Gitme	47
5.2 Eriřim Noktasını İnceleme / Açıklama.	48
5.3 Ağ Ayarlarını Sağlama	49
5.4 Temel Ayarları Güncelleme	50
5.5 Bağımsız Bir Eriřim Noktasının Temel Ayarları.	50
5.6 Bir Bakışta Ağınızı Tanıma: Gösterge Simgelerini Anlama	50

5.1 Temel Ayarlara Gitme

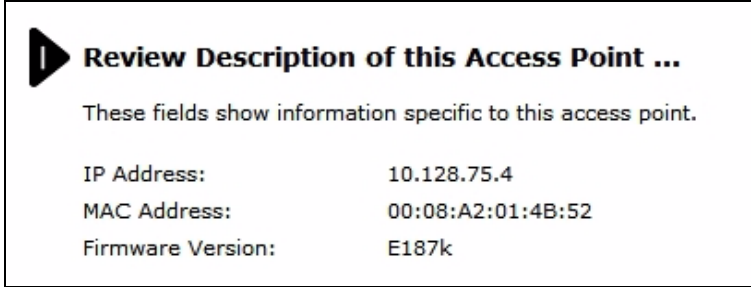
Başlangıç ayarlarını yapılandırmak için **Basic Settings** (Temel Ayarlar) seçeneğine tıklayın.

Erişim noktasının IP adresini tarayıcınıza yazdığınızda *Basic Settings* (Temel Ayarlar) sayfası görüntülenen varsayılan sayfadır.

Şekil 5.1 Temel Ayarlar

Basic Settings (Temel Ayarlar) sayfasındaki alanları; “Erişim Noktasını İnceleme / Açıklama”, sayfa 48’ de anlatıldığı gibi doldurun.

5.2 Erişim Noktasını İnceleme / Açıklama



Tablo 5.1 Temel Ayarlar Ekran Seçenekleri

Alan	Açıklama
<i>IP Address</i> (<i>IP Adresi</i>)	Bu erişim noktasına atanan IP adresini gösterir. IP adresi, halihazırda DHCP ya da "Guest Interface Settings (Konuk Arabirimi Ayarları)", sayfa 143'te açıklandığı gibi statik olarak Ethernet (kablolu) ayarları aracılığıyla atandığı için bu alan düzenlenebilir bir alan değildir.
<i>MAC Address</i> (<i>MAC Adresi</i>)	<p>Erişim noktasının MAC adresini gösterir.</p> <p>MAC adresi, bir arabirimi ağa tanıtan herhangi bir cihazın kalıcı ve benzersiz donanım adresidir. MAC adresi üretici tarafından atanır. MAC adresini değiştiremezsiniz. Arabirimin benzersiz bir tanımlayıcısı olduğu için burada bilgi amaçlı değiştirilmiştir.</p> <p>Burada görülen adres, köprüye (br0) ait MAC adresidir. AP, dışardaki diğer ağlar tarafından bu adresle bilinir.</p> <p>AP'deki Konuk ve Dahili arabirimlerinin MAC adreslerini görmek için <i>Status > Interfaces</i> (Durum > Arabirimler) sekmesine gidin.</p>
<i>Firmware Version</i> (<i>Ürün Yazılımı Sürümü</i>)	<p>Erişim noktasında yüklü olan ürün yazılımının sürümüyle ilgili bilgi verir.</p> <p>9160 G2 Kablosuz Ağ Geçidi cihazının yeni ürün yazılımı sürümleri çıktıkça yeni özelliklerden ve geliştirmelerden faydalanmak için erişim noktanızdaki ürün yazılımını yükseltebilirsiniz.</p> <p>Ürün yazılımını yükseltmeyle ilgili talimatlar için bkz. "Ürün Yazılımını Yükseltme", sayfa 317.</p>


5.3 Ağ Ayarlarını Sağlama

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster.

Current Password	<input type="password"/>
New Password	<input type="password" value="*****"/>
Confirm new password	<input type="password" value="*****"/>
Network Name (SSID)	<input type="text" value="Psion Teklogix"/>

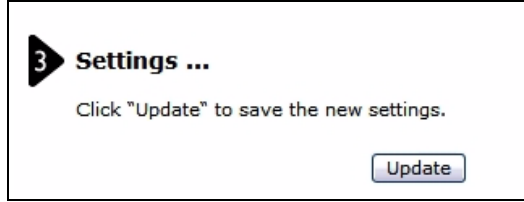
Tablo 5.2 Yönetici Şifresi ve Kablosuz Ağ

Alan	Açıklama
<i>Current Password</i> (Geçerli Şifre)	Geçerli yönetici şifresini girin. Geçerli şifreyi değiştirmeden önce doğru olarak girmeniz gerekir.
<i>New Password (Yeni Şifre)</i>	<p>Yeni bir yönetici şifresi girin. Şifrenizi girerken başkalarının görmesini engellemek için, girdiğiniz karakterler " * " karakterleri olarak görünecektir.</p> <p>Yönetici şifresi en fazla 8 karakterden oluşan alfanümerik bir dize olmalıdır. Özel karakterler ve boşluk kullanmayın.</p> <p> Kablosuz ağınıza korumanın ilk adımı olarak varsayılan yönetici şifrenizi değiştirmenizi öneririz.</p>
<i>Confirm New Password</i> (Yeni Şifreyi Doğrula)	Yeni şifreyi doğru girdiğinizi onaylamak için tekrar girin.
<i>Network Name (Ağ Adı)</i> (SSID)	<p>Kablosuz ağ için karakter dizesi olarak bir ad girin. Bu ad, bu ağdaki tüm erişim noktaları için geçerlidir. Daha fazla erişim noktası eklediğinizde erişim noktaları bu SSID'yi paylaşır.</p> <p><i>Hizmet Kümesi Tanımlayıcı (SSID)</i>, en fazla 32 karakterden oluşan alfanümerik bir dizedir.</p> <p>Not: Yönettiğiniz AP'ye kablosuz istemci olarak bağlanırsanız SSID'yi sınırlamanız AP bağlantısını yitirmenize yol açar. Bu yeni ayarı kaydettikten sonra yeni SSID'ye tekrar bağlanmanız gerekir.</p>



Not: 9160 G2 Kablosuz Ağ Geçidi, aynı anda birden fazla yapılandırma değişiklikleri için tasarlanmamıştır. Birden fazla erişim noktası içeren bir ağına varsa, Yönetim Web sayfalarında birden fazla yönetici oturum açmışsa ve yapılandırmada değişiklikler yapıyorsa kümedeki tüm erişim noktaları senkronize kalır ancak birden fazla kullanıcı tarafından belirtilen tüm yapılandırma değişikliklerinin uygulanması garanti edilmez.

5.4 Temel Ayarları Güncelleme



Yeni yapılandırmayı inceledikten sonra ayarları uygulamak ve erişim noktalarını kablosuz bir ağ olarak dağıtmak için **Update** (Güncelle) düğmesine tıklayın.

5.5 Bağımsız Bir Erişim Noktasının Temel Ayarları

Bağımsız bir erişim noktasının *Basic Settings* (Temel Ayarlar) sekmesi yalnızca geçerli modun bağımsız olduğunu gösterir. Söz konusu erişim noktasını mevcut bir kümeye eklemek isterseniz *Cluster > Access Point* (Küme > Erişim Noktası) sekmesine gidin..


Daha fazla bilgi için bkz. “Kümeleme Başlatma”, sayfa 60.

5.6 Bir Bakışta Ağınızı Tanıma: Gösterge Simgelerini Anlama

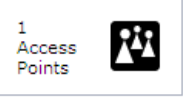
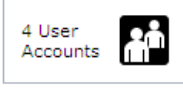
Yönetim Web sayfalarındaki Küme ayarları sekmelerinin hepsi, geçerli ağ aktivitesini gösteren görsel gösterge simgelerini içerir.

5.7 Farklı Renk ve Stillerle Kullanıcı Arabirimini Görüntüleme

Tablo 5.3 Gösterge Simgeleri

Simge	Açıklama
	<p>Ağınızda bir ya da daha fazla AP kullanılabilir durumdaysa "Kablosuz Ağ Mevcut" simgesi görüntülenir. Kümeleme simgesi, geçerli erişim noktasının "Clustered" (Kümelenmiş) bir AP mi yoksa "Not Clustered" (Kümelenmemiş) (bağımsız ya da durum değişikliği devam eden) bir AP mi olduğunu gösterir.</p> <p>Kümeleme hakkında bilgi için bkz. “Kümelemeyi Anlama”, sayfa 56.</p>

Tablo 5.3 Gösterge Simgeleri (Devamı)

Simge	Açıklama
	"Access Point" (Erişim Noktası) simgesi, bu ağdaki kullanılabilir durumda olan erişim noktalarının sayısını gösterir. Erişim noktalarını yönetmeyle ilgili bilgi için bkz. Bölüm 6: "Erişim Noktalarını ve Kümeleri Yönetme".
	"User Accounts" (Kullanıcı Hesapları) simgesi, Kullanıcı hesaplarının bu ağda oluşturduğu ve etkinleştirdiği istemci sayısını gösterir. Erişim noktasında dahili kimlik doğrulama sunucusuyla kullanmak üzere kullanıcı hesapları oluşturma hakkında bilgi için bkz. Bölüm 7: "Kullanıcı Hesaplarını Yönetme". Dahili kimlik doğrulama sunucusunu kullanma seçeneğini sunan şu güvenlik modlarına da bakın: "IEEE 802.1x", sayfa 108 ve "WPA Kurumsal", sayfa 113.

9160 G2 Kablosuz Ağ Geçidi cihazının Yönetim Web sayfaları (1) Kurumsal stil ve (2) Ev stili olmak üzere iki farklı renk temasında ve stilinde sunulur.

Görüntülediğiniz Kullanıcı Arabiriminin stilini istediğiniz gibi değiştirebilirsiniz.

Stil değiştirmek için herhangi bir Yönetim Web sayfasının alt kısmında "Style: Corporate, Home" (Stil: Kurumsal, Ev) düğmesini bulun ve **Corporate** (Kurumsal) ya da **Home** (Ev) seçeneklerinden birini belirleyin.



ERİŞİM NOKTALARINI VE KÜMELERİ YÖNETME

6

6.1 Genel Bakış	55
6.2 Erişim Noktası Yönetimine Gitme	55
6.3 Kümelemeyi Anlama	56
6.3.1 Küme Nedir?	56
6.3.2 Bir Küme Kaç AP Destekleyebilir?	56
6.3.3 Hangi Tür AP'ler Birlikte Kümelenebilir?	56
6.3.4 Koordinatör AP'nin Diğer Küme Üyeleriyle İlişkisi Nedir?	57
6.3.5 Hangi Ayarlar Küme Yapılandırmasının Bir Parçası Olarak Paylaşılır, Hangileri Paylaşılmaz?	57
6.3.5.1 Küme Yapılandırmasında Paylaşılan Ayarlar	57
6.3.5.2 Kümeyle Paylaşılmayan Ayarlar	58
6.3.6 Küme Oluşturma	58
6.3.7 Küme Büyüklüğü ve Üyelik	58
6.3.8 Küme İçi Güvenliği	58
6.4 Erişim Noktası Ayarlarını Anlama	59
6.4.1 Konum Açıklamasını Değiştirme	60
6.4.2 Küme Adını Ayarlama	60
6.5 Kümeleme Başlatma	60
6.6 Kümelemeyi Durdurma	61
6.7 Belirli Bir AP'nin Yapılandırma Bilgileri ve Bağımsız AP'leri Yönetme	61
6.7.1 Bir URL'deki IP Adresini Kullanarak AP'ye Gitme	62
6.8 Oturum İzleme	62
6.8.1 Oturum İzleme Bölümüne Gitme	62
6.8.2 Oturum İzleme Bilgilerini Anlama	62
6.8.3 Erişim Noktası Oturum Bilgilerini Göüntüleme	64
6.8.4 Oturum Bilgilerini Sıralama	64
6.8.5 Oturum Bilgilerini Yenileme	64

6.1 Genel Bakış

9160 G2 Kablosuz Ağ Geçidi, kümelenen erişim noktalarının o anki temel yapılandırma ayarlarını (konum, IP adresi, MAC adresi, durum ve kullanılabilirlik) gösterir ve kümenin bir üyesi olan belirli AP'ler için tam yapılandırmaya gitme yolları sağlar.

Bağımsız erişim noktaları ya da bu kümenin üyesi olmayan erişim noktaları, bu listede görünmez. Bağımsız erişim noktalarını yapılandırmak için erişim noktasının IP adresini bilmeniz ve onu bir URL'de kullanmanız gerekir (<http://ErişimNoktasınınIPAdresi>).



Not: 9160 G2 Kablosuz Ağ Geçidi, aynı anda birden fazla yapılandırma değişiklikleri için tasarlanmamıştır. Birden fazla erişim noktası içeren bir ağız varsa, Yönetim Web sayfalarında birden fazla yönetici oturum açmışsa ve yapılandırmada değişiklikler yapıyorsa kümedeki tüm erişim noktaları senkronize kalır ancak birden fazla kullanıcı tarafından belirtilen tüm yapılandırma değişikliklerinin uygulanması garanti edilmez.

6.2 Erişim Noktası Yönetimine Gitme

Bir kümedeki erişim noktaları hakkındaki bilgileri görüntülemek ya da düzenlemek için **Cluster > Access Points** (Küme > Erişim Noktaları) sekmesine gidin.

Şekil 6.1 Erişim Noktaları İçin Küme Ayarları

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

Stop Clustering

Clustering Options...

Enter the location of this AP.
Location: Vicky's Office - top shelf

Enter the name of the cluster for this AP to join.
Cluster Name: vicky-cluster

Update

6.3 Kümelemeyi Anlama

9160 G2 Kablosuz Ağ Geçidi cihazının önemli özelliklerinden biri, aynı alt ağdaki bir ağda yer alan diğer 9160 G2 Kablosuz Ağ Geçidi cihazlarıyla dinamik, yapılandırmaya duyarlı bir grup (*küme* olarak adlandırılır) oluşturabilmesidir. Erişim noktaları kendi kendini düzenleyen bir kümede yer alabilir. Bu durum, kablosuz ağınıza daha kolay dağıtmanızı, yönetmenizi ve korumanızı sağlar. Küme, tek bir yönetim noktası sunar ve erişim noktalarının ayrı kablosuz cihazlar serisi olarak değil, tek bir kablosuz ağ olarak dağıtımını görüntülemenize olanak sağlar.

6.3.1 Küme Nedir?

Küme, 9160 G2 Kablosuz Ağ Geçidi yönetimi aracılığıyla tek bir grup olarak koordine edilen bir grup erişim noktasıdır. Küme "adları" farklı olduğu sürece, aynı alt ağda birden fazla kümeniz olabilir.

6.3.2 Bir Küme Kaç AP Destekleyebilir?

Şu an bir kümede yer alabilecek erişim noktalarının sayısı ile ilgili kesin bir sınır yoktur. Doğrulama testleri, aynı alt ağda bir düzine ya da daha fazla erişim noktasının desteklendiğini doğrulamıştır. Herhangi bir zamanda, bir kümeye gerektiği kadar AP ekleyebilirsiniz.

6.3.3 Hangi Tür AP'ler Birlikte Kümelenebilir?

Tek bir 9160 G2 Kablosuz Ağ Geçidi, tek başına ("tek AP'lik Küme") ve diğer 9160 G2 Kablosuz Ağ Geçidi cihazlarıyla küme oluşturabilir. Erişim noktalarının aynı kümenin üyesi olabilmeleri için:

- Üretici tarafından belirtilen uyumlu cihazlar olmaları gerekir (erişim noktalarının uyumlu tasarım özellikleri olmalıdır).
- Aynı telsiz yapılandırmasında olmaları gerekir (hepsi ya tek telsizli ya da iki telsizli AP olmalıdır).
- Aynı bant yapılandırmasında olmaları gerekir (hepsi ya tek bant AP ya da çift bant AP olmalıdır).
- Aynı *LAN*'da olmaları gerekir.

Ağda farklı AP'lerin olması 9160 G2 Kablosuz Ağ Geçidi kümelenmesini olumsuz biçimde etkilemez. Ancak yönetim amaçlı olarak kümelenme davranışlarını anlamak faydalı olacaktır:

- Kümeye eklenen erişim noktaları aynı şekilde adlandırılmalıdır. Küme adı ayarlama hakkında daha fazla bilgi için bkz. sayfa 60.
- Başka markaların erişim noktaları kümeye katılamaz. Bu AP'ler kendi ilişkili Yönetim araçlarıyla yönetilmelidir.

6.3.4 Koordinatör AP'nin Diğer Küme Üyeleriyle İlişkisi Nedir?

Küme yapılandırması, yapılandırma güncellemelerinin paylaşılması ve gruba yeni katılan ya da gruptan ayrılan AP'lerin takibi, küme üyeleri arasından seçilen bir *koordinatör* AP tarafından yönetilir. Koordinatör AP kullanılamıyorsa koordinatör sorumlulukları yeni bir küme üyesine atanır. Bu süreç, bu görev için her zaman en uygun olacak AP'nin belirlenmesi için hesap eskiliğini (kıdemi), küme büyüklüğünü ve diğer faktörleri dikkate alan bir kural dizisine dayanan tamamen otomatik bir süreçtir.

Koordinatör olan AP kümenin ihtiyaçlarına bağlı olarak değişebileceği için hangi AP'nin koordinatör olduğunu takip etmeye ya da buna dikkat etmeye gerek yoktur. Yönetim Web sayfalarında yer alan koordinatör AP'ler ve diğer küme üyeleriyle ilgili yapılandırma bilgilerinde küçük farklılıklar dikkatinizi çekebileceğinden bu kavrama bu bölümde değinmek istedik.

6.3.5 Hangi Ayarlar Küme Yapılandırmasının Bir Parçası Olarak Paylaşılır, Hangileri Paylaşılmaz?

9160 G2 Kablosuz Ağ Geçidi Yönetim Web sayfaları aracılığıyla tanımlanan yapılandırma ayarlarının çoğu *küme yapılandırmasının* bir parçası olarak küme üyelerine geçer.

6.3.5.1 Küme Yapılandırmasında Paylaşılan Ayarlar

Küme yapılandırması şunları içerir:

- Ağ adı (SSID).
- Yönetici şifresi.
- Kullanıcı hesapları ve kimlik doğrulama.
- Kablosuz arabirim ayarları.
- Konuk Karşılama ekranı ayarları.
- Ağ Zaman Protokolü (NTP) ayarları.
- Telsiz ayarları.

Yalnızca mod, Kanal, Bölme Eşiği, RTS Eşiği ve Hız Grupları kümede senkronize edilir. Uyarı Aralığı, DTIM Süreci, Maksimum İstasyon Sayısı ve Aktarım Gücü kümelenmez.



Not: Kanal Planlama etkinleştirildiğinde telsiz kanalı kümede senkronize edilmez. Bkz. "Otomatik Kanal Atamayı Başlatma/Durdurma", sayfa 78

- Güvenlik ayarları.
- *QoS* kuyruk parametreleri.
- MAC adresi filtreleme.

6.3.5.2 Kümeyle Paylaşılmayan Ayarlar

Kümelenen erişim noktaları arasında *paylaşılmayan* ve çoğu doğası gereği benzersiz olmak zorunda olan birkaç istisna şunlardır:

- IP adresleri.
- MAC adresleri.
- Konum açıklamaları.
- Yük Dengeleme ayarları.
- WDS köprüleri.
- Ethernet (Kablolu) Ayarları.
- Konuk arabirimi yapılandırması.

Paylaşılmayan ayarlar, her erişim noktası için Yönetim sayfasında ayrı ayrı yapılandırılmalıdır. Geçerli kümenin üyesi olan bir erişim noktasının Yönetim Web sayfasına gitmek için, geçerli AP'nin *Cluster > Access Points* (Küme > Erişim Noktaları) sayfasındaki IP Adresi bağlantısına tıklayın.

6.3.6 Küme Oluşturma

Etkinleştirilen kümeye ilk AP yerleştirildiğinde küme oluşturulmuş olur. AP, mevcut bir kümeyle birleşmeye çalışır. Alt ağda aynı küme adına sahip başka AP'ler bulamazsa kendi kümesini oluşturur.

6.3.7 Küme Büyüklüğü ve Üyelik

Şu an bir kümede yer alabilecek AP'lerin sayısı ile ilgili kesin bir sınır yoktur. Doğrulama testleri, aynı alt ağda bir düzine ya da daha fazla erişim noktasının desteklendiğini doğrulamıştır. Herhangi bir zamanda, bir kümeye gerektiği kadar AP ekleyebilirsiniz.

Küme üyeliği şu faktörler tarafından belirlenir:

- Küme Adı - Aynı ada sahip AP'ler aynı kümeye katılır (bkz. "Küme Adını Ayarlama", sayfa 60).
- Kümelenmenin etkin olup olmadığı - Yalnızca kümelenmenin etkinleştirildiği AP'ler bir kümeye katılabilir. (bkz. "Kümelenme Başlatma", sayfa 60 ve "Kümelenmeyi Durdurma", sayfa 61).

6.3.8 Küme İçi Güvenliği

Kümelenme bileşeni, kullanım kolaylığı için yeni cihazların güçlü bir kimlik doğrulaması gerekmeden kümeye katılmasına izin verecek şekilde tasarlanmıştır. Ancak, bir kümede yer alan erişim noktaları arasındaki tüm veri iletişimi, Güvenli Yuva Katmanı (SSL) kullanılarak gündelik dinlemelere karşı korunur. Cihazların bağlı olduğu özel kablolu ağın güvenli olduğu varsayılır. Hem küme yapılandırma dosyası hem de kullanıcı veritabanı SSL kullanılarak erişim noktaları arasında aktarılır.

6.4 Erişim Noktası Ayarlarını Anlama

Access Point (Erişim Noktası) sekmesi, kümedeki tüm erişim noktalarıyla ilgili bilgi sunar. Bu sekmeden konum açıklamalarını, MAC adreslerini, IP adreslerini görüntüleyebilir, *kümelenen* erişim noktalarını etkinleştirebilir (başlatabilir) ya da devre dışı bırakabilir (durdurabilir) ve erişim noktalarını kümeden silebilirsiniz. Ayrıca, bir erişim noktasının konum açıklamasını da değiştirebilirsiniz. IP adresi bağlantıları bir erişim noktasındaki yapılandırma ayarlarına ve verilere gitmek yolu sunar.

Bağımsız erişim noktaları (bu kümenin üyesi olmayan erişim noktaları), bu sayfada görünmez.

Location	MAC Address	IP Address
Vicky's Office - top shelf	00:0C:41:16:A3:12	10.10.100.238
Vicky's Office - lower shelf	00:00:04:7F:00:00	10.10.100.245

Tablo 6.1, erişim noktası ayarlarını ve bilgi ekranını ayrıntılı biçimde açıklar.

Tablo 6.1 Erişim Noktası Ayarlar 1

Alan	Açıklama
<i>Location</i> (Konum)	Erişim noktasının fiziksel olarak nerede olduğunu açıklar.
<i>MAC Address</i> (MAC Adresi)	<p>Erişim noktasının Ortam Erişim Denetimi (MAC) adresi.</p> <p>MAC adresi, bir arabirimi ağa tanıtan herhangi bir cihazın kalıcı ve benzersiz donanım adresidir. MAC adresi üretici tarafından atanır. MAC adresini değiştiremezsiniz. Erişim noktasının benzersiz bir tanımlayıcısı olduğu için burada bilgi amaçlı değiştirilmiştir.</p> <p>Burada görülen adres, köprüye (br0) ait MAC adresidir. AP, dışarıdaki diğer ağlar tarafından bu adresle bilinir.</p> <p>AP'deki Konuk ve Dahili arabirimlerinin MAC adreslerini görmek için <i>Status > interfaces</i> (Durum > Arabirimler) sekmesine gidin.</p>

Tablo 6.1 Erişim Noktası Ayarlar (Devamı)

Alan	Açıklama
<i>IP Address</i> (<i>IP Adresi</i>)	Erişim noktasının IP adresini belirtir. Her IP adresi, o erişim noktasına ait Yönetim Web sayfasına giden bir bağlantıdır. Belirli bir erişim noktasının Yönetim Web sayfasına gitmek için bu bağlantıları kullanabilirsiniz. Bu özellik, bir küme üyesinin küme yapılandırma değişikliklerini aldığından emin olmak, belirli bir erişim noktasında gelişmiş ayarlar yapılandırmak ya da bağımsız erişim noktalarını küme moduna dönüştürmek için belirli bir erişim noktasındaki verileri görüntülemeye fayda sağlar.

6.4.1 Konum Açıklamasını Değiştirme

Konum açıklamasında değişiklikler yapmak için:

1. *Cluster > Access Points* (Küme > Erişim Noktaları) sekmesine gidin.
2. *Clustering Options* (Kümeleme Seçenekleri) kısmında *Location* (Konum) alanına AP'nin yeni konumunu yazın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

6.4.2 Küme Adını Ayarlama

AP'nizin katılmasını istediğiniz kümenin adını ayarlamak için aşağıdakileri yapın:

1. *Cluster > Access Points* (Küme > Erişim Noktaları) sekmesine gidin.
2. *Clustering Options* (Kümeleme Seçenekleri) kısmında *Cluster Name* (Küme Adı) alanına yeni küme adını yazın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.



Not: Birden fazla AP'nin belirli bir kümeye katılmasını istiyorsanız tüm AP'lerin Küme Adı alanında belirtilen Küme Adına sahip olması gerekir. Küme adı farklıysa AP kümeye katılamaz.

6.5 Kümeleme Başlatma

Kümeleme başlatmak ve belirli bir erişim noktasını bir kümeye eklemek için aşağıdakileri yapın:

1. Bağımsız erişim noktasının Yönetim Web sayfalarına gidin. (Bkz. “Bir URL'deki IP Adresini Kullanarak AP'ye Gitme”, sayfa 62.)
Bağımsız erişim noktasının Yönetim Web sayfaları görüntülenir.
2. Bağımsız erişim noktası için **Cluster > Access Points** (Küme > Erişim Noktaları) sekmesine gidin.

3. **Start Clustering** (Kümelemeyi Başlat) düğmesine tıklayın.
Erişim noktası artık bir küme üyesidir. *Cluster > Access Points* (Küme > Erişim Noktaları) sekmeli sayfadaki kümelenen erişim noktaları listesinde yer alır.



Not: Bazı durumlarda küme senkronizasyonu durabilir. Kümeye bir erişim noktası eklendikten sonra AP listesi eklenen AP'yi içermiyorsa ya da tamamlanmamış bir ekran gösteriyorsa Ek C: "Sorun Giderme" kısmında yer alan Küme Kurtarma bilgilerine bakın.

6.6 Kümelemeyi Durdurma

Kümelemeyi durdurmak ve belirli bir erişim noktasını bir kümeden çıkarmak için aşağıdakileri yapın:

1. Kümeden çıkarmak istediğiniz erişim noktasının Yönetim Web sayfasına gidin.
2. **Cluster > Access Points** (Küme > Erişim Noktaları) sekmesine tıklayın.
3. Erişim noktasını Kümeden çıkarmak için **Stop Clustering** (Kümelemeyi Durdur) düğmesine tıklayın.

Değişiklik ilgili erişim noktasının *Status* (Durum) alanına yansıyor ve erişim noktası durumu artık *küme* yerine *bağımsız* olarak görünecektir.



Not: Bazı durumlarda küme senkronizasyonu durabilir. Bir erişim noktasını kümeden çıkardıktan sonra AP listesi halen silinen AP'yi içeriyorsa ya da tamamlanmamış bir ekran gösteriyorsa tarayıcınızı yenileyin. Sorun devam ediyorsa Ek C: "Sorun Giderme" kısmında yer alan Küme Kurtarma bilgilerine bakın.

6.7 Belirli Bir AP'nin Yapılandırma Bilgileri ve Bağımsız AP'leri Yönetme

9160 G2 Kablosuz Ağ Geçidi, genel olarak *kümelenen* erişim noktalarının merkezi yönetimi için tasarlanmıştır. Bir kümedeki tüm erişim noktaları aynı yapılandırmayı yansıtır. Bu durumda, yönetim için gerçekte hangi erişim noktasına bağlandığınız fark etmez.

Ancak, belirli bir erişim noktasının bilgilerini görüntülemek ve yönetmek istediğiniz durumlar olabilir. Örneğin, istemci ilişkileri ya da erişim noktası olayları gibi durum bilgilerini kontrol etmek isteyebilirsiniz. Ya da, *bağımsız* modda çalışan bir erişim noktasındaki özellikleri yapılandırmak ve yönetmek isteyebilirsiniz. Bu gibi durumlarda, Erişim Noktasının sekmesinde yer alan IP adresi bağlantısına tıklayarak her erişim noktasının Yönetim Web arabirimine gidebilirsiniz.

Kümelenen tüm erişim noktaları *Cluster > Access Points* (Küme > Erişim Noktası) sayfasında görüntülenir. Kümelenen erişim noktalarına gitmek için listede yer alan belirli bir küme üyesinin IP adresine tıklayabilirsiniz.

6.7.1 Bir URL'deki IP Adresini Kullanarak AP'ye Gitme

Belirli bir erişim noktasının Yönetim Web sayfasına, bu erişim noktasının IP adresini doğrudan bir web tarayıcının adres çubuğuna URL şeklinde yazarak bağlanabilirsiniz:

http://ErişimNoktasınınIPAdresi

ErişimNoktasınınIPAdresi, izlemek ya da yapılandırmak istediğiniz erişim noktasının adresine işaret eder. Bağımsız erişim noktaları için bu yöntem, yapılandırma bilgilerine gitmenin tek yoludur.

6.8 Oturum İzleme


9160 G2 Kablosuz Ağ Geçidi cihazı, belirli bir erişim noktasıyla ilişkilenen istemciler, veri hızları, alma/verme istatistikleri, sinyal gücü ve eylemsiz süre dahil, gerçek zamanlı oturum izleme bilgileri sunar.


6.8.1 Oturum İzleme Bölümüne Gitme


Oturum izleme bilgilerini görüntülemek için **Cluster > Sessions** (Küme > Oturumlar) sekmesine tıklayın.

Şekil 6.2 Oturum İzleme Bilgileri

Manage sessions associated with the cluster

Clustered 

1 Access Points 

0 User Accounts 

Sessions...
You may sort the following table by clicking on any of the column names.
Display

User	AP Location	User MAC	Idle	Rate (Mbps)	Signal	Utilization	Rx Total	Tx Total	Error Rate	Idle
Ciara	not set	00:90:4b:93:f4:35	150	54	44	0.1 %	78944	107640	0	150
Sean	not set	00:0c:f1:3e:99:ae	190	11	44	0.4 %	4462	3147	0	190

You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By selecting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

6.8.2 Oturum İzleme Bilgilerini Anlama

Sessions (Oturumlar) sayfası kümedeki erişim noktalarıyla ilişkili olan istemciler hakkındaki bilgileri gösterir. Her istemci kullanıcı adı ve kullanıcı **MAC** adresinin yanı sıra istemcinin o an bağlı olduğu AP (konum) ile tanımlanır.

İstemci oturumlarıyla ilgili belirli istatistikleri görüntülemek için Display (Göster) açılır listesinden bir öğe seçin ve **Go** (Git) seçeneğine tıklayın. *Eylemsiz Süre*, *Veri Hızı*, *Sinyal*, *Kullanım* gibi hepsi Tablo 6.2, sayfa 63'te ayrıntıyla açıklanan bilgileri görüntüleyebilirsiniz.

Bu bağlamda "oturum", bir kullanıcının benzersiz bir MAC adresi olan bir istemci cihazında (istasyon), kablolu ağ ile bağlantı kurduğu zaman dilimidir. Oturumlar, istemci ağda oturum açtığında başlar ve istemci kasıtlı olarak oturumu kapattığında ya da herhangi bir sebepten ötürü bağlantısı koptuğunda sona erer.



Not: Oturum ile ilişki aynı şey değildir; ilişki, bir istemcinin belirli bir erişim noktasına bağlantısını ifade eder. Bir istemci ağ bağlantısı, aynı oturum kapsamında kümelenen AP'lerin birinden diğerine geçebilir. Bir istemci istasyonu AP'ler arasında gezinirken halen oturumda kalabilir.

İlişkileri izleme ve bağlantı bütünlüğünü izleme hakkında bilgi için bkz. "İlişkili Kablosuz İstemciler", sayfa 129.

Tablo 6.2 Oturum iBilgiler

Alan	Açıklama
<i>User Name</i> (Kullanıcı Adı)	IEEE 802.1x istemcilerinin istemci kullanıcı adını belirtir. Not: Bu alan, yalnızca IEEE 802.1x güvenlik modunu ve yerel kimlik doğrulama sunucusunu kullanarak AP'lere bağlanan istemciler içindir. (Bu mod hakkında daha fazla bilgi için bkz. "IEEE 802.1x", sayfa 108.) RADIUS sunucusuyla IEEE 802.1x ya da diğer güvenlik modlarını kullanan AP'lerin istemcilerinin kullanıcı adları burada görünmez.
<i>AP Location</i> (AP Konumu)	Erişim noktasının konumunu belirtir. Bu bilgi <i>Basic Settings</i> (Temel Ayarlar) sekmesinde belirtilen konum açıklamasından türetilir.
<i>User MAC Address</i> (Kullanıcı MAC Adresi)	Kullanıcının istemci cihazının (istasyon) MAC adresini belirtir. MAC adresi bir ağdaki her düğümü benzersiz biçimde tanımlayan bir donanım adresidir.
<i>Idle Time</i> (Eylemsiz Süre)	Bu istasyonun aktif olmadığı süreyi belirtir. Bir istasyon, herhangi bir veri almadığı ya da aktarmadığı zamanlarda "eylemsiz" olarak değerlendirilir.
<i>Data Rate</i> (Veri Hızı)	Bu erişim noktasının belirli bir istemciye veri aktarma hızını belirtir. Veri aktarma hızı <i>megabit/saniye</i> (Mb/sn) cinsinden ölçülür. Bu değer, erişim noktasında kullanılan IEEE 802.11 modu için belirtilen hız grubu aralığında olmalıdır. Örneğin, 802.11a için 6 - 54 Mb/sn.
<i>Signal</i> (Sinyal)	İstemcinin erişim noktasından aldığı telsiz frekansı (RF) sinyalinin gücünü gösterir. Sinyal için kullanılan ölçü, <i>Alınan Sinyal Gücü Göstergesi</i> (RSSI) olarak bilinen bir IEEE 802.11 değeridir ve 0-100 arası bir değer olmalıdır. RSSI, istemci istasyonunun ağ arabirim kartında (NIC) uygulanan bir IEEE 802.1x mekanizması tarafından belirlenir.

Tablo 6.2 Oturum iBilgiler (Devamı)

Alan	Açıklama
<i>Utilization</i> (Kullanım)	Bu istasyonun kullanım oranıdır. Örneğin, istasyon, zamanının %90'ında "aktif" (veri alıyor ve aktarıyor) ve kalan %10'da aktif değilse istasyonun kullanım oranı %90'dır.
<i>Receive Total</i> (Toplam Alınan)	İstemcinin geçerli oturum sırasında aldığı toplam paket sayısını belirtir.
<i>Transmit Total</i> (Toplam Aktarılan)	Geçerli oturum sırasında istemciye aktarılan toplam paket sayısını belirtir.
<i>Error Rate</i> (Hata Oranı)	Bu erişim noktasında aktarım sırasında düşen zaman çerçevesi yüzdesini belirtir.

6.8.3 Erişim Noktası Oturum Bilgilerini Görüntüleme

Ağdaki tüm erişim noktalarının oturum bilgilerini aynı anda görüntüleyebilir ya da ekranın üst kısmındaki açılır menüden seçtiğiniz bir erişim noktasının oturum bilgilerini görüntülemek için ekranı ayarlayabilirsiniz.

Tüm erişim noktalarıyla ilgili bilgileri görüntülemek için sayfanın üst kısmındaki **Show all access points** (Tüm erişim noktalarını göster) radyo düğmesini seçin.

Belirli bir erişim noktasının oturum bilgilerini görüntülemek için **Show only this access point** (Yalnızca bu erişim noktasını göster) radyo düğmesini seçin ve açılır menüden erişim noktasının adını seçin.

6.8.4 Oturum Bilgilerini Sıralama

Tablolarda gösterilen bilgileri belirli bir göstergeyle sıralamak için istediğiniz sütun başlığına tıklayın. Örneğin, tablodaki satırları Kullanım oranına göre sıralanmış olarak görmek istiyorsanız **Utilization** (Kullanım) sütun başlığına tıklayın. Girişler Kullanım oranına göre sıralanır.

6.8.5 Oturum Bilgilerini Yenileme

Refresh (Yenile) düğmesine basarak *Session Monitoring* (Oturum İzleme) sayfasında görüntülenen bilgileri güncelleyebilirsiniz.

KULLANICI HESAPLARINI YÖNETME

7

7.1 Genel Bakış	67
7.2 Kullanıcı Yönetimine Gitme	67
7.2.1 Kullanıcı Hesaplarını Görüntüleme	68
7.2.2 Kullanıcı Ekleme	68
7.2.3 Kullanıcı Hesaplarını Düzenleme	69
7.2.4 Kullanıcı Hesaplarını Etkinleştirme ve Devre Dışı Bırakma	70
7.2.5 Bir Kullanıcı Hesabını Etkinleştirme	70
7.2.6 Bir Kullanıcı Hesabını Devre Dışı Bırakma	71
7.2.7 Bir Kullanıcı Hesabını Kaldırma	71
7.3 Kullanıcı Veritabanını Yedekleme ve Geri Yükleme	71
7.3.1 Kullanıcı Veritabanını Yedekleme	71
7.3.2 Veritabanını Yedekleme Dosyasından Geri Yükleme	71

7.1 Genel Bakış

9160 G2 Kablosuz Ağ Geçidi, istemcilerin erişim noktalarına erişimlerinin kontrolüyle ilgili kullanıcı yönetimi özellikleri içerir.

Kullanıcı yönetimi ve kimlik doğrulama her zaman kullanıcı kimliğinin doğrulanması ve kullanıcı yönetimi için bir **RADIUS** sunucusunun kullanılmasını gerektiren şu iki güvenlik moduyla birlikte kullanılmalıdır:

- IEEE 802.1x modu (bkz. “IEEE 802.1x”, sayfa 108, Bölüm 10: “Güvenliği Yapılandırma”).
- RADIUS içeren WPA modu (bkz. “WPA Kurumsal”, sayfa 113, Bölüm 10: “Güvenliği Yapılandırma”).

9160 G2 Kablosuz Ağ Geçidi cihazında gömülü dahili RADIUS sunucusunu ya da sağladığınız harici bir RADIUS sunucusunu kullanmayı seçebilirsiniz. Gömülü RADIUS sunucusunu kullanmayı seçerseniz kullanıcı hesapları oluşturmak ve yönetmek için erişim noktasındaki Yönetim Web sayfasını kullanın. Harici RADIUS sunucusunu seçerseniz kullanıcı hesaplarını o sunucunun Yönetici arabiriminde oluşturmanız ve yönetmeniz gerekir.

Kullanıcı Yönetimi sayfasında istemci *kullanıcı hesaplarını* oluşturabilir, düzenleyebilir, kaldırabilir ve görüntüleyebilirsiniz. Her kullanıcı hesabı bir kullanıcı adı ve şifreden oluşur. Burada belirtilen kullanıcı grubu, oturum açabilen ve kablosuz ağınız aracılığıyla yerel ve olasılıkla harici ağlara erişmek için bir veya daha fazla erişim noktası kullanabilen onaylı *istemcileri* temsil etmektedir.



Not: Burada belirtilen kullanıcılar, kablosuz ağ yöneticileri değil, AP'leri bağlantı hub'ı olarak kullanan erişim noktası istemcileridir. Yalnızca yönetici kullanıcı adı ve şifresi olan ve yönetim URL'sini bilenler yönetici olarak giriş yapabilir ve yapılandırma ayarlarını görüntüleyip değiştirebilir.

7.2 Kullanıcı Yönetimine Gitme

Kullanıcı hesaplarını oluşturmak ve değiştirmek için **User Management** (Kullanıcı Yönetimi) sekmesine tıklayın.

Şekil 7.1 Kullanıcı Hesaplarını Yönetme

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Manage user accounts

User Accounts...

0 User Accounts

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

☐ Edit Username Real name Status

Selected users:

[\[backup or restore the user database\]](#)

Add a user...

To add a user, fill in the fields below and click: "Add Account".

Username

Real name

Password

Password (again for safety)

7.2.1 Kullanıcı Hesaplarını Görüntüleme

Kullanıcı hesapları, ekranın üst kısmındaki *User Accounts...* (Kullanıcı Hesapları...) bölümünde gösterilir. Kullanıcıyla ilgili Username (Kullanıcı Adı), Real name (Gerçek Ad) ve Status (Durum) (enabled [etkin] ya da disabled [devre dışı]) bilgileri yer alır. Mevcut bir kullanıcı hesabında değişiklik yapmak için önce kullanıcı adının yanındaki kutuyu işaretleyin ve ardından istediğiniz işlemi seçin. (Bkz. "Kullanıcı Hesaplarını Düzenleme", sayfa 69.)

7.2.2 Kullanıcı Ekleme

Yeni bir kullanıcı oluşturmak için şunları yapın:

1. *Add a User...* (Kullanıcı Ekle...) kısmında şu alanları doldurun:

Tablo 7.1 Yeni Kullanıcı Alanları

Alan	Açıklama
<i>Username (Kullanıcı Adı)</i>	Bir kullanıcı adı yazın. Kullanıcı adları, maksimum 237 karakterden oluşan alfanümerik dizelerdir. Özel karakterler ve boşluk kullanmayın.
<i>Real name (Gerçek Ad)</i>	Bilgilendirme amaçlı olarak kullanıcının tam adını yazın. Gerçek adlar için 256 karakterlik bir sınırlama vardır.
<i>Password (Şifre)</i>	Bu kullanıcı için bir şifre belirleyin. Şifreler, maksimum 256 karakterden oluşan alfanümerik dizelerdir. Özel karakterler ve boşluk kullanmayın.

- İlgili alanları doldurduktan sonra hesap eklemek için **Add Account** (Hesap Ekle) seçeneğine tıklayın.

Yeni kullanıcı *User Accounts...* (Kullanıcı Hesapları...) kısmında görüntülenir. Kullanıcı hesabını oluşturduğunuzda hesap varsayılan olarak **etkindir**.



Not: Yönetim kullanıcı arabirimi tarafından erişim noktası başına 100 kullanıcı hesabı sınırlaması getirilmiştir. Ağ kullanımı, her kullanıcıdan gelen talebe bağlı olarak daha pratik bir sınırlama getirebilir.

7.2.3 Kullanıcı Hesaplarını Düzenleme

Bir kullanıcı hesabı oluşturduğunuzda hesap *Kullanıcı Yönetimi* Yönetim Web sayfasının üst kısmında yer alan *User Accounts...* (Kullanıcı Hesapları...) bölümünde görüntülenir.

Mevcut bir hesapta değişiklik yapmak için ilk önce kullanıcı adının yanındaki kutucuğu tıklayarak işaretleyin.

User Accounts...

To enable or disable a user, click the "Enable" or "Disable" button. Likewise, to remove a user, click the "Remove" button. Ensure that you have selected at least one user prior to any of these actions. **Note:** These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

<input type="checkbox"/> Edit	Username	Real name	Status
<input type="checkbox"/> [Edit]	Engineer	Mary SMith	enabled
<input type="checkbox"/> [Edit]	Manager	Tom Jones	enabled
<input type="checkbox"/> [Edit]	Tester	Joe Bloggs	enabled

Selected users:

[\[backup or restore the user database\]](#)

Ardından **Edit** (Düzenle), **Enable** (Etkinleştir), **Disable** (Devre Dışı Bırak) ya da **Remove** (Kaldır) eylemlerinden birini seçin.

7.2.4 Kullanıcı Hesaplarını Etkinleştirme ve Devre Dışı Bırakma

Kullanıcının istemci olarak oturum açması ve erişim noktasını kullanması için kullanıcı hesabının etkinleştirilmesi gerekir.

Tüm kullanıcı hesaplarını *etkinleştirebilir* ve *devre dışı bırakabilirsiniz*. Bu özellik sayesinde, hesapları kaldırmak ya da yeniden oluşturmak zorunda kalmadan bir dizi kullanıcı hesabına sahip olabilir ve kullanıcıların ağa erişimini onaylayıp engelleyebilirsiniz. Kullanıcıların nadiren ağa erişmesinin gerektiği durumlarda bu özellik işinize yarayabilir. Örneğin, şirketinizle düzenli ancak belirli aralıklarla iş yapan yüklenicilerin 3 ay ağa erişmesi gerekirken sonraki 3 ay şirketinizle çalışmayabilir ve daha sonra başka bir iş için tekrar ağa erişmesi gerekebilir. Bu gibi kullanıcı hesaplarını gerektiğinde etkinleştirip devre dışı bırakabilir ve erişimlerini uygun şekilde kontrol edebilirsiniz.

7.2.5 Bir Kullanıcı Hesabını Etkinleştirme

Bir kullanıcı hesabını etkinleştirmek için kullanıcı adının yanındaki kutucuğu işaretledikten sonra **Enable** (Etkinleştir) seçeneğine tıklayın. *Etkinleştirilmiş* hesabı olan bir kullanıcı, ağınızdaki kablosuz erişim noktasında istemci olarak oturum açabilir.

7.2.6 Bir Kullanıcı Hesabını Devre Dışı Bırakma

Bir kullanıcı hesabını devre dışı bırakmak için kullanıcı adının yanındaki kutucuğu işaretledikten sonra **Disable** (Devre Dışı Bırak) seçeneğine tıklayın.

Devre dışı bırakılmış hesabı olan bir kullanıcı, ağınızdaki kablosuz erişim noktasında istemci olarak oturum açamaz. Ancak kullanıcı veritabanında kalır ve daha sonra gerektiğinde etkinleştirilebilir.

7.2.7 Bir Kullanıcı Hesabını Kaldırma

Bir kullanıcı hesabını kaldırmak için kullanıcı adının yanındaki kutucuğu işaretledikten sonra **Remove** (Kaldır) seçeneğine tıklayın.

Bu kullanıcıyı daha sonra tekrar eklemek isteyebileceğinizi düşünüyorsanız hesabı tamamen kaldırmak yerine *devre dışı bırakmayı* düşünebilirsiniz.

7.3 Kullanıcı Veritabanını Yedekleme ve Geri Yükleme

Mevcut kullanıcı hesapları grubunun bir kopyasını, bir yedekleme yapılandırma dosyasına kaydedebilirsiniz. Yedekleme dosyası, AP'deki kullanıcı hesaplarını önceden kaydedilen bir yapılandırmaya geri yüklemek için ileriki bir zamanda kullanılabilir.

7.3.1 Kullanıcı Veritabanını Yedekleme

Bu erişim noktasına ait kullanıcı hesaplarının yedek kopyasını oluşturmak için:

1. [backup or restore the user database] (kullanıcı veritabanını yedekle ya da geri yükle) bağlantısına tıklayın.

File Download or Open (Dosya İndir ya da Aç) iletişim kutusu görüntülenir.

2. Bu ilk iletişim kutusunda **Save** (Kaydet) seçeneğini belirleyin.

Bir dosya tarayıcı açılır.

Dosyayı kaydetmek istediğiniz dizine gitmek için dosya tarayıcıyı kullanın ve dosyayı kaydetmek için **OK** (Tamam) seçeneğine tıklayın.

Varsayılan dosya adını kullanabilir (wirelessUsers.ubk) ya da yedekleme dosyasını yeniden adlandırabilirsiniz ancak dosyayı .ubk uzantısıyla kaydettiğinizden emin olun.

7.3.2 Veritabanını Yedekleme Dosyasından Geri Yükleme

Kullanıcı veritabanını yedekleme dosyasından geri yüklemek için:

1. Restore (Geri Yükle) alanına yolun tamamını ve dosya adını yazarak ya da **Browse**'a (Gözet) tıklayıp dosyayı seçerek kullanmak istediğiniz yedekleme yapılandırma dosyasını seçebilirsiniz.
(Yalnızca Kullanıcı Veritabanı Yedekleme işleviyle oluşturulan ve .ubk yedekleme yapılandırma dosyası olarak kaydedilen dosyalar (wirelessUsers.ubk gibi) Geri Yükleme işlemi için kullanılabilir.)
2. **Restore** (Geri Yükle) düğmesine tıklayın.
Yedekleme geri yükleme işlemi tamamlandığında kullanıcı veritabanının başarıyla geri yüklendiğini belirten bir mesaj görüntülenir. (Bu, zaman alan bir işlem değildir; geri yükleme süreci hemen tamamlanır.)
Geri yüklenen kullanıcı hesaplarını görmek için **User Management** (Kullanıcı Yönetimi) sekmesine tıklayın.

8.1 Kanal Yönetimine Gitme	75
8.2 Kanal Yönetimini Anlama	75
8.2.1 Çalışma Şekli Hakkında Kısa Bilgi	75
8.2.2 Merak Edenler İçin: Çakışan Kanallar Hakkında Daha Fazla Bilgi	76
8.2.3 Örnek: Bir Ağın Kanal Yönetiminden Önceki ve Sonraki Durumu	76
8.3 Kanal Yönetimi Ayarlarını Yapılandırma ve Görüntüleme	77
8.3.1 Otomatik Kanal Atamayı Başlatma/Durdurma	78
8.3.2 Geçerli Kanal Atamalarını Görüntüleme ve Kilit Koyma	78
8.3.3 Son Önerilen Değişiklik Grubunu Görüntüleme	79
8.3.4 Gelişmiş Ayarları Yapılandırma (Kanal Planlarını Özelleştirme/ Programlama)	80

8.1 Kanal Yönetimine Gitme

Oturum izleme bilgilerini görüntülemek için **Cluster > Channel Management** (Küme > Kanal Yönetimi) sekmesine tıklayın.

Şekil 8.1 Kanal Atamalarını Yönetme

The screenshot displays the 'Channel Management' interface. On the left is a sidebar with a list of settings: Basic Settings, User Management, Cluster, Access Points, Sessions, Channel Management (selected), Wireless Neighborhood, Security, Status, Interfaces, Events, Transmit/Receive, Client Associations, Neighboring Access Points, Manage, Ethernet Settings, 802.11 Settings, and 802.11 Advanced Settings. The main content area is titled 'Automatically manage channel assignments'. It includes a 'Channels ...' section with a 'Start' button and the text 'automatically re-assigning channels'. Below this is a table for 'Current Channel Assignments' with columns: IP Address, Radio, Band, Channel, and Locked. The table lists two entries: 10.10.100.238 on radio 00:0C:41:16:A3:12 (Band G, Channel 2) and 10.10.100.245 on radio 00:00:04:7F:00:00 (Band G, Channel 3). An 'Apply' button is at the bottom right of the table. To the right of the table are three icons: 'Clustered' (antenna), '2 Access Points' (two people), and '3 User Accounts' (three people). Below the table is a section for 'Proposed Channel Assignments (3 hours, 40 minutes and 52 seconds old)' with a table showing one entry: 10.10.100.238 on radio 00:0C:41:16:A3:12 (Proposed Channel 2). At the bottom is an 'Advanced' section with two settings: 'Change channels if interference is reduced by at least 5%' (dropdown) and 'Determine if there is better set of channel settings every 1 Minute' (dropdown). An 'Update' button is at the bottom right of the advanced section.

IP Address	Radio	Band	Channel	Locked
10.10.100.238	00:0C:41:16:A3:12	G	2	<input type="checkbox"/>
10.10.100.245	00:00:04:7F:00:00	G	3	<input type="checkbox"/>

IP Address	Radio	Proposed Channel
10.10.100.238	00:0C:41:16:A3:12	2

8.2 Kanal Yönetimini Anlama

Channel Management (Kanal Yönetimi) etkinleştirildiğinde 9160 G2 Kablosuz Ağ Geçidi cihazı, karşılıklı paraziti (ya da kümenin dışındaki diğer erişim noktalarıyla olan paraziti) azaltmak için otomatik olarak kümelenen erişim noktaları tarafından kullanılan telsiz kanalları atar. Bu durum, Wi-Fi bant genişliğini maksimum düzeye getirir ve kablosuz ağınızda verimli bir iletişim sağlanmasına yardımcı olur.

(Otomatik kanal atamaları almak için kanal yönetimini başlatmanız gereklidir. Kanal yönetimi, yeni AP'de varsayılan olarak devre dışıdır. Bkz. “Otomatik Kanal Atamayı Başlatma/Durdurma”, sayfa 78.)

8.2.1 Çalışma Şekli Hakkında Kısa Bilgi

Belirli aralıklarla (varsayılan **1 saattir**) ya da istendiğinde (**Update** [Güncelle] düğmesine basıldığında), Kanal Yöneticisi AP'leri kanal kullanımı için eşler ve kümedeki parazit seviyelerini ölçer. Önemli oranda kanal paraziti algılanırsa Kanal Yöneticisi, AP'lerin bazılarını ya da tamamını verimlilik algoritmasına (ya da *otomatik kanal planına*) göre otomatik olarak yeni kanallara atar.

8.2.2 Merak Edenler İçin: Çakışan Kanallar Hakkında Daha Fazla Bilgi

Telsiz frekansı (RF) yayını Kanal, erişim noktasındaki telsizin veri aktarma ve alma için kullandığı telsiz spektrumu bölümünü tanımlar. Bir erişim noktası için kullanılabilir kanalların menzili, erişim noktasının **IEEE 802.11** modu (bant olarak da bilinir) tarafından belirlenir.

IEEE **802.11b/802.11g** modları (802.11 b/g) 1-11 arası kanalların (1 ve 11 dahil) kullanımını desteklerken IEEE **802.11a** modu, ardışık olmayan daha geniş bir kanal grubunu (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165) destekler.

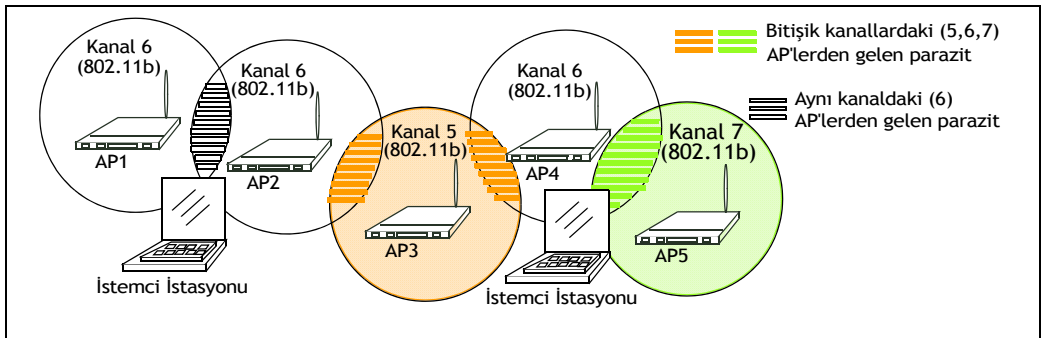
Birbirlerinin menziline olan birden fazla erişim noktası aynı ya da *çakışan* kanallarda yayın yaparken parazit oluşabilir. Bu parazitin ağ üzerindeki etkisi, büyük miktarlardaki veri ve medya trafiğinin bant genişliği için yarıştığı yoğun zamanlarda artabilir.

Kanal Yöneticisi, kümelenen AP'lerin hangi bantta (b/g ya da a) olduğunu algılar ve birbirleriyle parazit oluşturmamanı önceden belirlenmiş bir kanal koleksiyonu kullanır. "b/g" telsiz bandı için klasik parazitsiz kanallar grubu 1, 6, 11'dir. 1, 4, 8, 11 kanalları minimum çakışma oluşturur. Benzer bir parazitsiz kanallar grubu "a" telsiz bandı için de kullanılır. "a" telsiz bandı, hiçbir kanal çakışmadığından o mod için olan tüm kanalları içerir.

8.2.3 Örnek: Bir Ağın Kanal Yönetiminden Önceki ve Sonraki Durumu

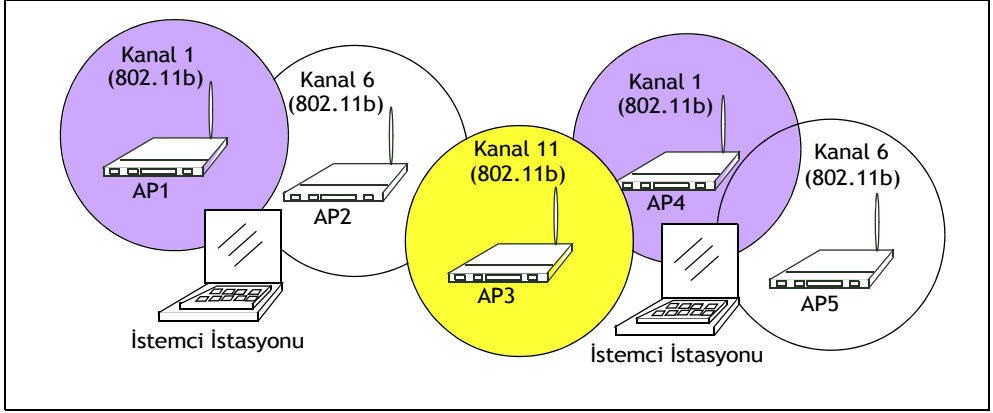
Otomatik kanal yönetimi olmadan kümelenen AP'lere yapılacak kanal atamaları, çakışacak ve parazit oluşturacak *ardışık kanallarda* yapılabilir. Örneğin, Şekil 8.2'de gösterildiği gibi AP1 kanal 6'ya, AP2 kanal 6'ya ve AP3 kanal 5'e atanabilir.

Şekil 8.2 Otomatik Kanal Yönetimi Olmadan



Otomatik kanal yönetimi kullanıldığında kümedeki AP'ler 8.3'te gösterildiği gibi otomatik olarak parazit oluşturmeyan kanallara atanır.

Şekil 8.3 Kanal Yönetimi Etkinleştirildiğinde



8.3 Kanal Yönetimi Ayarlarını Yapılandırma ve Görüntüleme

Kanal Yönetimi sayfası, kümelenen erişim noktalarının önceki, şimdiki ve planlanan kanal atamalarını gösterir. Otomatik kanal atama, varsayılan olarak devre dışıdır. Kümedeki kanal kullanımını planlanan aralıklarla optimize etmek için kanal yönetimini kullanmaya başlayabilirsiniz.

Bu sayfadan kümedeki tüm AP'lerin kanal atamalarını görüntüleyebilir, otomatik kanal yönetimini başlatabilir/durdurabilir ve geçerli kanal eşlemelerini (AP'lerden kanallara) manuel olarak "güncelleyebilirsiniz". Manuel güncellemede, Kanal Yöneticisi kanal kullanımını değerlendirir ve gerekirse geçerli Gelişmiş Ayarları temel alarak paraziti azaltmak için AP'leri yeni kanallara yeniden atayabilir.

Gelişmiş ayarları kullanarak kanalların yeniden atanmasını tetikleyen parazit azaltma potansiyelini düzenleyebilir, otomatik güncelleme programını değiştirebilir ve atama için kullanılan kanal grubunu yeniden yapılandırabilirsiniz.

Aşağıdaki bölümlerde kanal yönetiminin ağızda nasıl yapılandırılacağı ve kullanılacağı açıklanmaktadır:

- “Otomatik Kanal Atamayı Başlatma/Durdurma”, sayfa 78.
- “Geçerli Kanal Atamalarını Görüntüleme ve Kilit Koyma”, sayfa 78.
- “Geçerli Kanal Ayarlarını Güncelleme (Manuel)”, sayfa 79.

- “Son Önerilen Değişiklik Grubunu Görüntüleme”, sayfa 79.
- “Gelişmiş Ayarları Yapılandırma (Kanal Planlarını Özelleştirme/ Programlama)”, sayfa 80.
- “Gelişmiş Ayarları Güncelleme”, sayfa 81.

8.3.1 Otomatik Kanal Atamayı Başlatma/Durdurma

Otomatik kanal atama, varsayılan olarak devre dışıdır (kapalıdır).

- Otomatik kanal atamayı başlatmak için **Start** (Başlat) düğmesine basın. Otomatik kanal atama etkinleştirildiğinde Kanal Yöneticisi kümelenen erişim noktaları tarafından kullanılan telsiz kanallarını periyodik olarak eşler ve gerektiğinde küme üyeleri ya da kümenin dışındaki AP'lerle olan paraziti azaltmak için kümelenen AP'lerdeki kanalları yeniden atar.



Not: Kanal Yönetimi, bir kümedeki tüm AP'lerin telsiz kanallarını senkronize eden varsayılan küme davranışını geçersiz kılar. Kanal Yönetimi etkinleştirildiğinde telsiz kanalı kümedeki diğer AP'lerde senkronize edilmez. “Küme Yapılandırmasında Paylaşılan Ayarlar”, sayfa 57'deki Telsiz Ayarları bölümünde yer alan nota bakın.

- Otomatik kanal atamayı durdurmak için **Stop** (Durdur) düğmesine tıklayın. (Hiçbir kanal kullanımı eşlemesi ya da yeniden kanal atama işlemi yapılmaz. Kanal ataması, yalnızca manuel güncellemelerden etkilenir).

8.3.2 Geçerli Kanal Atamalarını Görüntüleme ve Kilit Koyma

Geçerli Kanal Ayarları kümedeki tüm erişim noktalarını IP Adreslerine göre listeler. Ekranda her AP'nin yayın yaptığı bant, her AP'nin kullandığı geçerli kanal ve bir AP'yi geçerli telsiz kanalında "kilitleyerek" başka bir kanala yeniden atanmamasını sağlayan bir seçenek görüntülenir. Geçerli Kanal Ayarlarıyla ilgili ayrıntılar aşağıda verilmiştir.

Tablo 8.1 Geçerli Kanal Ayarları

Alan	Açıklama
<i>IP Address (IP Adresi)</i>	Erişim noktasının IP Address (IP Adresi)'ni belirtir.
<i>Radio (Telsiz)</i>	Erişim noktasının MAC adresini belirtir.
<i>Band (Bant)</i>	Erişim noktasının yayın yaptığı bandı (b/g ya da a) belirtir.
<i>Channel (Kanal)</i>	Erişim noktasının o an yayın yaptığı telsiz Kanal adını belirtir.

Tablo 8.1 Geçerli Kanal Ayarları (Devamı)

Alan	Açıklama
<i>Locked (Kilitli)</i>	<p>Bu erişim noktasının geçerli kanalda kalmasını istiyorsanız Locked (Kilitli) seçeneğine tıklayın.</p> <p>"Locked" (Kilitli) onay kutusu bir erişim noktası için işaretlendiğinde (etkinleştirildiğinde) otomatik kanal yönetimi planları, AP'yi optimizasyon stratejisinin bir parçası olarak başka bir kanala yeniden atamaz. Bunun yerine, kilitli kanalı olan AP'ler, planın gerekliliklerinden biri olarak göz önünde bulundurulur.</p> <p>Update (Güncelle) seçeneğine tıkladığınızda kilitli AP'lerin "Current Channel" (Geçerli Kanal) ve "Proposed Channel" (Önerilen Kanal) alanlarında aynı kanalın görüntülendiğini görürsünüz. Kilitli AP'ler geçerli kanallarında kalır.</p>

8.3.2.1 Geçerli Kanal Ayarlarını Güncelleme (Manuel)

Current Channel Settings (Geçerli Kanal Ayarları) ekranında **Update** (Güncelle) düğmesine tıklayarak istediğiniz zaman manuel bir kanal yönetimi güncellemesi yapabilirsiniz.

8.3.3 Son Önerilen Değişiklik Grubunu Görüntüleme

Son Önerilen Değişiklik Grubu, son kanal planını gösterir. Plan, kümedeki tüm erişim noktalarını IP Adreslerine göre listeler ve her AP'nin geçerli ve önerilen kanallarını gösterir. Kilitli kanallar yeniden atanmaz ve kanalların AP'ler arasındaki dağıtımının optimizasyonu, kilitli AP'lerin geçerli kanallarında kalacağını göz önünde bulundurur. "Kilitli" olmayan AP'ler, plan sonuçlarına bağlı olarak önceden kullandıkları kanaldan farklı bir kanala atanabilir.

Tablo 8.2 AP'nin Kanal Planı

Alan	Açıklama
<i>IP Address (IP Adresi)</i>	Erişim noktasının IP Address (IP Adresi)'ni belirtir.
<i>Current (Geçerli)</i>	Erişim noktasının o an yayınladığı telsiz kanalını belirtir.
<i>Proposed (Önerilen)</i>	Kanal Planı uygulandığında bu erişim noktasının yeniden atanacağı telsiz kanalını belirtir.

8.3.4 Gelişmiş Ayarları Yapılandırma (Kanal Planlarını Özelleştirme/ Programlama)

Kanal Yönetimini sunulduğu şekilde (*Gelişmiş Ayarları* güncellemeden) kullandığınızda, parazit %25 ya da daha fazla azaltıldığında kanallara her saatte bir otomatik olarak ince ayar yapılır. Ağ meşgul olsa bile kanallar yeniden atanır. Uygun kanal grupları kullanılır (IEEE 802.11b/g kullanan AP'ler için "b/g" ve IEEE 802.11a kullanan AP'ler için "a").

Bu varsayılanlar kanal yönetimini uygulamaya ihtiyaç duyduğunuz durumların çoğunu karşılamak üzere tasarlanmıştır.

Kanalların yeniden atanmasını tetikleyen parazit azaltma potansiyelini düzenlemek, otomatik güncelleme programını değiştirmek ve atama için kullanılan kanal grubunu yeniden yapılandırmak için *Gelişmiş Ayarları* kullanabilirsiniz.

Tablo 8.3 Gelişmiş Ayarlar

Alan	Açıklama
<i>Advanced (Gelişmiş)</i>	"Advanced" (Gelişmiş) açma/kapatma düğmesine tıklayarak kanal planlama algoritmasının zamanlamasını ve ayrıntılarını değiştirmenizi sağlayan ekran ayarlarını görüntüleyip gizleyebilirsiniz. Bu ayarlar varsayılan olarak gizlidir .
<i>Change channels if interference is reduced by at least __ (Parazit en az __ azaltıldığında kanalları değiştir)</i>	Önerilen planın uygulanması için gereken minimum parazit azaltma oranını belirtin. Varsayılan değer yüzde 25 'tir. %25 - %75 arası yüzde oranları arasında seçim yapmak için açılır menüyü kullanın. Bu ayar, yeniden kanal atama için bir geçit faktörü belirlemenizi sağlayarak ağın verimlilikteki küçük artışlar için sürekli olarak kesintiye uğramasını önler. Örneğin, kanal parazitinin %75 azaltılması gerekiyorsa ve önerilen kanal atamaları parazitini yalnızca %30'unu azaltıyorsa kanallar yeniden atanmaz. Ancak, en az kanal paraziti oranını %25 olarak değiştirip Update (Güncelle) düğmesine tıkladığınızda önerilen kanal planı uygulanır ve kanallar gerektiği şekilde yeniden atanır.
<i>Determine if there is better set of channel settings every __ (her __ sıklıkla daha iyi bir kanal grubu ayarının olup olmadığını sapt)</i>	Otomatik güncelleme programını belirlemek için açılır menüyü kullanın. Zaman aralıkları "1 Dakika" ile "6 Ay" arasındadır. Varsayılan ayar "1 Saattir" (Her saatte bir kanal kullanımı yeniden değerlendirilir ve sonucunda elde edilen kanal planı uygulanır).

Tablo 8.3 Gelişmiş Ayarlar (Devamı)

Alan	Açıklama
<i>Use these channels when applying channel assignments (Kanal atamalarını uygularken bu kanalları kullan)</i>	<p>Belirli bir bantta ("b/g" ya da "a") parazitsiz bir kanallar grubu seçin. Seçenekler şunlardır:</p> <ul style="list-style-type: none">• b/g - 1-6-11 kanalları• b/g - 1-4-8-11 kanalları• a <p>IEEE 802.11b/802.11g modları (802.11 b/g) 1-11 arası kanalların kullanılmasını destekler. "b/g" telsiz bandı için klasik parazitsiz kanallar grubu 1, 6, 11'dir. 1, 4, 8, 11 kanalları minimum çakışma oluşturur.</p> <p>IEEE 802.11a modu ardışık olmayan daha geniş bir kanal grubunu (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165) destekler. Tüm "a" bandı kanalları parazitsizdir.</p>
<i>Apply channel modifications even when the network is busy (Kanal değişikliklerini ağ meşgul olsa bile uygula)</i>	<p>Bu ayarı etkinleştirmek ya da devre dışı bırakmak için tıklayın.</p> <p>Onay işareti, ayarın etkinleştirildiğini ve kanal değişikliklerinin ağ meşgul olsa bile uygulanacağını gösterir. Bu seçenek işaretlenmemişse kanal değişiklikleri meşgul bir ağa uygulanmaz.</p> <p>Bu ayar (ve parazit azaltma ayarı), kanalları yeniden atama işleminin ağ performansı üzerindeki etkisi ile meşgul bir zamanda istemcilerde neden olacağı kesintileri karşılaştırarak fayda/zarar oranını belirlemenize yardımcı olmak için tasarlanmıştır.</p>

8.3.4.1 Gelişmiş Ayarları Güncelleme

Bu ayarları uygulamak için *Advance Settings* (Gelişmiş Ayarlar) bölümünde **Update** (Güncelle) düğmesine tıklayın.

Gelişmiş Ayarlar uygulandıkları anca geçerlilik kazanır ve otomatik kanal yönetiminin yapılış biçimini etkiler. (Yeni minimum parazit azaltma oranı, programlanan ayarlama aralığı, kanal grubu ve ağ meşgul ayarları otomatik ve manuel güncellemelerde göz önünde bulundurulur).

KOMŞU KABLOSUZ AĞLAR

9

9.1 Komşu Kablosuz Ağlar Ekranına Gitme	85
9.2 Komşu Kablosuz Ağlarla İlgili Bilgileri Anlama	85
9.3 Komşu Kablosuz Ağları Görüntüleme	86
9.4 Bir Küme Üyesinin Ayrıntılarını Görüntüleme	88

Wireless Neighborhood (Komşu Kablosuz Ağlar) ekranı kümedeki erişim noktasının menzilineki erişim noktalarını gösterir. Bu sayfa, komşu erişim noktalarının her birine ait tanımlayıcı bilgileri (SSID'leri ve MAC adresleri), küme durumunu (hangi AP'ler üye, hangileri değil) ve her AP'nin yayın yaptığı kanal, sinyal gücü vb. gibi istatistik bilgileri dahil, komşu erişim noktaları hakkında ayrıntılı bilgi verir.

9.1 Komşu Kablosuz Ağlar Ekranına Gitme

Komşu Kablosuz Ağları görüntülemek için **Cluster > Wireless Neighborhood** (Küme > Komşu Kablosuz Ağlar) sekmesine tıklayın.

Şekil 9.1 Kümede Olan ve Olmayan Komşu AP'ler

View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ☐ In cluster ☐ Not in cluster ☒ Both

	Cluster	
	10.10.100.245 00:00:04:7F:00:00 (Vicky's Office - lower shelf)	10.10.100.238 00:0C:41:16:A3:12 (Vicky's Office - top shelf)
Neighbors (11)		
Vicky's AP-2 (WIP-bld-48b)		54
Vicky's AP-2 (WIP-bld-48b)	75	
IONEGA_NAS	29	46
TEKLOGIX...	20	
novatec	23	
Pronghorn 2.0.2		11
tsunami	18	
tsunami	70	41
Radio 1 - SSID 1	36	41
BradLabNetwork	5	19
Ray's GW 7001 2.0.3		11

Clustered

2 Access Points

3 User Accounts

Wireless Neighborhood shows those access points within range of any access point in the cluster.

This page provides a detailed view of neighboring access points including identifying information (SSIDs and MAC addresses) for each, cluster status (which are members and non-members), and statistical information such as the channel each AP is broadcasting on, signal strength, and so forth.

[More ...](#)

9.2 Komşu Kablosuz Ağlarla İlgili Bilgileri Anlama

Komşu Kablosuz Ağlar ekranı her küme üyesinin menzilineki tüm erişim noktalarını gösterir, hangi erişim noktalarının hangi küme üyelerinin menziline olduğunu görüntüler ve küme üyeleriyle küme üyesi olmayan AP'leri ayırt eder.

Komşu Kablosuz Ağlar ekranı, her komşu erişim noktası için tanımlayıcı bilgileri (**SSID** ya da Ağ Adı, **IP Address (IP Adresi)**, **MAC** adresi) ve telsiz istatistiklerini (sinyal gücü, kanal, uyarı aralığı) gösterir. Seçtiğiniz bir AP'nin telsiz menzilineki AP'ler hakkında daha fazla istatistik bilgisi için AP'ye tıklayabilirsiniz.

Komşu Kablosuz Ağlar Ekranı:

- Kablosuz bir etki alanındaki beklenmedik (ya da *rogue*) erişim noktalarını algılayıp yerlerini belirleyerek oluşabilecek riskleri sınırlamak için aksiyon almanızı sağlar.
- Kapsama beklentilerini doğrular. Hangi AP'lerin hangi sinyal gücündeysen diğer AP'ler tarafından görülebildiğini belirleyerek AP dağıtımının planlama hedeflerinizi karşıladığını doğrulayabilmenizi sağlar.
- Hataları algılar. Kapsama düzenindeki beklenmedik değişiklikler renk kodlarıyla oluşturulan tabloda tek bakışta görülebilir.

9.3 Komşu Kablosuz Ağları Görüntüleme

Komşu Kablosuz Ağlarla ilgili ayrıntılı bilgiler aşağıda verilmiştir.

Tablo 9.1 Komşu Kablosuz Ağlarla İlgili İstatistikler

Alan	Açıklama
<i>Display Neighboring APs</i> (Komşu AP'leri Göster)	Görünümü değiştirmek için aşağıdaki radyo düğmelerinden birine tıklayın: <ul style="list-style-type: none">• <i>In cluster</i> (Kümedekiler) - Yalnızca küme üyesi olan komşu AP'leri gösterir.• <i>Not in cluster</i> (Kümede olmayanlar) - Yalnızca küme üyesi olmayan komşu AP'leri gösterir.• <i>Both</i> (İkisi de) - Küme üyesi olan ve olmayan tüm komşu AP'leri gösterir.
<i>Cluster (Küme)</i>	Tablonun üst kısmındaki "Cluster" (Küme) listesi, kümedeki tüm erişim noktalarının IP adreslerini gösterir. (Bu liste "Erişim Noktası Yönetimine Gitme", sayfa 55'teki <i>Cluster > Access Points</i> [Küme Erişim Noktaları] sekmesinde yer alan küme üyeleri listesinin aynısıdır). Kümede yalnızca bir AP varsa burada AP'nin "kendi içinde kümelendiğini" ifade eden tek bir IP adresi sütunu görüntülenir. Belirli bir AP ile ilgili daha fazla ayrıntı görüntülemek için AP'nin IP adresine tıklayabilirsiniz (bkz. Şekil 9.2, sayfa 88).

Tablo 9.1 Komşu Kablosuz Ağlarla İlgili İstatistikler (Devamı)

Alan

Açıklama

Neighbors (Komşular)

Kümelenen AP'lerin biri ya da birden fazlasıyla komşu olan erişim noktaları, soldaki sütunda SSID'lerine (Ağ Adı) göre listelenmiştir. Bir küme üyesinin komşusu olduğu algılanan bir erişim noktası da bir küme üyesi olabilir. Kendileri de küme üyesi olan komşular, her zaman listenin başında yer alır, konum göstergesi içerir ve üzerinde kalın bir çubukla gösterilir.

Komşular listesindeki her AP'nin sağ tarafında yer alan renkli çubuklar, IP adresleri sütunun başında gösterilen küme üyeleri tarafından algılanan her bir komşu AP'nin sinyal gücünü gösterir.

Bu AP'yi (bir küme üyesi), IP adresi 10.10.100.246 olan (sinyal gücü 54) AP'ler görebilir...

...ancak IP adresi 10.10.100.223 olanlar göremez.

Neighbors (88)	Cluster		
	10.10.100.246 (not set)	10.10.100.223 (not set)	10.10.100.213 (not set)
TEKLOGIX... (not set)		2	48
TEKLOGIX... (not set)			
TEKLOGIX... (not set)	54	0	
TEKLOGIX... (not set)	34	5	26
TEKLOGIX... (not set)	22		50
Brad Lab 105	20	18	27
wi-fi-a	46		34
guest	4	6	48
int	4	5	48
g10_wgt624_guest	21	14	33

- **Lacivert Çubuk** - Lacivert çubuk ve yüksek sinyal gücü (örneğin 50), IP adresi sütunun üst kısmında listelenen AP'nin gördüğü Komşudan algılanan iyi sinyal gücünü belirtir.
- **Mavi Çubuk** - Mavi çubuk ve daha düşük sinyal gücü (örneğin 20 veya daha az), IP adresi sütunun üst kısmında listelenen AP'nin gördüğü Komşudan algılanan orta ya da zayıf sinyal gücünü belirtir.
- **Beyaz Çubuk** - Beyaz çubuk ve 0 rakamı, küme üyelerinden biri tarafından algılanan bir komşu AP'nin, IP adresi sütunun üst kısmında listelenen AP tarafından algılanmadığını belirtir.
- **Açık Gri Çubuk** - Açık gri çubuk ve sinyal gücünü gösteren bir sayının olmaması, bir Komşunun diğer küme üyeleri tarafından algılandığını ancak IP adresi sütunun üst kısmında listelenen AP tarafından algılanmadığını belirtir.
- **Koyu Gri Çubuk** - Koyu gri çubuk ve sinyal gücünü gösteren bir sayının olmaması, IP adresi sütunun üst kısmında listelenen AP'nin *bu AP* olduğunu (AP'nin kendisini ne kadar iyi algıladığını göstermek mümkün olmadığı için) belirtir.

9.4 Bir Küme Üyesinin Ayrıntılarını Görüntüleme

Küme üyesi olan bir AP ile ilgili ayrıntıları görüntülemek için sayfanın üst kısmında yer alan küme üyesi **IP adresine** tıklayın.

Şekil 9.2 Küme Üyesi AP ile İlgili Ayrıntılar


View neighboring access points


Wireless Neighborhood...


The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ☐ In cluster ☐ Not in cluster ☒ Both

	Cluster	
	<u>10.10.100.245</u> 00:00:04:7F:00:00 (Vicky's Office - lower shelf)	<u>10.10.100.238</u> 00:0C:41:16:A3:12 (Vicky's Office - top shelf)
Neighbors (10)		
Vicky's Network (WIP-bld-48b)		45
Vicky's Network (WIP-bld-48b)	51	
IOMEGA_NAS	37	49
TEKLOGIX...	22	
novatec		
Pronghorn 2.0.2		20
tsunami	18	10
tsunami	54	42
BradLabNetwork	11	
Ray's GW 7001 2.0.3		17

Clustered 

2 Access Points 

3 User Accounts 

Neighbor Details

10.10.100.245						
SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
IOMEGA_NAS	00:03:2F:27:4E:EE	1	10	37	100	74203
TEKLOGIX...	00:0C:41:0A:30:3E	6	10	22	100	74203
Vicky's Network (WIP-bld-48b)	00:0C:41:16:A3:12	2	10	51	100	74203
novatec	00:0E:81:01:01:1A	6	10	-4	100	74203
tsunami	00:13:5F:56:E8:00	10	10	18	100	74203
tsunami	00:14:A8:36:28:40	4	10	54	100	74203

Aşağıdaki tabloda, seçilen bir AP ile ilgili ayrıntılar açıklanmaktadır.

Tablo 9.2 Erişim Noktası İstatistikleri

Alan	Açıklama
<i>SSID</i>	<p>Erişim noktasının <i>Hizmet Kümesi Tanımlayıcısıdır (SSID)</i>.</p> <p>SSID, en çok 32 karakterden oluşan ve bir kablosuz yerel alan ağını benzersiz biçimde tanımlayan alfanümerik bir dizedir. Ağ Adı olarak da bilinir.</p> <p>SSID, Basic Settings (Temel Ayarlar) bölümünde (bkz. Bölüm 5: "Temel Ayarları Yapılandırma") ya da <i>Manage > 802.11 Settings</i> (Yönet > 802.11 Ayarları) bölümünde ayarlanır (bkz. Bölüm 13: "Kablosuz Arabiriminin Ayarlama").</p> <p>Aynı erişim noktasındaki bir Konuk ağı ve Dahili ağ her zaman iki farklı ağ adına sahip olmalıdır.</p>
<i>MAC Address</i> (MAC Adresi)	<p>Komşu erişim noktasının MAC adresini gösterir.</p> <p>MAC adresi bir ağıdaki her düğümü benzersiz biçimde tanımlayan bir donanım adresidir.</p>
<i>Channel</i> (Kanal)	<p>Erişim noktasının o an hangi kanalda yayın yaptığını gösterir.</p> <p>Kanal, telsizin alma/verme için kullandığı telsiz spektrumu kısmını tanımlar.</p> <p>Kanal, <i>Manage > 802.11 Advanced Settings</i> (Yönet > 802.11 Gelişmiş Ayarları) bölümünde ayarlanır. (Bkz. Bölüm 16: "802.11 Telsiz Ayarlarını Yapılandırma".)</p>
<i>Rate (Hız)</i>	<p>Erişim noktasının o anda hangi hızda aktarım yaptığını (megabit/saniye cinsinden) gösterir.</p> <p>Geçerli hız her zaman <i>Rates</i> (Hızlar) kısmında gösterilen Desteklenen Hızlardan biridir.</p>
<i>Signal (Sinyal)</i>	<p>Bu erişim noktasından yayılan ve desibel (Db) cinsinden ölçülen telsiz sinyalinin gücünü gösterir.</p>
<i>Beacon Interval</i> (Uyarı Aralığı)	<p>Bu erişim noktasının kullandığı Uyarı aralığını gösterir.</p> <p>Uyan anonsları, kablosuz ağların varlığını duyurmak için erişim noktası tarafından düzenli aralıklarla iletilir. Varsayılan olarak her 100 milisaniyede bir (ya da her 10 saniyede bir) uyarı anonsu gönderilir.</p> <p>Uyarı Aralığı, <i>Manage > 802.11 Advanced Settings</i> (Yönet > 802.11 Gelişmiş Ayarları) bölümünde ayarlanır. (Bkz. Bölüm 16: "802.11 Telsiz Ayarlarını Yapılandırma".)</p>
<i>Capability</i> (Özellik)	<p>İkili sisteme dönüştürüldüğünde her IEEE 802.11 özelliğini ya da işlevini belirten ve bu erişim noktasında "açık" mı yoksa "kapalı" mı olduğunu gösteren onaltılık sistemdeki bir sayıdır.</p>
<i>Beacon Age</i> (Uyarının Üzerinden Geçen Süre)	<p>Bu erişim noktasından gönderilen en son uyarının tarihini ve saatini gösterir.</p>

10.1 Kablosuz Ağlardaki Güvenlik Sorunlarını Anlama	93
10.1.1 Hangi Güvenlik Modunu Kullanmalıyım?	93
10.1.2 Güvenlik Modlarının Anahtar Yönetimi, Kimlik Doğrulama ve Şifreleme Algoritmaları Açısından Karşılaştırılması	94
10.1.2.1 Şifresiz Mod (Güvenli Değil) Ne Zaman Kullanılmalı?	94
10.1.2.2 Statik WEP Ne Zaman Kullanılmalı?	95
10.1.2.3 IEEE 802.1x Ne Zaman Kullanılmalı?	96
10.1.2.4 Kişisel WPA Ne Zaman Kullanılmalı?	97
10.1.2.5 Kurumsal WPA Ne Zaman Kullanılmalı?	98
10.1.3 SSID Yayınını Engellemek Güvenliği Artırır Mı?	99
10.1.4 İstasyon Ayırma Ağı Nasıl Korur?	100
10.2 Güvenlik Ayarlarını Yapılandırma	100
10.2.1 SSID Yayını, İstasyon Ayırma ve Güvenlik Modu	101
10.2.2 Güvenlik Modları	102
10.2.2.1 Yok (Düz metin)	102
10.2.2.2 Statik WEP	103
10.2.2.3 IEEE 802.1x	108
10.2.2.4 WPA Kişisel	111
10.2.2.5 WPA Kurumsal	113
10.3 Ayarları Güncelleme	118

Aşağıdaki bölümler 9160 G2 Kablosuz Ağ Geçidi cihazında Güvenlik ayarlarının nasıl yapılandırıldığını açıklamaktadır.

10.1 Kablosuz Ağlardaki Güvenlik Sorunlarını Anlama

Kablosuz ortamları doğaları gereği kablolu ortamlardan daha az güvenlidir. ÖrneĖin bir Ethernet Ağ Arabirim Kartı (**NIC**), paketlerini koaksiyel veya çift bükümlü kablo gibi fiziksel bir ortam aracılığıyla aktarır. Kablosuz bir NIC, kablosuz bir LAN ağına fiziksel erişim ya da karmaşık bir ekipman olmadan kolayca dokunulmasını sağlayarak telsiz sinyallerini kablosuz olarak yayınlar. Bir dizüstü bilgisayar, kablosuz NIC'si ve biraz bilgi olan bir hacker, kablosuz ağınızın güvenliğini kolayca tehlikeye atabilir. Üstelik bunu yapmak için erişim noktasının normal menziline olmasına gerek yoktur. Hacker, istemci üzerinde gelişmiş bir anten kullanarak birkaç mil öteden ağa bağlanabilir.

9160 G2 Kablosuz Ağ Geçidi, kablosuz altyapınıza yalnızca istenilen kullanıcıların erişmesini sağlamak için bir dizi kimlik doğrulama ve şifreleme yöntemi sunar. Her bir güvenlik moduyla ilgili ayrıntılar aşağıdaki bölümlere açıklanmıştır.

Ayrıca ilgili bir konu başlığı olan Ek B: “Kablosuz İstemcilerde/RADIUS Sunucusunda Güvenlik Ayarları” kısmına da bakın.

10.1.1 Hangi Güvenlik Modunu Kullanmalıyım?

Genellikle, Dahili ağınızda yer alan, ortamınıza uygun olan en güçlü güvenlik modunu kullanmanızı öneriyoruz. Erişim noktasında güvenliĖi yapılandırırken önce güvenlik modunu seçmeniz gerekir. Ardından bazı modlarda bir kimlik doğrulama algoritması belirlemeniz ve belirtilen güvenlik modunu kullanmayan istemcilerin erişim noktasıyla ilişkilendirilmesine izin verip vermeyeceğinize karar vermeniz gerekir.

CCMP (AES) şifreleme algoritmasını kullanan *Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmetini (RADIUS)* içeren *Wi-Fi Korunmalı Erişim (WPA)*, mümkün olan en iyi veri korumasını sağlar ve tüm istemci istasyonlarının WPA doğrulaması isteyen öğeler içerdii durumlarda kesinlikle en iyi tercihtir. Ancak, geriye dönük uyumluluk ve istemcilerle ya da diğeri erişim noktalarıyla birlikte çalışma sorunları, RADIUS'u içeren WPA'yı farklı bir şifreleme algoritmasıyla yapılandırmanızı veya diğeri güvenlik modlarından birini seçmenizi gerektirebilir.

Bununla birlikte, bazı ağ türlerinde güvenlik bu denli öncelikli olmayabilir. Konuk ağlarında olduğu gibi yalnızca Internet ve yazıcı erişimi sağlıyorsanız güvenlik modunu *None (Plain-text)* (Yok - düz metin) olarak ayarlamanız uygun olur. İstemcilerin ağınıza tesadüfen bulmasını ve ağınıza bağlanmasını önlemek için SSID yayınını devre dışı bırakarak ağınıza adının belirtilmemesini sağlayabilirsiniz. Ağın hassas bilgilere erişimi yeteri kadar önlenmişse bu koruma seviyesi bazı durumlar için yeterlidir. Bu koruma seviyesi, konuk ağlar için sunulan tek seviyedir ve önceliğin istemcilerin ağa bağlanmasını mümkün olduğunca kolay hale getirdiği diğer senaryolar için doğru uygunluk dengesi olabilir. (Bkz. “SSID Yayınını Engellemek Güvenliği Artırır Mı?”, sayfa 99)

Aşağıda, bir modu diğerinden daha güvenli hale getiren faktörler, sunulan her modla ilgili açıklamalar ve hangi modun ne zaman kullanılacağıyla ilgili bilgiler yer almaktadır.

10.1.2 Güvenlik Modlarının Anahtar Yönetimi, Kimlik Doğrulama ve Şifreleme Algoritmaları Açısından Karşılaştırılması

Bir güvenlik protokolünün verimliliğini belirleyen üç ana faktör şunlardır:

- Protokolün anahtarları yönetme şekli.
- Protokolde entegre bir kullanıcı kimlik doğrulamasının olup olmaması.
- Protokolün verileri şifrelerken/verilerin şifresini çözerken kullandığı şifreleme algoritması ya da formülü.

Aşağıda, 9160 G2 Kablosuz Ağ Geçidi cihazında bulunan güvenlik modlarının listesinin yanı sıra, her modda kullanılan anahtar yönetimi, kimlik doğrulama ve şifreleme algoritmalarının açıklamaları yer almaktadır. Ayrıca bir modun diğer moddan daha uygun olduğu durumlarla ilgili bazı önerilerimizi de içermektedir.

- “Şifresiz Mod (Güvenli Değil) Ne Zaman Kullanılmalı?”, sayfa 94.
- “Statik WEP Ne Zaman Kullanılmalı?”, sayfa 95.
- “IEEE 802.1x Ne Zaman Kullanılmalı?”, sayfa 96.
- “Kişisel WPA Ne Zaman Kullanılmalı?”, sayfa 97.
- “Kurumsal WPA Ne Zaman Kullanılmalı?”, sayfa 98.

10.1.2.1 Şifresiz Mod (Güvenli Değil) Ne Zaman Kullanılmalı?

Güvenlik modunu varsayılan olarak *None (Plain-text)* (Yok - düz metin) seçeneğine ayarlamak hiçbir güvenlik sağlamaz. Bu modda veri şifrelenmez ancak ağda "düz metin" olarak gönderilir. Anahtar yönetimi, veri şifreleme ya da kullanıcı kimlik doğrulaması kullanılmaz.

Öneriler

Şifresiz mod, yani Yok (Düz Metin) modu güvenli olmadığı için Dahili ağda düzenli olarak kullanılması önerilmez. Bu mod, doğası gereği güvenli olmayan bir LAN olan ve Dahili LAN'daki hassas bilgilerden her zaman sanal veya fiziksel olarak ayrı olan Konuk ağında çalıştırılabileceğiniz tek moddur.

Bu nedenle *None (Plain-text)* (Yok - Düz Metin) güvenlik modunu yalnızca Konuk ağında; Dahili ağda ise yalnızca ilk kurulum, test veya sorun çözme sırasında kullanın.

Ayrıca Bkz.

Şifresiz güvenlik modunu yapılandırma hakkında bilgi için bkz. “Yok (Düz metin)”, sayfa 102.

10.1.2.2 Statik WEP Ne Zaman Kullanılmalı?

Statik *Kablolu Eş Değer Gizlilik (WEP)*, 802.11 kablosuz ağlar için bir veri şifreleme protokolüdür. Ağdaki tüm kablosuz istasyonlar ve erişim noktaları, veri şifreleme için statik 64 bit (40 bit gizli anahtar + 24 bit başlatma vektörü [IV]) ya da 128 bit (104 bit gizli anahtar + 24 bit IV) Paylaşılan Anahtarla yapılandırılır.

Tablo 10.1 Statik WEP Güvenlik Modu

Anahtar Yönetimi	Şifreleme Algoritması	Kullanıcı Kimlik Doğrulaması
Statik WEP , yönetici tarafından sağlanan sabit bir anahtar kullanır. WEP anahtarları farklı yuvalara yerleştirilir (9160 G2 Kablosuz Ağ Geçidi cihazında dört adede kadar). İstemci istasyonlarının erişim noktasındaki verilere erişmesi için aynı yuvaya aynı anahtarın yerleştirilmesi gerekir.	RC4 şifre dizisi, her 802.11 çerçevesinin çerçeve gövdesini ve döngüsel artıklık denetimini (CRC) şifrelemek için kullanılır.	Kimlik Doğrulama Algoritması "Shared Key" (Paylaşılan Anahtar) olarak ayarlandığında bu protokol temel bir kullanıcı kimlik doğrulaması sunar. Ancak Kimlik Doğrulama Algoritması "Open System" (Açık Sistem) olarak ayarlandığında herhangi bir kimlik doğrulaması gerçekleşmez. Algoritma "Both" (İkisi de) olarak ayarlandığında yalnızca WEP istemcilerinin kimlik onaylaması yapılır.

Öneriler

Statik WEP, Ethernet bağlantısı üzerinden şifrelenmemiş veri göndermeye eşdeğer bir güvenlik sunmak üzere tasarlanmıştır ancak bu modda önemli hatalar vardır ve hedeflenen bu güvenlik seviyesini bile sağlayamamaktadır.

Bu yüzden **Statik WEP'in güvenli mod olarak kullanılması önerilmez**. Statik WEP modunu yalnızca birlikte çalışabilirlik sorunlarından dolayı elinizdeki tek seçenek olduğunda ve ağınzındaki verilerin başkasının eline geçmesinden kaygılanmadığınız durumlarda kullanın.

Ayrıca Bkz.

Statik WEP güvenlik modunu yapılandırma hakkında bilgi için bkz. “Statik WEP”, sayfa 103.

10.1.2.3 IEEE 802.1x Ne Zaman Kullanılmalı?

IEEE 802.11, LAN üzerinden EAP Kuşatma (EAPOL) protokolü kullanılarak Genişletilebilir Kimlik Doğrulama Protokolünün (**EAP**) bir 802.11 kablosuz ağ üzerinden geçirilmesi standardıdır. Bu, Statik WEP'den daha yeni ve daha güvenli bir standarttır.

Tablo 10.2 IEEE 801.1x Güvenlik Modu

Anahtar Yönetimi	Şifreleme Algoritması	Kullanıcı Kimlik Doğrulaması
IEEE 802.1x, periyodik olarak yenilenen ve dinamik şekilde oluşturulan anahtarlar sunar. Her istasyon için farklı Tek yönlü yayın anahtarı vardır.	RC4 şifre dizisi, her 802.11 çerçevesinin çerçeve gövdesini ve döngüsel artıklık denetimini (CRC) şifrelemek için kullanılır.	IEEE 802.1x modu sertifikalar, Kerberos ve RADIUS sunuculu açık anahtar kimliği doğrulama gibi çeşitli kimlik doğrulama yöntemlerini destekler. 9160 G2 Kablosuz Ağ Geçidi cihazına gömülü RADIUS sunucusunu ya da harici bir RADIUS sunucusu kullanma seçeneğiniz vardır. Gömülü RADIUS sunucusu Korumalı EAP (PEAP) ve MSCHAP V2'yi destekler.

Öneriler

IEEE 802.1x modunda anahtarlar dinamik biçimde oluşturulduğu ve periyodik olarak değiştirildiği için bu mod Statik WEP modundan daha iyi bir seçenektir. Ancak kullanılan şifreleme algoritması Statik WEP'de kullanılan algoritmaya aynı olduğundan **Wi-Fi Korumalı Erişim (WPA)** veya **WPA2**'de kullanılan **TKIP** ve **CCMP (AES)** gibi daha gelişmiş şifreleme yöntemleri kadar güvenli değildir.

Ayrıca, desteklenen kimlik doğrulama yöntemlerinin çeşitliliği ve standart bir uygulama yönteminin olmaması gibi sebeplerle uyumluluk konusunda sorun yaşanabilir.

Bu nedenle IEEE 802.1x modu, **Wi-Fi Korumalı Erişim (WPA)** ya da **WPA2** kadar güvenli bir çözüm değildir. Bazı istemci istasyonlarınızda WPA olmadığından dolayı **WPA**'yı kullanamıyorsanız IEEE 802.1x modunu kullanmak yerine **WPA Kurumsal modunu** kullanmak daha iyi bir çözümdür.

Ağınızda harici bir RADIUS sunucunuz varsa AP'deki gömülü RADIUS sunucusunu kullanmak yerine bu sunucuyu kullanmanızı öneririz. Harici bir RADIUS sunucusu, yerel kimlik doğrulama sunucusundan daha iyi bir güvenlik sağlar.

Ayrıca Bkz.

IEEE 802.1x güvenlik modunu yapılandırma hakkında bilgi için bkz. “IEEE 802.1x”, sayfa 108.

10.1.2.4 Kişisel WPA Ne Zaman Kullanılmalı?

Wi-Fi Korumalı Erişim Kişisel *Önceden Paylaşılan Anahtar (PSK)*; *Gelişmiş Şifreleme Algoritması (AES)*, *Sayaç Modu/CBC-MAC Protokolü (CCMP)* ve *Geçici Anahtar Bütünlüğü Protokolü (TKIP)* mekanizmalarını içeren Wi-Fi İttifakı IEEE **802.11h** standardının bir uygulamasıdır. Bu mod, RADIUS içeren WPA 2 ile aynı şifreleme algoritmasını sunar ancak kullanıcı kimlik doğrulaması için bir RADIUS sunucusu entegre edemez.

Bu güvenlik modu, yalnızca orijinal **WPA**'yi destekleyen kablosuz istemciler için geriye dönük uyumluluk sunar.

Tablo 10.3 WPA Kişisel Güvenlik Modu

Anahtar Yönetimi	Şifreleme Algoritmaları	Kullanıcı Kimlik Doğrulaması
WPA Kişisel güvenlik modu, periyodik olarak yenilenen ve dinamik şekilde oluşturulan anahtarlar sunar. Her istasyon için farklı Tek yönlü yayın anahtarı vardır.	<ul style="list-style-type: none">Geçici Anahtar Bütünlüğü Protokolü (TKIP).Sayaç Modu/CBC-MAC Protokolü (CCMP) <i>Gelişmiş Şifreleme Standardı (AES)</i>.	Önceden Paylaşılan (PSK) bir anahtarın kullanılması, WEP 'deki paylaşılan anahtarların kullanıcı kimlik doğrulamasına benzer bir kullanıcı kimlik doğrulaması sağlar.

Öneriler

WPA Kurumsal seçeneği mevcutken WPA Kişisel modunun 9160 G2 Kablosuz Ağ Geçidi ile kullanılması önerilmez.

WPA Kurumsal modunu kullanmanızı engelleyecek birlikte çalışabilirlik sorunlarınıza yoksa WPA Kişisel yerine WPA Kurumsal modunu kullanmanızı öneririz.

Örneğin, ağınızdaki bazı cihazlar bir **RADIUS** sunucusuyla konuşan **EAP** içeren WPA ya da WPA2'yi desteklemeyebilir. Gömülü yazıcı sunucuları ya da uygulama için çok az alana sahip olan diğer küçük istemci cihazları RADIUS'u desteklemeyebilir. Bu gibi durumlarda WPA Kişisel modunu kullanmanızı öneririz.

Ayrıca Bkz.

Bu güvenlik modunu yapılandırma hakkında bilgi için bkz. “WPA Kişisel”, sayfa 111.

10.1.2.5 Kurumsal WPA Ne Zaman Kullanılmalı?

Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmetini (RADIUS) içeren Wi-Fi Korumalı Erişim Kurumsal; Gelişmiş Şifreleme Standardı (AES), Sayaç Modu/CBC-MAC Protokolü (CCMP) ve Geçici Anahtar Bütünlüğü Protokolü (TKIP) mekanizmalarını içeren Wi-Fi İttifakı IEEE 802.11h standardının bir uygulamasıdır. Bu mod, kullanıcıların kimliklerinin doğrulanması için bir RADIUS sunucusunun kullanılmasını gerektirir. WPA Kurumsal, kablosuz ağlar için mevcut en iyi güvenliği sağlar.

Bu güvenlik modu, yalnızca orijinal **WPA**'yi destekleyen kablosuz istemciler için geriye dönük uyumluluk da sunar.

Tablo 10.4 WPA Kurumsal Güvenlik Modu

Anahtar Yönetimi	Şifreleme Algoritmaları	Kullanıcı Kimlik Doğrulaması
WPA Kurumsal güvenlik modu, periyodik olarak yenilenen ve dinamik şekilde oluşturulan anahtarlar sunar. Her istasyon için farklı Tek yönlü yayın anahtarı vardır.	<ul style="list-style-type: none"> Geçici Anahtar Bütünlüğü Protokolü (TKIP). Sayaç Modu/CBC-MAC Protokolü (CCMP) Gelişmiş Şifreleme Standardı (AES). 	Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmeti (RADIUS) 9160 G2 Kablosuz Ağ Geçidi cihazına gömülü RADIUS sunucusunu ya da harici bir RADIUS sunucusu kullanma seçeneğiniz vardır. Gömülü RADIUS sunucusu Korumalı EAP (PEAP) ve MSCHAP V2'yi destekler.

Öneriler

WPA Kurumsal modu **önerilen moddur**. WPA modlarıyla kullanılan **CCMP (AES)** ve **TKIP** şifreleme algoritmaları, Statik **WEP** ya da IEEE 802.1x modları için kullanılan **RC4** algoritmasından çok daha iyidir. Bu nedenle, mümkün olan her durumda CCMP (AES) ya da TKIP kullanılmalıdır. Tüm WPA modları bu şifreleme yöntemlerini kullanmanıza izin verir, bu yüzden WPA seçeneği mevcutken diğer güvenlik modlarının yerine WPA'yı kullanmanızı öneririz. Ayrıca, bu modun kullanıcı kimlik doğrulaması için RADIUS sunucusuyla birlikte çalışması, WPA Kişisel moduna kıyasla avantaj sağlar.

Ağınızda harici bir RADIUS sunucunuz varsa AP'deki gömülü RADIUS sunucusunu kullanmak yerine bu sunucuyu kullanmanızı öneririz. Harici bir RADIUS sunucusu, yerel kimlik doğrulama sunucusundan daha iyi bir güvenlik sağlar.

WPA Kurumsal güvenlik moduyla kullanılan seçenekler arasında seçim yapmak için aşağıdaki talimatları izleyin:

1. Kablosuz bir ağda kullanabileceğiniz en iyi güvenlik, CCMP (AES) şifreleme algoritmasıyla birlikte kullanılan WPA Kurumsal modudur. AES, birden çok ağ katmanı için kullanılabilen simetrik 128 bit blok veri şifreleme tekniğidir. Bu teknik, şu an kablosuz ağlar için mevcut olan en etkili şifreleme sistemidir. Ağdaki tüm istemciler veya diğer AP'ler WPA/CCMP ile uyumluysa bu şifreleme algoritmasını kullanın. (Tüm istemciler WPA2 ile uyumluysa yalnızca WPA2 istemcilerini desteklemeyi seçin.)
2. İkinci en iyi seçenek, şifreleme algoritması TKIP ve CCMP olarak ayarlanan WPA Kurumsal modudur. Bu mod, CCMP ilişkili olmayan WPA istemci istasyonlarına izin verir, Çoklu gönderim ve Yayın çerçevelerinin şifrenmesi için TKIP kullanır ve Tek yönlü yayın (AP'den tek istasyona) çerçeveleri için istemcilerin CCMP ya da TKIP arasında seçim yapmasını sağlar. Bu WPA yapılandırması, güvenlikten belirli bir derece ödün vererek daha fazla birlikte çalışabilirlik sağlar. CCMP'yi destekleyen istemci istasyonları Tek yönlü yayın çerçeveleri için bu yapılandırmayı kullanabilir. "Both" (İkisi de) şifreleme algoritması ayarlıyken AP'den istasyona birlikte çalışabilirlik sorunlarıyla karşılaşıyorsanız TKIP'yi seçmeniz gerekir. (Sonraki seçeneğe bakın.)
3. Üçüncü en iyi seçenek, WPA Kurumsal modunun **TKIP** şifreleme algoritmasıyla kullanılmasıdır. Bazı istemciler hem CCMP hem de TKIP ile birlikte çalışabilirlik sorunları yaşar. Bu sorunu yaşıyorsanız şifreleme algoritması olarak TKIP'yi seçin. Bu, standart bir WPA modudur ve istemci Kablosuz yazılımı güvenlik özelliklerini içeren en fazla birlikte çalışabilirlik sunan moddur. TKIP, **Wi-Fi WPA** sertifikasyonunda test edilen tek şifreleme algoritmasıdır.

Ayrıca Bkz.

Bu güvenlik modunu yapılandırma hakkında bilgi için bkz. "WPA Kurumsal", sayfa 113.

10.1.3 SSID Yayını Engellemek Güvenliği Artırır mı?

İstasyonların erişim noktasını otomatik olarak keşfetmemesi için bu yayını kaldırabilirsiniz (engelleyebilirsiniz). AP'nin SSID yayını kaldırıldığında ağ adı, istemci istasyonundaki Mevcut Ağlar Listesinde görülmez. İstemcinin bu AP'ye bağlanabilmesi için doğrulama isteyen öğede yapılandırılan ağ adını tam olarak bilmesi gerekir.

SSID yayını devre dışı bırakmak, istemcilerin ağınıza yanlışlıkla bağlanmasını önler ancak bir hacker'ın basit bir bağlanma ya da şifrenmemiş trafiği izleme denemesini bile önleyemez.

Bu durum, konuk ağında olduğu gibi öncelik faktörünün istemcilerin ağa bağlanmasını kolaylaştırdığı ve hassas bilgilerin yer almadığı korumasız ağlar için minimum düzeyde koruma sağlar. (Ayrıca bkz "Konuk Ağı", sayfa 102.)

10.1.4 İstasyon Ayırma Ağı Nasıl Korur?

Station Isolation (İstasyon Ayırma) etkinleştirildiğinde erişim noktası kablosuz istemciler arası iletişimi engeller. Erişim noktası, ağdaki kablosuz istemcileri ve kablolu cihazları arasındaki veri trafiğine izin vermeye devam eder ancak kablosuz istemciler arasındaki veri trafiğini engeller.

Trafik engelleme, *WDS* bağlantıları aracılığıyla ağa bağlanan kablosuz istemcilere kadar uzanır; bu istemciler İstasyon Engelleme özelliği açıkken birbirleriyle iletişim kuramaz.

WDS hakkında daha fazla bilgi için bkz. Bölüm 20: “Kablosuz Dağıtım Sistemi”.

10.2 Güvenlik Ayarlarını Yapılandırma

Güvenlik modunu ayarlamak için *Security* (Güvenlik) sekmesine gidin ve alanları aşağıda anlatıldığı gibi güncelleyin.

Şekil 10.1 Güvenlik Ayarları Sayfası

Basic Settings	Modify Internal Network security settings
User Management	<input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation
Cluster	Mode: <input type="text" value="WPA Personal"/>
Access Points	WPA Versions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2
Sessions	Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)
Channel Management	Key: <input type="text" value="reoreore"/>
Wireless Neighborhood	<input type="button" value="Update"/>
Security	
Status	
Interfaces	

Aşağıdaki yapılandırma bilgileri erişim noktasındaki güvenlik modlarının nasıl yapılandırıldığını açıklamaktadır. Erişim noktasıyla veri alışverişinde bulunmak isteyen her kablosuz istemcinin, erişim noktasıyla aynı güvenlik moduyla ve erişim noktası güvenliğiyle tutarlı şifreleme anahtarları ayarlarıyla yapılandırılması gerektiğini unutmayın.

İki telsizli bir AP'de bu Güvenlik Ayarları iki telsiz için de geçerlidir.



Not: Düz metin dışındaki tüm güvenlik modları yalnızca "Dahili" ağ yapılandırması için geçerlidir. "Konuk" ağında yalnızca Düz metin modunu kullanabilirsiniz. (Konuk ağları hakkında daha fazla bilgi için bkz. Bölüm 14: “Konuk Erişimİnİ Ayarlama”).

10.2.1 SSID Yayını, İstasyon Ayırma ve Güvenlik Modu

Erişim noktasında güvenliđi yapılandırmak için Tablo 10.5'te anlatıldığı gibi bir güvenlik modu seçin ve ilgili alanları doldurun.



Not: Ayrıca, ekstra önlem almak için Tablo 10.5, sayfa 101'de anlatıldığı gibi SSID yayınına izin verebilir/yayını engelleyebilir ve İstasyon Ayırmayı etkinleştirebilir/devre dışı bırakabilirsiniz.

Tablo 10.5 Güvenlik Ayarları

Alan	Açıklama
<i>Broadcast SSID</i> (SSID Yayını)	<p>Broadcast SSID (SSID Yayını) seçeneđini etkinleştirmek için doğrudan yanındaki kutucuđu işaretleyin. Erişim noktası varsayılan olarak uyarı anonslarındaki <i>Hizmet Kumesi Tanımlayıcısını (SSID)</i> yayınlar (izin verir).</p> <p>İstasyonların erişim noktasını otomatik olarak keşfetmemesi için bu yayını kaldırabilirsiniz (engelleyebilirsiniz). AP'nin SSID yayını kaldırıldığında ağ adı, istemci istasyonundaki Mevcut Ağlar Listesinde görülmez. İstemcinin bu AP'ye bağlanabilmesi için doğrulama isteyen ögede yapılandırılan ağ adını tam olarak bilmesi gerekir.</p>
<i>Station Isolation</i> (İstasyon Ayırma)	<p>Station Isolation (İstasyon Ayırma) seçeneđini etkinleştirmek için doğrudan yanındaki kutucuđu işaretleyin.</p> <ul style="list-style-type: none">• Station Isolation (İstasyon Ayırma) <i>devre dışı bırakıldığında</i> kablosuz istemciler erişim noktası aracılığıyla veri alışverişı yaparak normal bir şekilde birbirleriyle iletişim kurabilir.• Station Isolation (İstasyon Ayırma) <i>etkinleştirildiğinde</i> erişim noktası kablosuz istemciler arası iletişimi engeller. Erişim noktası, ağdaki kablosuz istemcileri ve kablolu cihazları arasındaki veri trafiđine izin vermeye devam eder ancak kablosuz istemciler arasındaki veri trafiđini engeller. Trafik engelleme, WDS bağlantıları aracılığıyla ağa bağlanan kablosuz istemcilere kadar uzanır; bu istemciler İstasyon Engelleme özelliđi açıkken birbirleriyle iletişim kuramaz. WDS hakkında daha fazla bilgi için bkz. Bölüm 20: "Kablosuz Dağıtım Sistemi".
<i>Security Mode</i> (Güvenlik Modu)	<p><i>Security Mode</i>'u (Güvenlik Modu) seçin. Aşağıdakilerden birini seçin:</p> <ul style="list-style-type: none">• "Yok (Düz metin)", sayfa 102.• "Statik WEP", sayfa 103.• "IEEE 802.1x", sayfa 108.• "WPA Kişisel", sayfa 111.• "WPA Kurumsal", sayfa 113. <p>Konuk ağında seçilebilecek tek güvenlik modu "None (Plain-text)" (Yok - Düz Metin) modudur. (Daha fazla bilgi için, bkz. Bölüm 14: "Konuk Erişimlini Ayarlama").</p> <p>"None (Plain-text) (Yok - Düz metin) dışındaki tüm güvenlik modları yalnızca "Dahili" ağ yapılandırması için geçerlidir.</p>

10.2.2 Güvenlik Modları

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Personal

- None (Plain-text)
- Static WEP
- IEEE802.1x
- WPA Personal
- WPA Enterprise

WPA2 ☒ CCMP (AES) ☐

Cipher: WPA Personal

Key: reoreore

10.2.2.1 Yok (Düz metin)

Yok (ya da düz metin güvenlik), 9160 G2 Kablosuz Ağ Geçidi cihazına ve bu cihazdan aktarılan verilerin şifrelenmediği anlamına gelir.

Güvenlik Modunuz olarak *Yok (Düz Metin)* modunu seçerseniz AP'deki diğer seçenekler yapılandırılmaz. Bu güvenlik modu, ilk ağ yapılandırması sırasında ya da sorun çözerken kullanışlı olabilir ancak güvenli olmadığı için Dahili ağda düzenli kullanılması önerilmez.

Konuk Ağı

"Yok (Düz metin)" modu doğası gereği güvenli olmayan bir **LAN** olan ve Dahili LAN'daki hassas bilgilerden her zaman sanal veya fiziksel olarak ayrı olan Konuk ağında çalıştırabileceğiniz tek moddur. Örneğin, konuk ağı günlük ziyaretçiler için Internet ve yazıcı erişimi sağlayabilir.

Konuk AP'de güvenliğin olmamasının sebebi, konukların istemcilerde herhangi bir güvenlik ayarı yapmadan mümkün olduğunca kolay biçimde bağlantı kurmalarını sağlamaktır.

Bir konuk ağında minimum koruma seviyesi sağlamak için SSID (ağ adı) yayını kaldırarak (engelleyerek) istasyonların erişim noktanızı otomatik olarak bulmasını önleyebilirsiniz. (Ayrıca bkz "SSID Yayını Engellemek Güvenliği Artırır mı?", sayfa 99.)

Konuk ağı hakkında daha fazla bilgi için bkz. Bölüm 14: "Konuk Erişimlini Ayarlama".

10.2.2.2 Statik WEP

☒ Broadcast SSID ☐ Station Isolation

Mode: Static WEP

Transfer key index: 1

Key Length: ☐ 64 bits ☒ 128 bits ☐ 152 bits

Key Type: ☐ ASCII ☒ Hex

WEP Keys: (Characters required: 26)

1:

2:

3:

4:

Authentication : ☒ Open system ☐ Shared key

Kablolu Eş Değer Gizlilik (WEP), 802.11 kablosuz ağlar için bir veri şifreleme protokolüdür. Ağdaki tüm kablosuz istasyonlar ve erişim noktaları, veri şifreleme için statik 64 bit (40 bit gizli anahtar + 24 bit başlatma vektörü [IV]) ya da 128 bit (104 bit gizli anahtar + 24 bit IV) Paylaşılan Anahtarla yapılandırılır. 64 bit ve 128 bit WEP anahtarlarını erişim noktaları ve istemci istasyonlarında karışık kullanamazsınız.

Statik WEP, mevcut olan en güvenli mod değildir ancak üçüncü bir şahsın şifrelenmemiş kablosuz trafiği kolayca açığa çıkarmasını önlediği için "Yok (Düz metin)" güvenlik ayarından daha fazla koruma sağlar. (Daha fazla güvenlik modu için bkz. "IEEE 802.1x", sayfa 108, "WPA Kişisel", sayfa 111 ya da "WPA Kurumsal", sayfa 113.)

WEP kablosuz ağda dolaşan verileri statik bir anahtar kullanarak şifreler. (Şifreleme algoritması RC4 adı verilen bir "şifre dizisi"dir.) Erişim noktası verileri istemci istasyonuna iletmek için bir anahtar kullanır. Her istemci istasyonu, erişim noktasından aldığı verinin şifresini çözmek için aynı anahtarı kullanmalıdır.

İstemci istasyonları erişim noktasına veri aktarırken farklı anahtarlar kullanabilir. (Hepsi aynı anahtarı da kullanabilir ancak bu şekilde bir istasyon başka bir istasyon tarafından gönderilen verinin şifresini çözebileceği için bu yöntem daha az güvenlidir.) *Statik WEP* Güvenlik Modunu seçtiğinizde aşağıdaki şekilde ve Tablo 10.6, sayfa 104'te açıklandığı gibi erişim noktası ayarlarıyla ilgili gerekli bilgileri sağlayın.

Tablo 10.6 Statik WEP Güvenlik Ayarları

Alan	Açıklama
<i>Transfer Key Index</i> (Aktarma Anahtarı Dizini)	Açılır menüden bir anahtar dizini seçin. Anahtar dizinleri 1-4 arasındadır. Varsayılan 1'dir. Aktarma Anahtarı Dizini, erişim noktasının aktardığı verileri şifrelemek için hangi WEP anahtarını kullanacağını belirtir.
<i>Key Length</i> (Anahtar Uzunluğu)	Aşağıdaki radyo düğmelerinden birine tıklayarak anahtarın uzunluğunu belirleyin: <ul style="list-style-type: none">• 64 bit• 128 bit
<i>Key Type</i> (Anahtar Türü)	Aşağıdaki radyo düğmelerinden birine tıklayarak anahtarın türünü belirleyin: <ul style="list-style-type: none">• ASCII• Hex (Onaltılı)
<i>Characters Required</i> (Gerekli Karakter Sayısı)	WEP anahtarında gerekli karakter sayısını belirtir. Gerekli karakter sayısı, Anahtar Uzunluğu ve Anahtar Türünü nasıl ayarladığınıza göre otomatik olarak güncellenir.
<i>WEP Keys</i> (WEP Anahtarları)	En fazla dört WEP anahtarı belirleyebilirsiniz. Her metin kutusuna her bir anahtar için bir karakter dizesi girin. "ASCII"yi seçerseniz 0-9, a-z ve A-Z tam sayı ve harflerinin herhangi bir kombinasyonunu girin. "ONALTILI"yı seçerseniz onaltılık sistemde 0-9 ve a-f ya da A-F'nin kombinasyonundan oluşan herhangi bir değer girin. Her anahtar için "Characters Required" (Gerekli Karakter Sayısı) alanında belirtilen sayıda karakter kullanın. Bunlar, erişim noktası kullanılırken istasyonlarla paylaşılan RC4 WEP anahtarlarıdır. Her istemci istasyonu, burada anlatıldığı gibi AP'de aynı yuvada yer alan bu aynı WEP anahtarlarından birini kullanacak şekilde yapılandırılmalıdır. (Bkz. "Statik WEP ile İlgili Unutulmaması Gereken Kurallar", sayfa 105.)

Tablo 10.6 Statik WEP Güvenlik Ayarları

Alan	Açıklama
<i>Authentication Algorithm</i> (Kimlik Doğrulama Algoritması)	<p>Kimlik doğrulama algoritması, statik WEP güvenlik modu kullanılırken bir istemci istasyonunun bir erişim noktasıyla ilişkilmesine izin verilip verilmemesini belirlemek için kullanılan yöntemi tanımlar. Aşağıdaki açılır menüdeki seçeneklerden birini belirleyerek kullanmak istediğiniz kimlik doğrulama algoritmasını seçin:</p> <ul style="list-style-type: none">• Open System. (Açık Sistem)• Shared Key. (Paylaşılan Anahtar)• Both. (İkisi de) <p>Açık Sistem kimlik doğrulaması, herhangi bir istemci istasyonunun doğru WEP anahtarına sahip olup olmamasına bakılmaksızın erişim noktasıyla ilişkilmesine izin verir. Bu algoritma aynı zamanda düz metin, IEEE 802.1x ve WPA modlarında da kullanılır. Kimlik doğrulama algoritması "Açık Sistem" olarak ayarlandığında herhangi bir istemci erişim noktasıyla ilişkilenebilir.</p> <p>Bir istemci istasyonunun erişim noktasıyla ilişkilmesine izin verilmesi, erişim noktasıyla veri trafiği alışverişi yapabilmesini garantilemez. Bir istasyonun erişim noktasından gelen verilere başarıyla erişebilmesi, bu verilerin şifresini çözebilmesi ve bu erişim noktasına okunabilir veriler aktarabilmesi için doğru WEP anahtarına sahip olması gerekir.</p> <p>Paylaşılan Anahtar kimlik doğrulaması, istemci istasyonunun erişim noktasıyla ilişkilmesi için doğru WEP anahtarına sahip olmasını gerektirir. Kimlik doğrulama algoritması "Paylaşılan Anahtar" olarak ayarlandığında, yanlış WEP anahtarına sahip bir istasyonun erişim noktasıyla ilişkilenebilir.</p> <p>İkisi de, varsayılan ayardır. Kimlik doğrulama algoritması "Both" (İkisi de) olarak ayarlandığında:</p> <ul style="list-style-type: none">• WEP anahtarını paylaşılan anahtar modunda kullanmak üzere yapılandırılan istemci istasyonlarının erişim noktasıyla ilişkilmesi için geçerli bir WEP anahtarına sahip olması gerekir.• WEP anahtarını açık sistem modunda (paylaşılan anahtar modu etkin değilken) kullanmak üzere yapılandırılan istemci istasyonları, doğru WEP anahtarına sahip olmasalar bile erişim noktasıyla ilişkilenebilirler.

Statik WEP ile İlgili Unutulmaması Gereken Kurallar

- Tüm istemci istasyonlarının Kablosuz LAN (WLAN) güvenliğinin WEP olarak ayarlanması gerekir. Ayrıca AP'den istasyona veri aktarımlarının şifresini çözmek için tüm istemcilerin AP'de belirtilen WEP anahtarlarından birine sahip olması gerekir.
- İstasyon aktarımlarının şifresini çözmek için AP'nin istasyondan AP'ye aktarımlarda istemcinin kullandığı tüm anahtarlara sahip olması gerekir.

- Aynı anahtarın tüm düğümlerde aynı yuvada bulunması gerekir (AP ve istemcilerde). Örneğin; AP, abc123 anahtarını WEP anahtarı 3 olarak tanımlarsa istemcinin de aynı dizeyi WEP anahtarı 3 olarak tanımlaması gerekir.
- Bazı kablosuz istemci yazılımlarında (Funk Odyssey gibi), birden çok WEP anahtarı yapılandırılabilir ve bir "aktarma anahtarı dizini" istemci istasyonu tanımlayabilirsiniz. Ardından, aktardıkları verileri farklı anahtarlar kullanarak şifreleyecek şekilde istasyonları ayarlayabilirsiniz. Böylece, komşu AP'lerin birbirlerinin aktarımlarının şifresini çözmesini önlemiş olursunuz.

Statik WEP Kullanımı Örnekleri

Örneğin, erişim noktasında üç WEP anahtarı yapılandırdığınızı düşünelim. Bu örneğe göre, AP için Aktarma Anahtarı Dizini 3'tür. Bu da, 3. yuvadaki WEP anahtarının erişim noktasının gönderdiği verileri şifrelemek için kullanacağı anahtar olduğu anlamına gelir.

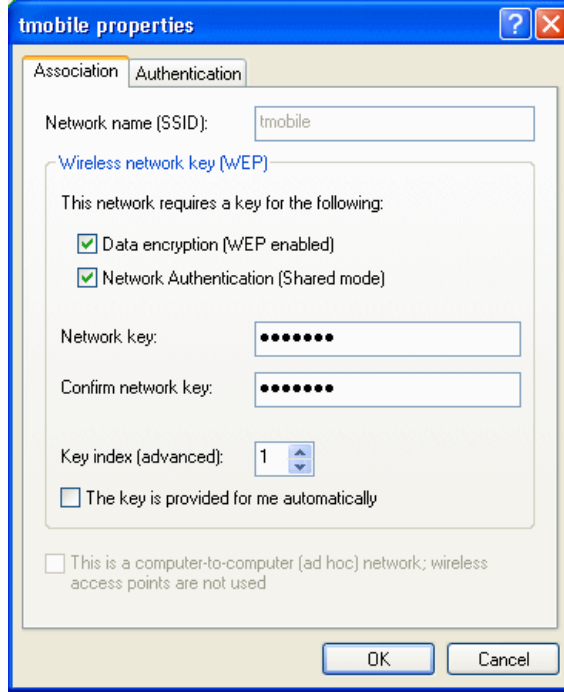
Şekil 10.2 AP Aktarma Anahtarının Erişim Noktasında Ayarlanması

The screenshot shows a configuration window for WEP. At the top, there are two checkboxes: 'Broadcast SSID' (checked) and 'Station Isolation' (unchecked). Below this is a 'Mode:' dropdown menu set to 'Static WEP'. Underneath is a 'Transfer key index:' dropdown menu set to '3'. Then, there are three radio buttons for 'Key Length': '64 bits' (selected), '128 bits', and '152 bits'. Below that are two radio buttons for 'Key Type': 'ASCII' (selected) and 'Hex'. The 'WEP Keys:' section has a note '(Characters required: 5)' and four input fields labeled 1, 2, 3, and 4. Field 1 contains 'abcde', field 2 contains 'fghij', field 3 contains 'klmno', and field 4 is empty. At the bottom, there are two checkboxes for 'Authentication': 'Open system' (checked) and 'Shared key' (unchecked).

Ardından, tüm istemci istasyonlarını WEP anahtarını kullanacak şekilde ayarlamamız ve her istemciye AP'de tanımladığımız yuva/anahtar kombinasyonlarından birini sağlamanız gerekir.

Bu örnekte bir Windows istemcide WEP anahtarı 1'i ayarlayalım.

Şekil 10.3 Kablosuz İstemciye WEP Anahtarı Sağlama



İkinci bir istemci istasyonunuz varsa bu istasyonun da AP'de tanımlanan WEP anahtarlarından birine sahip olması gerekir. İlk istasyona verdiğiniz WEP anahtarının aynısını bu istasyona da verebilirsiniz. Ya da, daha güvenli bir çözüm için ikinci istasyona farklı bir WEP anahtarı (örneğin, anahtar 2) sağlarsınız; böylece iki istasyon birbirinin aktarımının şifresini çözemez.

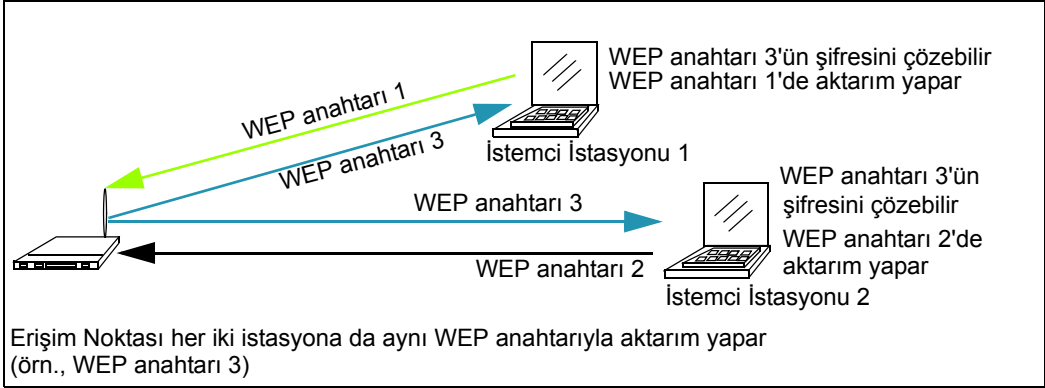
İstemci İstasyonlarında Aktarma Anahtarı Dizinlerine Sahip Statik WEP

Bazı Kablosuz istemci yazılımları (Funk Odyssey gibi) birden çok WEP anahtarı yapılandırmanıza ve istemci istasyonunda aktarma dizini ayarlamana olanak sağlar, böylece istasyondan AP'ye yapılan aktarımlarda kullanılacak farklı anahtarlar belirleyebilirsiniz. (Standart Windows kablosuz istemci yazılımı bunu yapmanıza izin vermez.)

Örneğimize devam edelim: Funk Odyssey istemci yazılımını kullandığınızda AP aktarımlarının şifresini çözebilmeleri için her istemciye WEP anahtarı 3'ü verebilir; ayrıca istemci 1'e, WEP anahtarı 1'i vererek bunu aktarım anahtarı olarak ayarlayabilirsiniz. Ardından istemci 2'ye, WEP anahtarı 2'yi vererek bunu aktarım anahtarı dizini olarak ayarlayabilirsiniz.

Şekil 10.2.2.3, AP'nin ve birden fazla WEP anahtarı ve bir aktarım anahtarı dizini kullanan iki istemci istasyonunun dinamiklerini göstermektedir.

Şekil 10.4 İstemci İstasyonlarında Birden Fazla WEP Anahtarı ve Aktarma Anahtarı Dizini Kullanımına Örnek



10.2.2.3 IEEE 802.1x

IEEE 802.11, bağlantı noktası tabanlı kimlik doğrulama ve anahtar yönetimi için altyapı tanımlayan standarttır. Genişletilebilir Kimlik Doğrulama Protokolü (**EAP**) mesajları, LAN üzerinden EAP Kuşatma (EAPOL) adlı bir protokol kullanılarak bir **IEEE 802.11** kablosuz ağı üzerinden gönderilir. IEEE 802.1x, periyodik olarak yenilenen ve dinamik şekilde oluşturulan anahtarlar sunar. Bir RC4 şifre dizisi, her 802.11 çerçevesinin çerçeve gövdesini ve döngüsel artıklık denetimini (CRC) şifrelemek için kullanılır.

Bu mod, kullanıcıların kimliklerinin doğrulanması için bir **RADIUS** sunucusunun kullanılmasını gerektirir. Dahili RADIUS sunucusu seçeneği etkinse *Cluster > User Management* (Küme > Kullanıcı Yönetimi) sekmesi aracılığıyla AP'de kullanıcı hesapları yapılandırın. Bu seçenek etkin değilse harici RADIUS sunucusunda kullanıcı hesapları yapılandırın.

Erişim noktası, Microsoft Internet Kimlik Doğrulama Sunucusu ya da 9160 G2 Kablosuz Ağ Geçidi dahili kimlik doğrulama sunucusu gibi **EAP**'yi destekleyen bir RADIUS sunucusu gerektirir. Kimlik doğrulama sunucusunun Windows istemcilerle çalışması için Korunmalı EAP (PEAP) ve **MSCHAP V2**'yi desteklemesi gerekir.

IEEE 802.1x modunu yapılandırırken gömülü RADIUS sunucusunu ya da sağladığınız harici RADIUS sunucusunu kullanmayı seçebilirsiniz. 9160 G2 Kablosuz Ağ Geçidi gömülü RADIUS sunucusu Korunmalı **EAP** (PEAP) ve MSCHAP V2'yi destekler.

Kendi RADIUS sunucunuz varsa sertifikalar, Kerberos ve açık anahtar kimliği doğrulama gibi IEEE 802.1x modunun desteklediği çeşitli kimlik doğrulama yöntemlerinden birini kullanabilirsiniz. Ancak, istemci istasyonlarının erişim noktasının kullandığı kimlik doğrulama yönteminin aynısını kullanacak şekilde yapılandırılması gerektiğini unutmayın. *IEEE 802.1x* Güvenlik Modunu seçtiyseniz aşağıdaki bilgileri sağlayın:

Security Mode

IEEE 802.1x

Authentication Server

Built-in

Radius IP

127 . 0 . 0 . 1

Radius Key

•••••

☐ Enable radius accounting

☒ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x


☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key: ••••••••

☐ Enable radius accounting

Tablo 10.7 IEEE 802.1x Güvenlik Ayarları

Alan	Açıklama
<i>Use internal radius server (Dahili radius sunucusunu kullan)</i>	<p>Açılır menüden aşağıdakilerden birini seçin:</p> <ul style="list-style-type: none">9160 G2 Kablosuz Ağ Geçidi ile birlikte verilen kimlik doğrulama sunucusunu kullanmak için Use internal radius server (Dahili radius sunucusunu kullan) alanının yanındaki kutucuğun işaretli olduğundan emin olun. Bu seçenek işaretlenmişse Radius IP'yi ve Radius Anahtarını belirtmeniz gerekmez; bu bilgiler otomatik olarak verilir. Dahili RADIUS sunucusu seçeneği etkinse <i>Cluster > User Management</i> (Küme > Kullanıcı Yönetimi) sekmesi aracılığıyla AP'de kullanıcı hesapları yapılandırın. Daha fazla bilgi için bkz. Bölüm 7: "Kullanıcı Hesaplarını Yönetme".Harici bir kimlik doğrulama sunucusu kullanmak için Use internal radius server (Dahili radius sunucusunu kullan) alanının yanındaki kutucuğun işaretli olmadığından emin olun. Bu kutucuğun işaretini kaldırırsanız kullanmak istediğiniz sunucunun Radius IP'sini ve Radius Anahtarını belirtmeniz gerekir. <p>Not: RADIUS sunucusu, IP adresi ve sunduğu farklı hizmetler için kullanılan UDP bağlantı noktası numaralarıyla tanımlanır. 9160 G2 Kablosuz Ağ Geçidi cihazının yeni sürümünde, erişim noktası tarafından kullanılan RADIUS sunucusu Kullanıcı Veri Bloğu Protokolü (UDP) bağlantı noktaları yapılandırılmaz. (9160 G2 Kablosuz Ağ Geçidi, kimlik doğrulama için RADIUS sunucusu UDP bağlantı noktası 1812'yi, hesaplama için 1813'ü kullanmak için doğrudan kodlanmıştır.)</p>
<i>Radius IP (Radius IP'si)</i>	<p>Metin kutusuna Radius IP'sini girin.</p> <p>Radius IP, RADIUS sunucusunun IP adresidir.</p> <p>(9160 G2 Kablosuz Ağ Geçidi dahili kimlik doğrulama sunucusu 127.0.0.1'dir.)</p> <p> Ağınızda harici bir RADIUS sunucunuz varsa AP'deki gömülü RADIUS sunucusunu kullanmak yerine bu sunucuyu kullanmanızı öneririz. Harici bir RADIUS sunucusu, yerel kimlik doğrulama sunucusundan daha iyi güvenlik sağlar.</p> <p>Kullanıcı hesapları kurmayla ilgili bilgi için bkz. Bölüm 7: "Kullanıcı Hesaplarını Yönetme".</p>
<i>Radius Key (Radius Anahtarı)</i>	<p>Metin kutusuna Radius Anahtarını girin.</p> <p>Radius Anahtarı, RADIUS sunucusu için paylaşılan gizli anahtardır. RADIUS anahtarını girerken başkalarının görmesini engellemek için, girdiğiniz metin "*" karakterleri olarak görünecektir.</p> <p>(9160 G2 Kablosuz Ağ Geçidi dahili kimlik doğrulama sunucusu anahtarı gizlidir.)</p> <p>Bu değer hiçbir zaman ağ üzerinden gönderilmez.</p>
<i>Enable radius accounting (Radius hesaplamayı etkinleştir)</i>	<p>Belirli bir kullanıcının sistem zamanı, aktardığı ve aldığı veri miktarı gibi harcadığı kaynakları takip etmek ve ölçmek istiyorsanız "Enable radius accounting" (Radius hesaplamayı etkinleştir) seçeneğinin yanındaki kutucuğu işaretleyin.</p>

10.2.2.4 WPA Kişisel

Wi-Fi Korumalı Erişim Kişisel, Sayaç modu/CBC-MAC Protokolü-Gelişmiş Şifreleme Algoritması (CCMP-AES) ve Geçici Anahtar Bütünlüğü Protokolü (TKIP) mekanizmalarını içeren bir Wi-Fi İttifakı IEEE **802.11i** standardıdır.

WPA'nın Kişisel versiyonu, Kurumsal WPA güvenlik modunda kullanılan IEEE 802.11 ve **EAP**'nin yerine önceden paylaşılan bir anahtar kullanır. PSK, yalnızca kimlik bilgilerinin ilk kontrolünde kullanılır. Bu güvenlik modu, orijinal **WPA**'yi destekleyen kablosuz istemciler için geriye dönük uyumluluk sunar.

WPA Kişisel Güvenlik Modunu seçtiyseniz ayarları Tablo 10.8, sayfa 112'de açıklandığı gibi tamamlayın.

Security Mode	WPA/WPA2 Personal (PSK)
<hr/>	
Supported Client Stations	Both
Cipher Suites	TKIP
Key	

<input checked="" type="checkbox"/> Broadcast SSID	<input type="checkbox"/> Station Isolation	
Mode:	WPA Personal	
WPA Versions:	<input checked="" type="checkbox"/> WPA	<input checked="" type="checkbox"/> WPA2
Cipher Suites:	<input checked="" type="checkbox"/> TKIP	<input type="checkbox"/> CCMP (AES)
Key:	reoreore	

Tablo 10.8 WPA Kişisel Güvenlik Ayarları

Alan	Açıklama
<i>WPA Versions</i> (<i>WPA Versiyonları</i>)	<p>Desteklemek istediğiniz istemci istasyonu türlerini seçin:</p> <ul style="list-style-type: none">• WPA• WPA2• Both (İkisi de) <p>WPA. Ağıdaki tüm istemci istasyonları orijinal WPA'yı destekliyor ancak hiçbirini yeni WPA2'yi desteklemiyorsa WPA'yı seçin.</p> <p>WPA2. Ağıdaki tüm istemci istasyonları WPA2'yi destekliyorsa IEEE 802.11i standardı başına en iyi güvenliği sağlayan WPA2'yi kullanmanızı öneririz.</p> <p>Both. (İkisi de) İstemcilerinizin bazıları WPA2'yi, bazıları da yalnızca orijinal WPA'yı destekliyorsa ikisini de seçin. Bu seçenek hem WPA hem de WPA2 istemci istasyonlarının ilişkilendirilmesini ve kimliklerinin doğrulanmasını sağlar ancak daha güçlü olan WPA2'yi destekleyen istemcilerde WPA2'yi kullanır.</p> <p>Bu WPA yapılandırması, güvenlikten belirli bir derece ödün vererek daha fazla birlikte çalışabilirlik sağlar.</p>

Tablo 10.8 WPA Kişisel Güvenlik Ayarları (Devamı)

Alan	Açıklama
<i>Cipher Suites</i> (Şifre Grubu)	<p>Kullanmak istediğiniz şifre grubunu seçin:</p> <ul style="list-style-type: none">• TKIP• CCMP (AES)• Both (İkisi de) <p>Geçici Anahtar Bütünlüğü Protokolü (TKIP) varsayılandır.</p> <p>TKIP, WEP anahtarından daha güvenli bir şifreleme çözümü sunar. TKIP, kullanılan şifreleme anahtarını daha sık değiştirir ve verileri şifrelemek için aynı anahtarın tekrar kullanılmamasını daha iyi garanti eder (WEP'in zayıf noktası). TKIP, istemciler ve erişim noktalarının paylaştığı 128 bit "geçici bir anahtar" kullanır. Geçici anahtar, verileri şifreleyecek anahtarları üretmek için 16 baytlık başlatma vektörü ve istemcinin MAC adresiyle birleştirilmiştir. Bu sayede her istemci istasyonu verileri şifrelemek için farklı bir anahtar kullanır. TKIP şifreleme için RC4 kullanır (WEP ile aynı). Ancak TKIP geçici anahtarları her 10.000 pakette bir değiştirip dağıtarak ağ güvenliğini önemli ölçüde geliştirir.</p> <p>Gelişmiş Şifreleme Algoritmasını (AES) kullanan Sayaç modu/CBC-MAC Protokolü (CCMP), IEEE 802.11i için kullanılan bir şifreleme yöntemidir. Şifreleme ve mesaj bütünlüğü için Şifre Bloğu Zincirleme Sayaç modu (CBC-CTR) ve Şifre Bloğu Zincirleme Mesajı Kimlik Doğrulama Kodu (CBC-MAC) ile birlikte bir CCM kullanır.</p> <p>Hem TKIP hem de CCMP(AES) seçeneklerini belirlerseniz İkili şifre AES, Grup şifresi TKIP olur. İkili şifre tek yönlü trafikte kullanılırken Grup şifresi çoklu/yayın trafiğinde kullanılır. Hem TKIP hem de AES istemcileri erişim noktasıyla ilişkilenebilir. WPA istemcilerinin AP ile ilişkilenebilmesi için aşağıdakilerden birine sahip olması gerekir:</p> <ul style="list-style-type: none">• Geçerli bir TKIP anahtar• Geçerli bir CCMP (AES) anahtar <p>Bir WPA Kişisel kullanmak için yapılandırılmayan istemciler AP ile ilişkilendirilemez.</p>
<i>Key (Anahtar)</i>	<p>Önceden Paylaşılan Anahtar WPA Kişisel için paylaşılan gizli anahtardır. En az 8, en fazla 63 karakter uzunluğunda bir dize girin.</p>

10.2.2.5 WPA Kurumsal

Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmetini (RADIUS) içeren Wi-Fi Korumalı Erişim Kurumsal; Gelişmiş Şifreleme Standardı (AES), Sayaç Modu/CBC-MAC Protokolü (CCMP) ve Geçici Anahtar Bütünlüğü Protokolü (TKIP) mekanizmalarını içeren Wi-Fi İttifakı IEEE 802.11h standardının bir uygulamasıdır. Kurumsal modu, kullanıcıların kimliklerinin doğrulanması için bir RADIUS sunucusunun kullanılmasını ve kullanıcı hesaplarının Cluster, User Management (Küme, Kullanıcı Yönetimi) sekmesinde yapılandırılmasını gerektirir.

Bu güvenlik modu, orijinal **WPA**'yi destekleyen kablosuz istemcilerle geriye dönük uyumluluk sağlar.

WPA Kurumsal modunu yapılandırırken yerleşik RADIUS sunucusunu ya da sağladığınız harici RADIUS sunucusunu kullanmayı seçebilirsiniz. 9160 G2 Kablosuz Ağ Geçidi yerleşik RADIUS sunucusu Korunmalı **EAP** (PEAP) ve MSCHAP V2'yi destekler.

"WPA Kurumsal" Güvenlik Modunu seçtiyseniz ayarları Tablo 10.9, sayfa 115'te açıklandığı gibi tamamlayın.

Security Mode	WPA/WPA2 Enterprise (RADIUS) ▼
Supported Client Stations	WPA ▼
	<input type="checkbox"/> Enable pre-authentication
Cipher Suites	TKIP ▼
Authentication Server	Built-in ▼
Radius IP	127 . 0 . 0 . 1
Radius Key	<input type="password"/>
	<input type="checkbox"/> Enable radius accounting
	<input checked="" type="checkbox"/> Allow non-WPA IEEE 802.1x clients

<input checked="" type="checkbox"/> Broadcast SSID	<input type="checkbox"/> Station Isolation
Mode:	WPA Enterprise ▼
WPA Versions:	<input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2
	<input type="checkbox"/> Enable pre-authentication
Cipher Suites:	<input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)
<input type="checkbox"/> Use internal radius server	
Radius IP:	10.128.14.14
Radius Key:	●●●●●●●●
<input type="checkbox"/> Enable radius accounting	


Tablo 10.9 WPA Kurumsal Güvenlik Ayarları

Alan	Açıklama
<i>WPA Versions</i> (<i>WPA Versiyonları</i>)	<p>Desteklemek istediğiniz istemci istasyonu türlerini seçin:</p> <ul style="list-style-type: none">• WPA• WPA2• Both (İkisi de) <p>WPA. Ağıdaki tüm istemci istasyonları orijinal WPA'yı destekliyor ancak hiçbirini yeni WPA2'yi desteklemiyorsa WPA'yı seçin.</p> <p>WPA2. Ağıdaki tüm istemci istasyonları WPA2'yi destekliyorsa IEEE 802.11i standardı başına en iyi güvenliği sağlayan WPA2'yi kullanmanızı öneririz.</p> <p>Both. (İkisi de) İstemcilerinizin bazıları WPA2'yi, bazıları da yalnızca orijinal WPA'yı destekliyorsa hem WPA'yı hem de WPA2'yi seçin. Bu seçenek hem WPA hem de WPA2 istemci istasyonlarının ilişkilendirilmesini ve kimliklerinin doğrulanmasını sağlar ancak daha güçlü olan WPA2'yi destekleyen istemcilerde WPA2'yi kullanır.</p> <p>Bu WPA yapılandırması, güvenlikten belirli bir derece ödün vererek daha fazla birlikte çalışabilirlik sağlar.</p>
<i>Enable pre-authentication</i> (<i>Önceden kimlik doğrulamayı etkinleştir</i>)	<p>WPA Versiyonları için yalnızca WPA2 ya da hem WPA hem de WPA2'yi seçtiyseniz WPA2 istemciler için önceden kimlik doğrulamayı etkinleştirebilirsiniz.</p> <p>WPA2 kablosuz istemcilerin önceden kimlik doğrulama paketi göndermesini istiyorsanız Enable pre-authentication (Önceden kimlik doğrulamayı etkinleştir) seçeneğine tıklayın. Önceden kimlik doğrulama bilgisi, istemcinin o an kullandığı erişim noktasından hedef erişim noktasına aktarılır. Bu özelliğin etkinleştirilmesi, birden fazla erişim noktasına bağlanan gezici istemcilerin kimliklerinin doğrulanmasını hızlandırır.</p> <p>Orijinal WPA bu özelliği desteklemediği için WPA Versiyonu olarak "WPA'yı" belirlediğinizde bu seçenek kullanılamaz.</p>

Tablo 10.9 WPA Kurumsal Güvenlik Ayarları (Devamı)

Alan	Açıklama
<i>Cipher Suites (Şifre Grubu)</i>	<p>Kullanmak istediğiniz şifreyi seçin:</p> <ul style="list-style-type: none">• TKIP• CCMP (AES)• Both (İkisi de) <p>Geçici Anahtar Bütünlüğü Protokolü (TKIP) varsayılandır.</p> <p>TKIP, WEP anahtarından daha güvenli bir şifreleme çözümü sunar. TKIP, kullanılan şifreleme anahtarını daha sık değiştirir ve verileri şifrelemek için aynı anahtarın tekrar kullanılmamasını daha iyi garanti eder (WEP'in zayıf noktası). TKIP, istemciler ve erişim noktalarının paylaştığı 128 bit "geçici bir anahtar" kullanır. Geçici anahtar, verileri şifreleyecek anahtar üretmek için 16 baytlık başlatma vektörü ve istemcinin MAC adresiyle birleştirilmiştir. Bu sayede her istemci istasyonu verileri şifrelemek için farklı bir anahtar kullanır. TKIP şifreleme için RC4 kullanır (WEP ile aynı). Ancak TKIP geçici anahtarları her 10.000 pakette bir değiştirip dağıtarak ağ güvenliğini önemli ölçüde geliştirir.</p> <p>Gelişmiş Şifreleme Algoritmasını (AES) kullanan Sayaç modu/CBC-MAC Protokolü (CCMP), IEEE 802.11i için kullanılan bir şifreleme yöntemidir. Şifreleme ve mesaj bütünlüğü için Şifre Bloğu Zincirleme Sayaç modu (CBC-CTR) ve Şifre Bloğu Zincirleme Mesajı Kimlik Doğrulama Kodu (CBC-MAC) ile birlikte bir CCM kullanır.</p> <p>TKIP ve CCMP'nin ikisi birden seçildiğinde hem TKIP hem de AES istemciler erişim noktasıyla ilişkilenebilir. RADIUS sunucusu içeren bir WPA kullanmak üzere yapılandırılan istemci istasyonlarının AP ile ilişkilenebilmesi için aşağıdakilerden birine sahip olması gerekir:</p> <ul style="list-style-type: none">• Geçerli bir TKIP RADIUS IP adresi ve geçerli bir paylaşılan Anahtar.• Geçerli bir CCMP (AES) IP adresi ve geçerli bir paylaşılan Anahtar. <p>RADIUS içeren WPA kullanmak için yapılandırılmayan istemciler AP ile ilişkilendirilemez.</p> <p>Varsayılan olarak hem TKIP hem de CCMP seçilidir. Hem TKIP hem de CCMP seçiliyken RADIUS içeren WPA kullanmak için yapılandırılan istemci istasyonlarının aşağıdakilerden birine sahip olması gerekir:</p> <ul style="list-style-type: none">• Geçerli bir TKIP RADIUS IP adresi ve RADIUS Anahtarı.• Geçerli bir CCMP (AES) IP adresi ve RADIUS Anahtarı.

Tablo 10.9 WPA Kurumsal Güvenlik Ayarları (Devamı)

Alan	Açıklama
<i>Use internal radius server (Dahili radius sunucusunu kullan)</i>	<p>9160 G2 Kablosuz Ağ Geçidi ile birlikte verilen yerleşik kimlik doğrulama sunucusunu ya da harici bir radius sunucusunu kullanmayı seçebilirsiniz.</p> <ul style="list-style-type: none">9160 G2 Kablosuz Ağ Geçidi ile birlikte verilen kimlik doğrulama sunucusunu kullanmak için Use internal radius server (Dahili radius sunucusunu kullan) alanının yanındaki kutucuğun işaretli olduğundan emin olun. Bu seçenek işaretlenmişse Radius IP'yi ve Radius Anahtarını belirtmeniz gerekmez; bu bilgiler otomatik olarak verilir. Dahili RADIUS sunucusu seçeneği etkinse <i>Cluster > User Management</i> (Küme > Kullanıcı Yönetimi) sekmesi aracılığıyla AP'de kullanıcı hesapları yapılandırın. Daha fazla bilgi için bkz. Bölüm 7: "Kullanıcı Hesaplarını Yönetme".Harici bir kimlik doğrulama sunucusu kullanmak için Use internal radius server (Dahili radius sunucusunu kullan) alanının yanındaki kutucuğun işaretli olmadığından emin olun. Bu kutucuğun işaretini kaldırırsanız kullanmak istediğiniz sunucunun Radius IP'sini ve Radius Anahtarını belirtmeniz gerekir. <p>Not: <i>RADIUS sunucusu, IP adresi ve sunduğu farklı hizmetler için kullanılan UDP bağlantı noktası numaralarıyla tanımlanır. 9160 G2 Kablosuz Ağ Geçidi cihazının yeni sürümünde, erişim noktası tarafından kullanılan RADIUS sunucusu Kullanıcı Veri Bloğu Protokolü (UDP) bağlantı noktaları yapılandırılmaz. (9160 G2 Kablosuz Ağ Geçidi, kimlik doğrulama için RADIUS sunucusu UDP bağlantı noktası 1812'yi, hesaplama için 1813'ü kullanmak için doğrudan kodlanmıştır.)</i></p>
<i>Radius IP (Radius IP'si)</i>	<p>Metin kutusuna Radius IP'sini girin. <i>Radius IP, RADIUS sunucusunun IP adresidir.</i></p> <p>(9160 G2 Kablosuz Ağ Geçidi dahili kimlik doğrulama sunucusu 127.0.0.1'dir.)</p> <p> Açınızda harici bir RADIUS sunucunuz varsa AP'deki gömülü RADIUS sunucusunu kullanmak yerine bu sunucuyu kullanmanızı öneririz. Harici bir RADIUS sunucusu, yerel kimlik doğrulama sunucusundan daha iyi bir güvenlik sağlar.</p> <p>Kullanıcı hesapları kurmayla ilgili bilgi için bkz. Bölüm 7: "Kullanıcı Hesaplarını Yönetme".</p>
<i>Radius Key (Radius Anahtarı)</i>	<p>Metin kutusuna Radius Anahtarını girin.</p> <p><i>Radius Anahtarı, RADIUS sunucusu için paylaşılan gizli anahtardır. RADIUS anahtarını girenken başkalarının görmesini engellemek için, girdiğiniz metin "*" karakterleri olarak görünecektir.</i></p> <p>(9160 G2 Kablosuz Ağ Geçidi dahili kimlik doğrulama sunucusu anahtarı gizlidir.)</p> <p>Bu değer hiçbir zaman ağ üzerinden gönderilmez.</p>
<i>Enable RADIUS Accounting (RADIUS Hesaplamayı Etkinleştir)</i>	<p>WPA istemci istasyonlarına, her istasyon için kullanıcı adı ve şifrelerle kimlik doğrulaması yapmak istiyorsanız Enable RADIUS Accounting (RADIUS Hesaplamayı Etkinleştir) seçeneğine tıklayın. Ayrıca bkz. Bölüm 7: "Kullanıcı Hesaplarını Yönetme".</p>

10.3 Ayarları Güncelleme

Güvenlik ayarlarını güncellemek için:

1. *Security* (Güvenlik) sekmesine gidin.
2. Güvenlik ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

11.1 Arabirimler	121
11.1.1 Ethernet (Kablolu) Ayarları	122
11.1.2 Kablosuz Ayarları	122
11.2 Olay Günlükleri	122
11.2.1 SürekliliğiEtkinleştirme ya da Devre Dışı Bırakma	123
11.2.2 Önem Derecesi	124
11.2.3 Derinlik.	124
11.2.4 Çekirdek Mesajlar İçin Günlük Aktarma Sunucusu	125
11.2.4.1 Uzaktan Günlük Oluşturmayı Anlama	125
11.2.4.2 Günlük Aktarma Sunucusunu Kurma	125
11.2.4.3 Durum, Olaylar Sayfasında Günlük Aktarma Sunucusunu Etkinleştirme/Devre Dışı Bırakma	126
11.2.5 Olaylar Günlüğü	127
11.3 Alma/Verme İstatistikleri	127
11.4 İlişkili Kablosuz İstemciler	129
11.4.1 Bağlantı Bütünlüğünü İzleme	130
11.5 Komşu Erişim Noktaları	130



Önemli: Burada anlatılan bakım ve izleme görevlerinin hepsi belirli erişim noktalarındaki görüntüleme ve onarım ayarlarıyla ilgilidir; birden fazla erişim noktasıyla otomatik olarak paylaşılan küme yapılandırmalarındaki ayarlarla ilgili değildir. Bu yüzden yapılandırmak istediğiniz belirli bir erişim noktası için Yönetim Web sayfalarına eriştiğinizden emin olmanız gerekir. Daha fazla bilgi için bkz. “Belirli Bir AP'nin Yapılandırma Bilgileri ve Bağımsız AP'leri Yönetme”, sayfa 61.

11.1 Arabirimler

Kablolu LAN ve kablosuz LAN (*WLAN*) ayarlarını izlemek için, izlemek istediğiniz erişim noktasında *Status > Interfaces* (Durum > Arabirimler) sekmesine gidin.



Not: İki telsizli bir erişim noktasında mevcut kablosuz ayarları hem Telsiz 1 hem de Telsiz 2 için gösterilir. Tek telsizli bir erişim noktasında ayarlar tek telsiz için gösterilir. İki telsizli bir AP'nin *Interfaces* (Arabirimler) sayfası aşağıdaki şekilde gösterilmiştir:

Şekil 11.1 Ağ Arabirim Sayfası

View settings for network interfaces

Wired Settings (Edit)	
LAN or Internal Interface	
MAC Address	00:08:A2:01:10:AC
VLAN ID	
IP Address	10.128.75.98
Subnet Mask	255.255.0.0
Guest Interface	
MAC Address	00:00:00:00:00:00
VLAN ID	
Subnet	
<hr/>	
Wireless Settings (Edit)	
Radio	
Mode	IEEE 802.11g
Channel	5 (2432 MHz)
Internal Interface	
MAC Address	00:08:A2:01:10:B0
Network Name (SSID)	SFGWPA /
Guest Interface	
MAC Address	n/a
Network Name (SSID)	TEKLOGIX GUEST /

? This page displays current Ethernet (Wired) and Wireless settings on the access point.

To configure Ethernet Settings, go to the [Ethernet \(Wired\) Settings](#) tab.

To configure Wireless Settings, go to the [Wireless Settings](#) tab.

[More ...](#)

Bu sayfa 9160 G2 Kablosuz Ağ Geçidi cihazının mevcut ayarlarını göstermektedir. Sayfada *Ethernet (Wired) Settings* (Ethernet [Kablolu] Ayarları) ve *Wireless Settings* (Kablosuz Ayarları) gösterilir.

11.1.1 Ethernet (Kablolu) Ayarları

Internal (Dahili) arabirim şunları içerir: Ethernet **MAC Adresi**, **IP Address (IP Adresi)**, **Alt Ağ Maskesi** ve İlişkili Ağ Kablosuz Adı (**SSID**).

Guest (Konuk) arabirimi şunları içerir: **MAC Adresi**, **VLAN Kimliği** ve İlişkili Ağ Kablosuz Adı (**SSID**).

Bu ayarlardan herhangi birini değiştirmek için **Edit** (Düzenle) bağlantısına tıklayın.

11.1.2 Kablosuz Ayarları

Radio (Telsiz) arabirimi şunları içerir: **Telsiz modu** ve **Kanal**. Ayrıca dahili ve konuk arabirimleri için **MAC adresleri** (salt okunur) ve Ağ Adları burada gösterilmiştir. (Daha fazla bilgi için bkz. Bölüm 13: “Kablosuz Arabiriminin Ayarlama” ve Bölüm 16: “802.11 Telsiz Ayarlarını Yapılandırma”).

Bu ayarlardan herhangi birini değiştirmek için **Edit** (Düzenle) bağlantısına tıklayın.

11.2 Olay Günlükleri

Belirli bir erişim noktasının sistem olaylarını ve çekirdek günlüğünü görüntülemek için, izlemek istediğiniz erişim noktasının Yönetim Web sayfalarındaki **Status > Events** (Durum > Olaylar) sekmesine gidin.

Şekil 11.2 Erişim Noktası Olayları

Time	Type	Service	Description
Jun 4 19:14:29	info	dropbear [3074]	exit after auth (admin): Exited normally
Jun 4 19:14:29	err	dropbear [3074]	chown /dev/tty0 0 0 failed: Read-only file system
Jun 4 18:25:30	info	hostapd	wlan0: STA 00:10:c6:36:6f:1f WPA: group key poll timed out (no reply was received)
Jun 4 18:24:00	info	hostapd	wlan0: STA 00:10:c6:36:6f:1f WPA: group key exchange completed

Events (Olaylar) sekmeli sayfa *Persistence* (Süreklilik) özelliğini etkinleştirmenize ya da devre dışı bırakmanıza izin verir. Bu sayfa ayrıca tüm sistem olaylarını ve hatalarını bir Çekirdek Günlüğünde toplamak için uzak bir "günlük aktarma sunucusu" etkinleştirme seçeneği sunar. (Bu seçenek için önce uzak bir aktarma sunucusunun kurulması gereklidir. Bkz. "Çekirdek Mesajlar İçin Günlük Aktarma Sunucusu", sayfa 125). *Events* (Olaylar) sekmeli sayfa, bu erişim noktası tarafından gerçekleştirilen en güncel olayları da listeler (bkz. "Olaylar Günlüğü", sayfa 127).



Not: 9160 G2 Kablosuz Ağ Geçidi, tarih ve zaman bilgisini ağ zaman protokolünü (NTP) kullanarak elde eder. Bu veri UTC formatında (Greenwich Saati olarak da bilinir) sunulur. Sunulan zaman formatını kendi yerel saatinize göre dönüştürmeniz gerekir. Ağ zaman protokolünü ayarlama hakkında bilgi için bkz. Bölüm 25: "Ağ Zaman Protokolü Sunucusu".

11.2.1 SürekliliğiEtkinleştirme ya da Devre Dışı Bırakma

Persistence (Süreklilik), *Events* (Olaylar) sekmeli sayfadan etkinleştirilebilir veya devre dışı bırakılabilir. Sürekli günlük NVRAM'de saklanır. Cihaz yeniden başlatıldıktan sonra bile tüm sürekli günlükler hala NVRAM'de korunur. Sürekli olmayan günlükler yalnızca cihaz çalıştığı sürece saklanır. 9160 G2'yi yeniden başlatırsanız sürekli olmayan tüm günlükler silinir.

Persistence (Süreklilik) özelliğinin *Events* (Olaylar) sekmeli sayfadan etkinleştirilmesi, tüm günlüklerin NVRAM'e yazılmasını ve cihaz yeniden başlatıldıktan sonra bile kurtarılabilesini sağlar.



Not: Sürekliliğin etkinleştirilmesinin devamlı bir yazma işlemine yol açacağı unutulmamalıdır. Bu durumun AP'nin Flash elemanını yıpratma riski vardır. Bu yüksek riski hesaba katarak Sürekliliği etkinleştirmenin gerçekten ihtiyaçlarınız için gerekli olup olmadığına karar vermeniz gereklidir.

Tablo 11.1 Sürekliliği Yapılandırma Ayarları

Alan	Açıklama
<i>Relay Log</i> (Aktarma Günlüğü)	<i>Persistence</i> (Süreklilik) seçeneğini etkinleştirin ya da devre dışı bırakın.
<i>Relay Host</i> (Aktarma Sunucusu)	0 ila 7 arasında bir <i>Severity</i> (Önem Derecesi) seviyesi belirleyin. <i>Severity</i> (Önem Derecesi) 7, en düşük önem seviyesini gösterirken <i>Severity</i> (Önem Derecesi) 0, en yüksek önem seviyesini gösterir. Önem Seviyeleri hakkında ayrıntılı bilgi için bkz. "Önem Derecesi", sayfa 124.
<i>Relay Port</i> (Aktarma Bağlantı Noktası)	1 ila 128 arası bir değer girebilirsiniz. <i>Depth</i> (Derinlik) hakkında daha fazla bilgi için bkz. "Derinlik", sayfa 124.

11.2.2 Önem Derecesi

Önem Derecesi yapılandırmasının amacı Olay günlüğünde gösterilen güvenlik mesajlarını filtrelemek ya da sınırlamaktır. Büyük ihtimalle tüm mesajların listesini görmek istemezsiniz. Daha az önemli ya da değerli olanlar *Severity* (Önem Derecesi) yapılandırma özelliği kullanılarak filtrelenebilir.

Önem Derecesini 7 olarak ayarladığınızda önem derecesi 7 ile 0 arasında olan tüm mesajlar Olay günlüğünde görünür. Alternatif olarak, mesajları filtrelemek isterseniz *Önem Derecesini* 4'e ayarlayabilirsiniz. Bu durumda önem derecesi 4 ile 0 arasında olan tüm mesajlar Olay günlüğünde görünür. Böylelikle daha az önemli olan mesaj ve notlar dikkate alınmaz.

Tablo 11.2 Önem Derecesi Yapılandırma Ayarları

Önem Seviyesi	Açıklama
0	<i>Emergency</i> (Acil durum): Sistem kullanılamaz
1	<i>Alert</i> (Uyarı): Hemen önlem alınmalıdır
2	<i>Critical</i> (Kritik): Kritik durum
3	<i>Error</i> (Hata): Hatalı durum
4	<i>Warning</i> (Uyarı): Uyarı gerektiren durumlar
5	<i>Notice</i> (Dikkat): Normal ancak önem teşkil eden durum
6	<i>Informational</i> (Bilgi amaçlı): Bilgi veren mesajlar
7	<i>Debug</i> (Hata ayıklama): Hata ayıklama seviyesinde mesajlar

11.2.3 Derinlik

Depth (Derinlik) alanındaki değer NVRAM'e kaydedilebilecek günlük girişi sayısını belirler. En fazla 128 giriş kaydedebilirsiniz. AP'nizin performansını günlük mesajlarını kullanarak izlemek istiyorsanız *Depth* (Derinlik) değerini maksimuma yani **128'e** ayarlamalısınız.

11.2.4 Çekirdek Mesajlar İçin Günlük Aktarma Sunucusu

- “Uzaktan Günlük Oluşturmayı Anlama”, sayfa 125.
- “Günlük Aktarma Sunucusunu Kurma”, sayfa 125.
- “Durum, Olaylar Sayfasında Günlük Aktarma Sunucusunu Etkinleştirme/Devre Dışı Bırakma”, sayfa 126.

11.2.4.1 Uzaktan Günlük Oluşturmayı Anlama

Çekirdek Günlüğü, Sistem Günlüğünde gösterilen sistem olaylarının ve düşen kare hızı vb. hata durumları gibi çekirdek mesajlarının kapsamlı listesidir.

Çekirdek Günlüğü mesajlarını doğrudan bir erişim noktasının Yönetim Web Kullanıcı Arabiriminden görüntüleyemezsiniz. Önce syslog (sistem günlüğü) işlemi yürüten ve ağınızda syslog "günlük aktarma sunucusu" olarak çalışan bir uzak sunucu kurmanız gerekir. Bu adımdan sonra syslog mesajlarını uzak sunucuya göndermek için 9160 G2 Kablosuz Ağ Geçidi cihazını yapılandırabilirsiniz.

Uzak sunucu kullanarak erişim noktalarının syslog mesajlarını toplamanın pek çok avantajı vardır. Örneğin:

- Birden fazla erişim noktasından syslog mesajları toplayabilirsiniz.
- Mesaj geçmişini tek bir erişim noktasındakinden daha uzun süre saklayabilirsiniz.
- Kodlanan yönetim işlemlerini ve uyarıları harekete geçirebilirsiniz.

11.2.4.2 Günlük Aktarma Sunucusunu Kurma

Çekirdek Günlüğü aktarmasını kullanmak için syslog mesajlarını almak üzere bir uzak sunucu yapılandırmanız gerekir. Bu prosedür, uzak günlük sunucusu olarak kullandığınız makinenin türüne göre değişiklik gösterir. Aşağıda syslog sunucusunu kullanarak uzak bir Linux sunucusunun nasıl yapılandırıldığı bir örnekle gösterilmiştir.

Linux syslogd Kullanımına Örnek

Aşağıdaki adımlar Linux sunucusunda syslog sunucusunu etkinleştirir. Bu adımları uygulayabilmek için tam yetkili kullanıcı kimliğine sahip olduğunuzdan emin olun.

1. Syslog aktarma sunucusu olarak kullanmak istediğiniz makinede tam yetkili kullanıcı olarak oturum açın.

Sonraki işlemler tam yetkili kullanıcı izinleri gerektirir. Tam yetkili olarak oturum açmadıysanız komut satırı istemine su yazarak tam yetkili (“super user [süper kullanıcı]”) haline gelin.

2. `/etc/init.d/syslogd`'yi düzenleyin ve dosyanın üst kısmındaki `SYSLOGD` değişkenine `"-r"` ekleyin. Düzenlediğiniz satır şu şekilde görünecektir:
`SYSLOGD="-r"`
Syslogd komut seçenekleri hakkında daha fazla bilgi için kılavuz (man) sayfalarına bakın. (Komut satırına `man syslogd` yazın.)
3. Tüm mesajları bir dosyaya göndermek istiyorsanız `/etc/syslog.conf` satırını düzenleyin. Örneğin, tüm mesajları `"AP_syslog"` adlı bir günlük dosyasına kaydetmek için şu satırı ekleyebilirsiniz:
`*.*-/tmp/AP_syslog`
Syslog.conf komut seçenekleri hakkında daha fazla bilgi için kılavuz (man) sayfalarına bakın. (Komut satırına `man syslog.conf` yazın.)
4. Komut satırı istemine şunu yazarak syslog sunucusunu yeniden başlatın:
`/etc/init.d/syslogd restart`



*Not: Syslog işlemi varsayılan olarak **514** bağlantı noktasını kullanır. Bu varsayılan bağlantı noktasını kullanmanızı öneririz. Ancak günlük bağlantı noktasını yeniden yapılandırmayı tercih ederseniz syslog'a atadığınız bağlantı noktası numarasının başka bir işlem tarafından kullanılmadığından emin olun.*

11.2.4.3 Durum, Olaylar Sayfasında Günlük Aktarma Sunucusunu Etkinleştirme/Devre Dışı Bırakma

Status > Events (Durum > Olaylar) sayfasında Günlük Aktarmayı etkinleştirmek ve yapılandırmak için *Log Relay* (Günlük Aktarma) seçeneklerini aşağıda anlatıldığı şekilde ayarların ve **Update** (Güncelle) seçeneğine tıklayın.

☒ Relay Log

Relay Host

Relay Port

Tablo 11.3 Günlük Aktarma Sunucusu Ayarları

Alan	Açıklama
<i>Relay Log</i> (Aktarma Günlüğü)	Günlük Aktarma Sunucusunun kullanımını etkinleştirin ya da devre dışı bırakın: Relay Log (Aktarma Günlüğü) onay kutusunu işaretlerseniz Günlük Aktarma Sunucusu etkinleşir ve <i>Relay Host</i> (Aktarma Sunucusu) ve <i>Relay Port</i> (Aktarma Bağlantı Noktası) alanları düzenlenebilir hale gelir.
<i>Relay Host</i> (Aktarma Sunucusu)	Aktarma Sunucusunun IP Address (IP Adresi) ya da DNS adını belirleyin. Not: <i>Devicescape Wireless Operations Center</i> uygulamasını kullanıyorsanız <i>Depo Sunucusunun</i> tüm erişim noktalarından <i>syslog</i> mesajlarını alması gerekir. Bu durumda <i>Operations Center'in Depo Sunucusu IP adresini Aktarma Sunucusu olarak kullanın.</i>
<i>Relay Port</i> (Aktarma Bağlantı Noktası)	Aktarma Sunucusundaki <i>syslog</i> işlemi için Bağlantı Noktası numarası belirleyin. Varsayılan bağlantı noktası 514 'tür.

Ayarları Güncelleme

Değişikliklerinizi güncellemek için **Update** (Güncelle) seçeneğine tıklayın.

Günlük Aktarma Sunucusunu *etkinleştirdiyseniz* **Update** (Güncelle) seçeneğine tıkladığınızda uzaktan günlük oluşturmayı etkinleştirmiş olursunuz. Erişim noktası, Günlük Aktarma Sunucusunu nasıl yapılandırdığınıza bağlı olarak çekirdek mesajlarını gerçek zamanlı görüntülenmek üzere uzak günlük sunucusu ekranına, belirli bir çekirdek günlüğü dosyasına ya da başka bir depolama alanına gönderir.

Günlük Aktarma Sunucusunu *devre dışı bıraktıysanız* **Update** (Güncelle) seçeneğine tıkladığınızda uzaktan günlük oluşturmayı devre dışı bırakmış olursunuz.

11.2.5 Olaylar Günlüğü

Olaylar Günlüğü, erişim noktasındaki istasyon ilişkilendirme, kimlik doğrulama ve diğer olaylar gibi sistem olaylarını gösterir. Gerçek zamanlı Olaylar Günlüğü, her zaman izlemekte olduğunuz erişim noktasının Yönetim Web Kullanıcı Arabirimi Sayfasında *Status, Events* (Durum, Olaylar) bölümünde gösterilir.

11.3 Alma/Verme İstatistikleri

Belirli bir erişim noktasının alma/verme istatistiklerini görüntülemek için, izlemek istediğiniz erişim noktasının Yönetim Web sayfalarındaki *Status > Events* (Durum > Olaylar) sekmesine gidin.



Not: Şekil 11.3, iki telsizli AP'ler için Alma/Verme sayfasını göstermektedir. Tek telsizli AP'lerin Yönetim Web sayfası biraz daha farklı görünür.

Şekil 11.3 Alma/Verme İstatistikleri Sayfası

Basic Settings	View transmit and receive statistics for this access point			
User Management				
Cluster				
Access Points				
Sessions				
Channel Management				
Wireless Neighborhood				
Security				
Status				
Interfaces				
Events				
Transmit/Receive				
Client Associations				
Neighboring Access Points				
Manage				
Ethernet Settings				
802.11 Settings				
802.11 Advanced Settings				
VWN				

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
IP Address	10.128.75.4			
MAC Address	00:08:A2:01:4B:52	00:00:00:00:00:00	00:08:A2:01:4B:56	n/a
VLAN ID				
Name (SSID)	SFG		TEKLOGIX GUEST	

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
Total packets	11329	0	4622	0
Total bytes	3482589	0	649463	0
Errors	0	0	2	0

Type	Ethernet		Radio	
Name	Guest	Internal	Guest	
Total packets	833047	0	37	0
Total bytes	89628621	0	3190	0
Errors	0	0	0	0

Bu sayfa, Tablo 11.4, sayfa 129 üzerinde açıklandığı gibi geçerli erişim noktası hakkındaki temel bilgileri ve bu erişim noktasının alma/verme istatistiklerinin gerçek zamanlı olarak görüntülenmesiyle ilgili bilgiler sunar. Belirtilen tüm alma/verme istatistikleri erişim noktasının en son başlatıldığı andan itibaren alınan verilerin toplamını gösterir. AP yeniden başlatılırsa, bu istatistikler yeniden başlatmadan itibaren alınan alma/verme verilerinin toplamını belirtir.

Tablo 11.4 Alma/Verme İstatistikleri

Alan	Açıklama
<i>IP Address</i> (<i>IP Adresi</i>)	Erişim noktasına ait IP Address (IP Adresi).
<i>MAC Address</i> (<i>MAC Adresi</i>)	Belirtilen arabirime ait Ortam Erişim Denetimi (MAC) adresi. MAC adresi, bir arabirimi ağa tanıtan herhangi bir cihazın kalıcı ve benzersiz donanım adresidir. MAC adresi üretici tarafından atanır. 9160 G2 Kablosuz Ağ Geçidi cihazının her arabirim için benzersiz bir MAC adresi vardır. İki telsizli bir erişim noktasının her bir telsizin arabirimi için farklı bir MAC adresi vardır.
<i>VLAN ID</i> (<i>VLAN Kimliği</i>)	Sanal LAN (VLAN) Kimliği. VLAN, tek bir fiziksel ağa bağlı olmasalar bile bir ağdaki cihazların bağılıymış gibi davranmalarını sağlayan yazılım tabanlı ve mantıklı bir şekilde bir araya getirildiği cihazlar grubudur. VLAN'lar aynı erişim noktasında dahili ve konuk ağları oluşturmak için kullanılabilir.
<i>Name (SSID)</i> (<i>Ad [SSID]</i>)	Kablosuz ağ adı. SSID olarak da bilinen bu alfanümerik anahtar, benzersiz bir kablosuz yerel alan ağı belirler. SSID, Basic Settings (Temel Ayarlar) sekmesinden ayarlanır. (Bkz. "Ağ Ayarlarını Sağlama", sayfa 49.)
Alma-Verme Bilgileri	
<i>Total Packets</i> (<i>Toplam Paket Sayısı</i>)	Bu erişim noktası tarafından gönderilen (Transmit [Verme] tablosunda) veya alınan (Receive [Alma] tablosunda) toplam paketleri gösterir.
<i>Total Bytes</i> (<i>Toplam Bayt</i>)	Bu erişim noktası tarafından gönderilen (Transmit [Verme] tablosunda) veya alınan (Receive [Alma] tablosunda) toplam bayt miktarını gösterir.
<i>Errors</i> (<i>Hatalar</i>)	Bu erişim noktasında veri gönderme ve almayla ilgili toplam hataları gösterir.

11.4 İlişkili Kablosuz İstemciler

Belirli bir erişim noktasıyla ilişkili istemci istasyonlarını görüntülemek için, izlemek istediğiniz erişim noktasının Yönetim Web sayfalarındaki *Status > Client Associations* (Durum > İstemci İlişkileri) sayfasına gidin.

İlişkili istasyonlar, her istasyonda alınan ve verilen paket trafiği bilgisiyle beraber gösterilir. (bkz Şekil 11.4, sayfa 130).

Şekil 11.4 İlişkili İstemci İstasyonları

Basic Settings	View list of currently associated client stations							
User Management								
Cluster								
Access Points	Network	Station	Status		From Station		To Station	
Sessions			Authenticated	Associated	Packets	Bytes	Packets	Bytes
Channel Management	wlan0	00:0c:f1:3e:99:ae	Yes	Yes	1732	261063	1517	510274
Wireless Neighborhood	wlan0	00:90:4b:93:f4:35	Yes	Yes	687	123005	572	155409
Security								
Status								
Interfaces								
Events								
Transmit/Receive								
Client Associations								
Neighboring Access Points								

11.4.1 Bağlantı Bütünlüğünü İzleme

9160 G2 Kablosuz Ağ Geçidi her bir ilişkili istemciyle olan bağlantısını sürekli olarak doğrulamak için (veri alışverişi olmadığında bile) *bağlantı bütünlüğünü izleme* özelliği sunar. Bunu yapmak için AP, devam eden başka bir trafik yokken istemcilere birkaç saniyede bir veri paketi gönderir. Bu sayede erişim noktası, normal trafiğin olmadığı zamanlarda bile istemcilerin ne zaman menzilden çıktığını tespit edebilir. Bir istemci 300 saniye kaybolduğunda (ilişkisi kesilmese bile menzilden çıktığında) istemci bağlantısı ilişkili istemciler listesinden çıkar.

11.5 Komşu Erişim Noktaları

"Komşu erişim noktaları" durum sayfası, Yönetim Web sayfalarını görüntülediğiniz erişim noktasının menzilineki tüm erişim noktalarının gerçek zamanlı istatistiklerini sunar. Kablosuz ağdaki diğer erişim noktaları hakkındaki bilgileri görüntülemek için *Status > Neighboring Access Points* (Durum > Komşu Erişim Noktaları) sayfasına gidin (bkz. Şekil 11.5, sayfa 131).

Şekil 11.5 Komşu Erişim Noktalarının Durumu

View neighboring access points													
AP Detection <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled <input type="button" value="Update"/>													
MAC	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates	
00:08:a2:01:13:20	100	AP		On	Off	2.4	11	1		2	Fri Jan 2 06:33:01 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:22:34	100	AP		On	On	2.4	3	1		3	Fri Jan 2 06:31:23 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:12:fc	100	AP		On	Off	2.4	6	1		1	Fri Jan 2 06:26:45 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:01:22:30	100	AP		On	On	2.4	6	1		1	Fri Jan 2 06:26:07 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	
00:08:a2:02:73:e4	100	AP	steve	On	On	2.4	6	1		6616	Fri Jan 2 06:34:40 1970	1,2,5,5,6,9,11,12,18,24,36,48,54	

Komşu erişim noktalarıyla ilgili bilgiler Tablo 11.5 üzerinde gösterilmiştir.

Tablo 11.5 Komşu Erişim Noktası İstatistikleri

Alan	Açıklama
<i>MAC</i>	Komşu erişim noktasının MAC adresini gösterir. MAC adresi bir ağdaki her düğümü benzersiz biçimde tanımlayan bir donanım adresidir.
<i>Radio (Telsiz)</i>	İki Telsizli AP'ler Komşu AP'leri "algılayan" erişim noktası iki telsizli bir erişim noktasıysa Radio (Telsiz) alanı dahil edilir. Radio (Telsiz) alanı komşu AP'nin şu telsizlerden hangisinde algılandığını belirtir: <ul style="list-style-type: none"> wlan0 (Telsiz 1) wlan1 (Telsiz 2) Tek Telsizli AP'ler Bu alan tek telsizli erişim noktalarının <i>Neighboring Access Points</i> (Komşu Erişim Noktaları) sayfasında bulunmaz.
<i>Beacon Int. (Uyarı Aralığı)</i>	Bu erişim noktasının kullandığı Uyarı aralığını gösterir. Uyarı anonsları, kablosuz ağların varlığını duyurmak için erişim noktası tarafından düzenli aralıklarla iletilir. Varsayılan olarak her 100 milisaniyede bir (ya da her 10 saniyede bir) uyarı anonsu gönderilir. Uyarı Aralığı <i>Manage > 802.11 Advanced Settings</i> (Yönet > 802.11 Gelişmiş Ayarları) sekmesi sayfa ayarları. (Bkz. Bölüm 16: "802.11 Telsiz Ayarlarını Yapılandırma".)
<i>Capability (Özellik)</i>	İkili sisteme dönüştürüldüğünde her IEEE 802.11 özelliğini ya da işlevini belirten ve bu erişim noktasında "açık" mı yoksa "kapalı" mı olduğunu gösteren onaltılık sistemdeki bir sayıdır.

Tablo 11.5 Komşu Erişim Noktası İstatistikleri (Devamı)

Alan	Açıklama
<i>Type (Tür)</i>	<p>Cihaz türünü belirtir:</p> <ul style="list-style-type: none">• AP, komşu cihazın Altyapı Modu içindeki IEEE 802.11 Kablosuz Ağ Çerçevesi ögesini destekleyen bir erişim noktası olduğunu belirtir.• Ad hoc, Ad hoc Modu ile çalışan bir komşu istasyonu belirtir. Ad hoc moduna ayarlanan istasyonlar standart bir erişim noktası kullanmadan doğrudan kendi aralarında iletişim kurar. Ad-hoc modu, "uçtan uca" modu ya da Bağımsız Temel Hizmet Kümesi (IBSS) olarak da bilinen bir IEEE 802.11 Kablosuz Ağ Çerçevesi ögesidir.
<i>SSID</i>	<p>Erişim noktasının Hizmet Kümesi Tanımlayıcısıdır (SSID).</p> <p>SSID, en çok 32 karakterden oluşan ve bir kablosuz yerel alan ağını benzersiz biçimde tanımlayan alfanümerik bir dizedir. "Ağ Adı" olarak da bilinir.</p> <p>SSID, Basic Settings (Temel Ayarlar) bölümünde (bkz. Bölüm 5: "Temel Ayarları Yapılandırma") ya da <i>Manage > Wireless Settings</i> (Yönet > Kablosuz Ayarları) bölümünde ayarlanır (bkz Bölüm 13: "Kablosuz Arabiriminin Ayarlama").</p> <p>Aynı erişim noktasındaki bir Konuk ağı ve Dahili ağ her zaman iki farklı ağ adına sahip olmalıdır.</p>
<i>Privacy (Gizlilik)</i>	<p>Komşu cihazda herhangi bir güvenliğin olup olmadığını belirtir.</p> <ul style="list-style-type: none">• Off (Kapalı), komşu cihazda Güvenlik modunun "Yok" olarak ayarlandığını (güvenliğin olmadığını) belirtir.• On (Açık), komşu cihazda bazı güvenlik önlemlerinin olduğunu belirtir. <p>Güvenlik AP'de, <i>Security</i> (Güvenlik) sekmesi sayfada yapılandırılır. Güvenlik ayarları hakkında daha fazla bilgi için bkz. Bölüm 10: "Güvenliği Yapılandırma".</p>
<i>WPA</i>	<p>Bu erişim noktasında WPA güvenliğin On (Açık) ya da Off (Kapalı) olduğunu gösterir.</p>
<i>Band (Bant)</i>	<p>IEEE 802.11 modunun bu erişim noktasında kullanıldığını belirtir. (Örnek: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)</p> <p>Gösterilen sayı aşağıda belirtilen şekilde modları belirtir:</p> <ul style="list-style-type: none">• 2.4 IEEE 802.11b modunu ya da IEEE 802.11g modunu belirtir.• 5 IEEE 802.11a modunu belirtir.

Tablo 11.5 Komşu Erişim Noktası İstatistikleri (Devamı)

Alan	Açıklama
<i>PHY</i>	<p>IEEE 802.11 modunun bu erişim noktasında kullanıldığını belirtir. (Örnek: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)</p> <p>Gösterilen sayı aşağıda belirtilen şekilde modları belirtir:</p> <ul style="list-style-type: none">• 4 IEEE 802.11b modunu belirtir• 7 IEEE 802.11g modunu belirtir• 8 IEEE 802.11a modunu belirtir• 256 Atheros Turbo modunu belirtir
<i>Channel (Kanal)</i>	<p>Erişim noktasının o an hangi kanalda yayın yaptığını gösterir.</p> <p>Kanal, telsizin alma/verme için kullandığı telsiz spektrumu kısmını tanımlar.</p> <p>Kanal, <i>Radio Settings</i> (Telsiz Ayarları) bölümünde ayarlanır. (Bkz. Bölüm 16: “802.11 Telsiz Ayarlarını Yapılandırma”.)</p>
<i>Rate (Hız)</i>	<p>Erişim noktasının o anda hangi hızda aktarım yaptığını (megabit/saniye cinsinden) gösterir.</p> <p>Geçerli hız her zaman <i>Rates</i> (Hızlar) kısmında gösterilen desteklenen hızlardan biridir.</p>
<i>Signal (Sinyal)</i>	<p>Bu erişim noktasından yayılan ve desibel (Db) cinsinden ölçülen telsiz sinyalinin gücünü belirtir.</p>

Tablo 11.5 Komşu Erişim Noktası İstatistikleri (Devamı)

Alan	Açıklama
<i>ERP</i>	<p><i>Genişletilmiş Hız Protokolü (ERP) IEEE 802.11g</i> istasyonları tarafından kullanılan protokolü belirtir.</p> <p>Bu alan, bu erişim noktasını kullanan bir <i>IEEE 802.11g</i> istemci istasyonunun, aynı kanalda <i>IEEE 802.11g</i> (ERP) istasyonu ile aynı <i>IEEE 802.11b</i> (ERP olmayan) istasyonlar ya da erişim noktaları olduğunda nasıl veri göndereceğini belirtir.</p> <p>Bir <i>IEEE 802.11g</i> istasyonu, ağda kendi kullandığı kanalı kullanan bir ya da daha fazla <i>IEEE 802.11b</i> düğümü olduğuna belirlerse <i>request-to-send</i> (gönderme istem kodu) (<i>RTS</i>) ve <i>clear-to-send</i> (göndermeye müsait) (<i>CTS</i>) korumalarını etkinleştirir.</p> <p>Geçerli kullanıcı arabiriminde gösterilen onaltılık sistemdeki sayı ikili sisteme dönüştürüldüğünde ERP işaretinin nasıl ayarlandığını gösterir.</p> <p>Bu AP için geçerli ERP ayarını belirlemek için aşağıdaki bilgileri izleyin:</p> <ul style="list-style-type: none">• 0x0, "Yok" anlamına gelir. Hiç <i>IEEE 802.11b</i> (ERP olmayan) istasyonunun mevcut olmadığını belirtir.• 0x1, bir <i>IEEE 802.11b</i> (ERP olmayan) cihazın mevcut olduğunu belirtir. Bu AP yalnızca <i>IEEE 802.11b</i> istasyonuna sahiptir. (Bu işaret hiçbir zaman tek başına kullanılmamalıdır.)• 0x2, <i>IEEE 802.11g</i> istasyonlarının <i>RTS/CTS</i> korumasını kullanması gerektiğini belirtir. Aynı kanalda yalnızca <i>IEEE 802.11b</i> istemci istasyonuna sahip bir AP daha vardır.• 0x3, ERP olmayan bir cihazın bulunduğunu ve <i>IEEE 802.11g</i> istasyonlarının <i>RTS/CTS</i> korumasını kullanması gerektiğini belirtir.• 0x4, <i>IEEE 802.11g</i> istasyonlarının Barker ön işaretini kullanması gerektiğini belirtir.• 0x5, <i>IEEE 802.11g</i> istasyonlarının 0x1 ile aynı protokolü Barker ön işaretiyle kullanması gerektiğini belirtir.• 0x6, <i>IEEE 802.11g</i> istasyonlarının 0x2 ile aynı protokolü Barker ön işaretiyle kullanması gerektiğini belirtir.• 0x7, <i>IEEE 802.11g</i> istasyonlarının 0x3 ile aynı protokolü Barker ön işaretiyle kullanması gerektiğini belirtir.
<i>Beacons (Uyarılar)</i>	Bu erişim noktasının en son başlatıldığı andan itibaren gönderdiği uyarıların sayısını belirtir.
<i>Last Beacon (Son Uyarı)</i>	Bu erişim noktasından gönderilen en son uyarının tarihini ve saatini gösterir.
<i>Rates (Hızlar)</i>	<p>Komşu erişim noktaları için desteklenen ve temel (bildirilen) hız gruplarını gösterir. Hızlar megabit/saniye (Mb/sn) cinsinden gösterilir.</p> <p>Tüm Desteklenen Hızlar listelenmiştir. Temel Hızlar kalın rakamlarla vurgulanmıştır.</p> <p>Hız grupları <i>Radio Settings</i> (Telsiz Ayarları) bölümünde yapılandırılır. (Bkz. Bölüm 16: "802.11 Telsiz Ayarlarını Yapılandırma".) Bir erişim noktası için gösterilen hızlar, <i>Radio Settings</i> (Telsiz Ayarları) bölümünde o AP için belirlenmiş mevcut hızlarla her zaman aynı olacaktır.</p>

ETHERNET (KABLOLU) ARABİRİMİ

12

12.1 Ethernet (Kablolu) Ayarlarına Gitme	137
12.1.1 DNS Ana Bilgisayar Adı	138
12.1.2 Konuk Erişimi.	138
12.1.2.1 Dahili Bir LAN ve Konuk Ağı Yapılandırma	138
12.1.2.2 Konuk Erişimini Etkinleştirme ya da Devre Dışı Bırakma	139
12.1.2.3 Sanal Konuk Ağı Belirleme	139
12.1.3 Sanal Kablosuz Ağlar	140
12.1.4 Dahili Arabirim Ayarları	141
12.1.5 Guest Interface Settings (Konuk Arabirimi Ayarları).	143
12.1.6 Ayarları Güncelleme	143

Ethernet (Kablolu) Ayarları, **Ethernet** yerel alan ağınızın (**LAN**) nasıl yapılandırılacağını anlatır.



*Not: Ethernet Ayarları küme elemanları arasında paylaşılmaz. Bu ayarlar Yönetim sayfalarında her erişim noktası için ayrı ayrı yapılandırılmalıdır. Geçerli kümenin üyesi olan bir erişim noktasının Yönetim Web sayfasına gitmek için, geçerli AP'nin Cluster > Access Points (Küme > Erişim Noktaları) sayfasındaki **IP Adresi** bağlantısına tıklayın. Küme elemanlarının paylaştığı ayarlar hakkında daha fazla bilgi için bkz. "Hangi Ayarlar Küme Yapılandırmasının Bir Parçası Olarak Paylaşılır, Hangileri Paylaşılmaz?", sayfa 57.*

12.1 Ethernet (Kablolu) Ayarlarına Gitme

9160 G2 Kablosuz Ağ Geçidi cihazında "Kablolu" adresini ve ilgili ayarları yapılandırmak için **Manage > Ethernet Settings** (Yönet > Ethernet Ayarları) sekmesine gidin ve ilgili alanları aşağıda anlatıldığı gibi güncelleyin.

Şekil 12.1 Ethernet Ayarlarına Genel Bakış

Basic Settings	Modify Ethernet (Wired) settings
User Management	DNS Hostname: PTX9160-Wireless-AP
Cluster	Guest Access: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Access Points	For Guest Access: VLAN on Ethernet Port
Sessions	Virtual Wireless Networks (Using VLANs on Ethernet Port 1): <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Channel Management	Internal Interface Settings
Wireless Neighborhood	MAC Address: 00:08:A2:01:4B:52
Security	VLAN ID: 2
Status	Management VLAN ID: 2
Interfaces	Untagged VLAN: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Events	Untagged VLAN ID: 1
Transmit/Receive	Connection Type: DHCP
Client Associations	Static IP Address: 192 . 168 . 1 . 10
Neighboring Access Points	Subnet Mask: 255 . 255 . 255 . 0
Manage	Default Gateway: 192 . 168 . 1 . 254
Ethernet Settings	DNS Settings via DHCP: <input checked="" type="radio"/> On <input type="radio"/> Off
802.11 Settings	DNS Nameservers:
802.11 Advanced Settings	DNS Domain: example.com
VWN	Guest Interface Settings
WDS	MAC Address: 00:00:00:00:00:00
Guest Login	VLAN ID:
MAC Filtering	Subnet: n/a
Load Balancing	<input type="button" value="Update"/>
Services	
QoS	

12.1.1 DNS Ana Bilgisayar Adı

Tablo 12.1 DNS Adını Ayarlama

Alan	Açıklama
<i>DNS Hostname</i> (<i>DNS Ana Bilgisayar Adı</i>)	<p>Erişim noktasının DNS adını metin kutusuna yazın.</p> <p>Bu, ana bilgisayar adıdır. ISP ya da ağ yöneticiniz tarafından veya sizin tarafınızdan sağlanabilir.</p> <p>Sistem adlarıyla ilgili kurallar şunlardır:</p> <ul style="list-style-type: none">• Bu ad en fazla 20 karakter uzunluğunda olabilir.• Yalnızca harfler, sayılar ve çizgiler kullanılabilir.• Ad, bir harfle başlamalı ve bir harf ya da sayıyla bitmelidir.

12.1.2 Konuk Erişimi

Aynı 9160 G2 Kablosuz Ağ Geçidi cihazında izole bir ağ üzerinden kontrollü konuk erişimi ve güvenli bir dahili **LAN** sağlayabilirsiniz.

12.1.2.1 Dahili Bir LAN ve Konuk Ağı Yapılandırma

Yerel Alan Ağı (LAN) bir binanın tek katı gibi kısıtlı alanları kapsayan bir iletişim ağıdır. LAN, birden fazla bilgisayar ile depolama cihazları ve yazıcılar gibi diğer ağ cihazlarını birbirine bağlar.

Ethernet, LAN'ı uygulayan en yaygın teknolojidir. **Wi-Fi (IEEE)** de bir diğer popüler LAN teknolojisidir.

9160 G2 Kablosuz Ağ Geçidi aynı erişim noktasında iki farklı LAN yapılandırmanıza imkan sağlar: Biri, güvenli *dahili* LAN, diğeri hiçbir güvenlik ayarı olmayan, dahili kaynaklara çok az ya da sıfır erişimi olan genel *konuk* ağı. Bu ağları yapılandırmak için hem Kablosuz hem de Ethernet (Kablolu) ayarları sağlamanız gerekir.

Ethernet (Kablolu) ayarlarının nasıl yapılandırıldığı hakkında daha fazla bilgi için aşağıdaki bölümlere bakın.

(Kablosuz ayarların nasıl yapılandırıldığı hakkında bilgi için bkz. Bölüm 13: “Kablosuz Arabiriminin Ayarlama”. Konuk Arabiriminin nasıl oluşturulduğu hakkında genel bilgiler için bkz. Bölüm 14: “Konuk Erişiminin Ayarlama”).

12.1.2.2 Konuk Erişimini Etkinleştirme ya da Devre Dışı Bırakma

9160 G2 Kablosuz Ağ Geçidi cihazında Konuk Erişimi özelliği varsayılan olarak **devre dışıdır**. AP'nize konuk erişimi sağlamak istiyorsanız *Ethernet (Wired) Settings* (Ethernet (Kablolu) Ayarları) sekmesine gidin.

Tablo 12.2 Konuk Erişimini Etkinleştirme/Devre Dışı Bırakma

Alan	Açıklama
<i>Guest Access</i> (Konuk Erişimi)	9160 G2 Kablosuz Ağ Geçidi cihazında Konuk Erişimi varsayılan olarak devre dışıdır . <ul style="list-style-type: none">Konuk Erişimini etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.Konuk Erişimini devre dışı bırakmak için Disabled (Devre dışı) seçeneğine tıklayın.

12.1.2.3 Sanal Konuk Ağı Belirleme

Konuk Erişimini etkinleştirirseniz erişim noktasındaki LAN bağlantı noktasını **VLAN** özellikli bir anahtardaki etiketli bir bağlantı noktasına bağladıktan sonra bu Yönetim sayfasında iki farklı Sanal LAN tanımlayarak bu erişim noktasında *sanal olarak* hem "Dahili" hem de "Konuk Ağı" oluşturmanız gerekir. (Daha fazla bilgi için bkz. Bölüm 14: "Konuk Erişimini Ayarlama"). Sanal olarak ayrı olan dahili ve konuk LAN'larını Tablo 12.3'te açıklandığı gibi oluşturun.

Tablo 12.3 Sanal Konuk Ağı Belirleme

Alan	Açıklama
<i>Guest Access</i> (Konuk Erişimi)	<ul style="list-style-type: none">Konuk Erişimini etkinleştirmek için Enabled (Etkin) seçeneğini belirleyin. (Bu seçeneği belirlerseniz bir sonraki ayar olan <i>For Guest access use</i> [Konuk erişiminin kullanılması için] ayarında VLAN'ları seçmeniz ve ardından sayfanın geri kalanında Konuk Ağın VLAN'ları hakkında bilgi vermeniz gerekir).Konuk Erişimini devre dışı bırakmak için Disabled (Devre Dışı) seçeneğini belirleyin.

Tablo 12.3 Sanal Konuk Ağı Belirleme (Devamı)

Alan	Açıklama
<i>For Guest Access (Konuk Erişimi İçin)</i>	<p>Bu erişim noktasında <i>sanal olarak</i> ayrı bir konuk ağı belirtin:</p> <ul style="list-style-type: none">Erişim noktası dahili LAN'ınıza yalnızca bir fiziksel bağlantıyla bağlandığından açılır menüden VLAN on Ethernet Port 1 (Ethernet Bağlantı Noktası 1'de VLAN) seçeneğini belirleyin. Bu işlem, bir VLAN ID'si sunmanız gereken "VLAN" ayarlarını etkinleştirir. Bkz. "Guest Interface Settings (Konuk Arabirimi Ayarları)", sayfa 143. <p>Önemli: <i>VLAN kullanmak için Konuk ve Dahili arabirimlerini yeniden yapılandırmanız erişim noktası bağlantınızı yitirebilirsiniz. Öncelikle, kullandığınız anahtarın ve DHCP sunucusunun IEEE 802.1Q standardına uygun şekilde VLAN'ları desteklediğini doğrulayın. Manage > Ethernet Settings (Yönet > Ethernet Ayarları) sayfasında VLAN'ı yapılandırdıktan sonra anahtardaki Ethernet kablosunu etiketli paket (VLAN) bağlantı noktasına fiziksel olarak yeniden bağlayın. Ardından Yönetim Web sayfaları aracılığıyla yeni IP adresine yeniden bağlanın. (Gerekirse VLAN ve DHCP yapılandırmalarıyla ilgili altyapı destek yöneticisine danışın.)</i></p>

12.1.3 Sanal Kablosuz Ağlar

Dahili ağı VLAN olarak yapılandırmak istiyorsanız (yapılandırılmış bir Konuk aığınız olsa da olmasa da) erişim noktasında "Sanal Kablosuz Ağları" etkinleştirebilirsiniz.

VLAN'larda ek sanal ağlar yapılandırmak istiyorsanız *Manage > VWN* (Yönet VWN) sekmesine giderek bu özelliği "VLAN'ları Yapılandırma", sayfa 161'de açıklandığı gibi etkinleştirebilirsiniz.

Tablo 12.4 Sanal Kablosuz Ağları Etkinleştirme

Alan	Açıklama
<i>Virtual Wireless Networks (Using VLANs on Ethernet Port 1) (Sanal Kablosuz Ağlar [Ethernet Bağlantı Noktası 1'deki VLAN'ları Kullanma])</i>	<ul style="list-style-type: none"><i>Enabled</i> (Etkin) seçeneğini belirleyerek VLAN'ları Dahili ağ ve ilave ağlar için etkinleştirin. (Bu seçeneği belirlerseniz yapılandırılmış bir Konuk Erişiminiz olsa da olmasa da VLAN'da Dahili ağı çalıştırabilir ve <i>Manage > VWN</i> (Yönet > VWN) sekmesinden "VLAN'ları Yapılandırma", sayfa 161'de açıklandığı gibi VLAN üzerinde ilave ağlar kurabilirsiniz.)<i>Disabled</i> (Devre Dışı) seçeneğini belirleyerek VLAN'ı Dahili ağ ve erişim noktasındaki diğer sanal ağlar için devre dışı bırakın.

12.1.4 Dahili Arabirim Ayarları

Dahili LAN'a yönelik Ethernet (Kablolu) ayarlarını yapılandırmak için ilgili alanları Tablo 12.5'te anlatıldığı gibi doldurun.

Tablo 12.5 Dahili LAN Ethernet Ayarları

Alan	Açıklama
<i>MAC Address (MAC Adresi)</i>	Erişim noktasındaki Ethernet bağlantı noktasının Dahili arabiriminin MAC adresini gösterir. Bu alan salt okunurdur, değiştirilemez.
<i>VLAN ID (VLAN Kimliği)</i>	<p>Dahili ve Konuk ağlarını "VLAN" ile yapılandırmayı seçtiğinizde bu alan etkinleştirilir.</p> <p>Dahili VLAN için 1 - 4094 arası bir sayı belirleyin.</p> <p>Bu eylem, erişim noktasının VLAN etiketli DHCP istekleri göndermesine yol açar. Anahtar ve DHCP sunucusu VLAN IEEE 802.1p çerçevelerini desteklemelidir. Erişim noktası DHCP sunucusuna erişebilmelidir.</p> <p>VLAN ve DHCP yapılandırmalarıyla ilgili Yöneticiye danışın.</p>
<i>Management VLAN ID (Yönetim VLAN Kimliği)</i>	<p>VWN'leri ya da Konuk erişimini VLAN aracılığıyla etkinleştirdiyse bu alan etkinleştirilir.</p> <p>Yönetim VLAN Kimliği için bir değer girin. Bu kimlik 1 - 4094 arası bir değer olabilir.</p> <p>Yönetim VLAN Kimliği, AP yönetilirken kullanılan VLAN'ı belirlemenizi sağlar. Bu VLAN'ı kullanarak AP'yi Web Kullanıcısı Arabirimi, Komut Satırı Arabirimi ve SNMP aracılığıyla yönetebilirsiniz.</p> <p>Bağlantı Türünün DHCP olarak ayarlanması erişim noktasının DHCP isteklerini VLAN etiketiyle göndermesine sebep olur. Anahtar ve DHCP sunucusu VLAN IEEE 802.1Q çerçevelerini desteklemelidir. Erişim noktası DHCP sunucusuna erişebilmelidir.</p> <p>Belirttiğiniz Yönetim VLAN Kimliğinde herhangi bir kısıtlama yoktur. Yönetim VLAN Kimliği; Dahili VLAN Kimliği, Konuk VLAN Kimliği, VWN VLAN Kimliği ve Etiketsiz VLAN Kimliği ile aynı olabilir.</p>
<i>Untagged VLAN (Etiketsiz VLAN)</i>	<p>VLAN aracılığıyla VWN'leri ve Konuk erişimini etkinleştirdiyse etiketsiz VLAN'ları etkinleştirebilir ya da devre dışı bırakabilirsiniz.</p> <p><i>Untagged VLAN</i> (Etiketsiz VLAN)'ı etkinleştirmek için Enabled (Etkin) seçeneğini belirleyin.</p> <p><i>Untagged VLAN</i> (Etiketsiz VLAN)'ı devre dışı bırakmak için Disabled (Devre Dışı) seçeneğini belirleyin.</p> <p><i>Etiketsiz VLAN</i> etkinleştirildiyse alınan paketlerden VLAN etiketi olmayanlar, belirtilen Etiketsiz VLAN Kimliği ile alınmışlar gibi davranılır.</p> <p><i>Etiketsiz VLAN</i> devre dışı bırakıldıysa alınan paketlerden VLAN etiketi olmayanlar, WDS bağlantılarına köprülenir. Köprülenmeyenler AP tarafından kullanılamaz.</p>

Tablo 12.5 Dahili LAN Ethernet Ayarları (Devamı)

Alan	Açıklama
<i>Untagged VLAN ID (Etiketsiz VLAN Kimliği)</i>	<p><i>Etiketsiz VLAN'ı etkinleştirdiyseniz bu alan etkinleşir.</i></p> <p><i>Etiketsiz VLAN Kimliği için bir değer girin. Bu değer 1 - 4094 arası olabilir.</i></p> <p>Belirttiğiniz Etiketsiz VLAN Kimliğinde herhangi bir kısıtlama yoktur. Etiketsiz VLAN Kimliği; Dahili VLAN Kimliği, Konuk VLAN Kimliği, VWN VLAN Kimliği ve Yönetim VLAN Kimliği ile aynı olabilir.</p>
<i>Connection Type (Bağlantı Türü)</i>	<p>DHCP ya da Static IP (Statik IP)'yi seçebilirsiniz.</p> <p><i>Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)</i>, merkezi bir sunucunun ağdaki cihazlara ağ yapılandırma bilgilerini nasıl sağlayacağını belirleyen bir protokoldür. DHCP sunucusu, istemci sistemine bir "kontrat" "sunar". Sağlanan bilgiler arasında IP adresleri, net maskeleri ve ayrıca DNS sunucularının adresleri ve ağ geçitleri yer alır.</p> <p><i>Statik IP</i>, tüm ağ ayarlarının manuel olarak sağlandığını belirtir. 9160 G2 Kablosuz Ağ Geçidi cihazının IP adresini, alt ağ maskesini, varsayılan ağ geçidinin IP adresini ve en az bir DNS ad sunucusunun IP adresini sağlamalısınız.</p> <p>DHCP'yi seçerseniz 9160 G2 Kablosuz Ağ Geçidi, DHCP Sunucusundan IP Adresini, alt ağ maskesini, DNS ve ağ geçidi bilgilerini alır.</p> <p>Statik IP'yi seçerseniz alanları <i>Static IP Settings</i> (Statik IP Ayarları) kısmında anlatıldığı gibi doldurun.</p> <p>Önemli: <i>Dahili ağınızda bir DHCP sunucusu yoksa ve kullanmayı da düşünmüyorsanız AP'yi başlattıktan sonra yapmanız gereken ilk şey, Bağlantı Türünü "DHCP"den "Static IP"ye (Statik IP) dönüştürmektir. Bağlantı Türünü Statik IP'ye dönüştürdüğünüzde AP'ye yeni bir Statik IP Adresi atayabilir ya da varsayılan adresi kullanabilirsiniz. Yeni bir adres atamanızı öneririz. Böylece, ileride aynı ağa başka bir 9160 G2 Kablosuz Ağ Geçidi eklerseniz her AP'nin IP adresi farklı olur.</i></p> <p>Varsayılan Statik IP adresini kurtarmanız gerektiğinde AP'yi "Fabrika Varsayılanları Yapılandırmasına Sıfırlama", sayfa 316'da anlatıldığı gibi varsayılan ayarlarına sıfırlayabilirsiniz.</p>
<i>Static IP Address (Statik IP Adresi)</i>	<p>Bağlantı Türü olarak Static IP'yi (Statik IP) seçtiğinizde bu alanlar etkinleşir.</p> <p>Statik IP adresini metin kutusuna yazın.</p>
<i>Subnet Mask (Alt Ağ Maskesi)</i>	<p>Alt Ağ Maskesini metin kutusuna yazın. Bu bilgiyi ISP ya da ağ yöneticinizden almanız gerekir.</p>
<i>Default Gateway (Varsayılan Ağ Geçidi)</i>	<p>Varsayılan Ağ Geçidini metin kutusuna yazın.</p>

Tablo 12.5 Dahili LAN Ethernet Ayarları (Devamı)

Alan	Açıklama
<i>DNS Settings via DHCP (DHCP aracılığıyla DNS Ayarları)</i>	<p>Alan Adı Sunucusu (DNS), bir ağ kaynağının açıklayıcı adını nümerik IP adresine dönüştüren bir sistemdir. Bu seçeneği etkinleştirmeyi seçebilirsiniz. Bu durumda DNS sunucularının IP adresleri DHCP aracılığıyla otomatik olarak atanır. (Bu seçenek yalnızca <i>Connection Type</i> (Bağlantı Türü) kısmında DHCP'yi seçtiğinizde kullanılabilir).</p> <p>Off (Kapalı) seçeneğini belirlerseniz statik IP adreslerini manuel olarak atamanız gerekir.</p>
<i>DNS Nameservers (DNS Ad Sunucuları)</i>	<p>Alan Adı Hizmeti (DNS), bir ağ kaynağının (örneğin, www.pSIONteklogix.com) açıklayıcı adını (<i>alanadı</i>) nümerik IP adresine (örneğin, 66.93.138.219) dönüştürür. DNS sunucusuna <i>Ad Sunucusu</i> denir.</p> <p>Genellikle biri Birincil Ad Sunucusu, diğeri İkincil Ad Sunucusu olmak üzere iki Ad Sunucusu vardır.</p>
<i>DNS Domain (DNS Alan Adı)</i>	DNS sunucularının alan adını tanımlayın.

12.1.5 Guest Interface Settings (Konuk Arabirimi Ayarları)

"Konuk" arabirimi Ethernet (Kablolu) Ayarlarını yapılandırmak için ilgili alanları aşağıda anlatıldığı gibi doldurun.

Tablo 12.6 Konuk Arabirimi Ethernet Ayarlarını Yapılandırma

Alan	Açıklama
<i>MAC Address (MAC Adresi)</i>	Erişim noktasındaki Ethernet bağlantı noktasının Konuk arabiriminin MAC adresini gösterir. Bu alan salt okunurdur, değiştirilemez.
<i>VLAN ID (VLAN Kimliği)</i>	Dahili ve Konuk ağlarını "VLAN" ile yapılandırmayı seçtiğinizde bu alan etkinleştirilir . Konuk VLAN için 1 - 4094 arası bir sayı belirleyin.
<i>Subnet (Alt Ağ)</i>	Konuk arabirimi için alt ağ adresini gösterir. Örnek: 192 . 168 . 1 . 0.

12.1.6 Ayarları Güncelleme

Ethernet ayarlarını güncellemek için:

1. *Ethernet Settings* (Ethernet Ayarları) sayfasına gidin.
2. Ethernet ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

KABLOSUZ ARABİRİMİNİ AYARLAMA

13

13.1 Kablosuz Ayarlarına Gitme	147
13.2 802.11d Düzenleyici Etki Alanı Desteğini Yapılandırma.	148
13.3 802.11h Düzenleyici Etki Alanı Kontrolü	148
13.4 Telsiz Arabirimini Yapılandırma	149
13.5 "Dahili" Kablosuz LAN Ayarlarını Yapılandırma	150
13.6 "Konuk" Ağı Kablosuz Ayarlarını Yapılandırma	151
13.7 Kablosuz Ayarlarını Güncelleme	152

Kablosuz Ayarları yerel alan ağının (**LAN**) özellikle erişim noktasındaki telsiz cihazıyla (**802.11** Modu ve Kanal) ve erişim noktası ağ arabirimiyle ilgili özelliklerini açıklar (Erişim noktası **MAC** adresi ve Kablosuz Ağ adı, **SSID** olarak da bilinir).

Aşağıdaki bölümler 9160 G2 Kablosuz Ağ Geçidi cihazında "Kablosuz" adresinin ve 802.IQv1 gibi ilgili ayarların nasıl yapılandırıldığını anlatmaktadır.

13.1 Kablosuz Ayarlarına Gitme

Bir erişim noktasının kablosuz adresini ayarlamak için *Manage > 802.11 Settings* (Yönet 802.11 Ayarları) sekmesine gidin. Açılan *Wireless Settings* (Kablosuz Ayarları) sayfasında ilgili alanları aşağıda anlatıldığı gibi güncelleyin.



Not: Şekil 13.1, iki telsizli AP'ler için Kablosuz Ayarları sayfasını gösterir. Tek telsizli AP'lerin Yönetim Web sayfası biraz daha farklı görünür.

Şekil 13.1 Kablosuz Ayarları Yapılandırması

Basic Settings	Modify wireless settings	
User Management	802.11d Regulatory Domain Support <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Cluster	IEEE802.11h support present.	
Access Points	Radio Interface	
Sessions	Mode	IEEE 802.11g
Channel Management	Channel	6
Wireless Neighborhood	Internal Settings	
Security	MAC Address	00:08:A2:01:4B:56
Status	SSID	SFG
Interfaces	Guest Settings	
Events	MAC Address	
Transmit/Receive	SSID	TEKLOGIX GUEST
Client Associations	<input type="button" value="Update"/>	
Neighboring Access Points		
Manage		
Ethernet Settings		
802.11 Settings		
802.11 Advanced Settings		

13.2 802.11d Düzenleyici Etki Alanı Desteğini Yapılandırma

Erişim noktası ülke kodu bilgisini yayınlamak için IEEE 802.11d Düzenleyici Etki Alanı Desteğini etkinleştirebilir ya da devre dışı bırakabilirsiniz.

Tablo 13.1 802.11d Desteğini Etkinleştirme

Alan	Açıklama
<i>802.11d Regulatory Domain Support (802.11d Düzenleyici Etki Alanı Desteği)</i>	<p>Erişim noktasında IEEE 802.11d desteğinin etkinleştirilmesi, AP'nin uyarılarının bir parçası olarak hangi ülkede çalıştırıldığını yayınlamasına yol açar.</p> <ul style="list-style-type: none">802.11d düzenleyici etki alanı desteğini etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.802.11d düzenleyici etki alanı desteğini devre dışı bırakmak için Disabled (Devre dışı) seçeneğine tıklayın. İki telsizli AP'lerde, Dahili arabirimde her telsiz için bir tane olmak üzere iki MAC adresi görüntülenir. <p>Not: IEEE 802.11d, IEEE 802.11 kablosuz LAN'ların yeniden yapılandırılmadan herhangi bir ülkede çalıştırılması için standart kurallar tanımlar. IEEE 802.11d, istemci istasyonlarının yeniden yapılandırılmadan herhangi bir ülkede çalıştırılmasına olanak sağlar. Deviceescape Referans AP'sinin belirli bir ülkede kullanılabilmesi için Üretici tarafından komut satırı arabirimi (CLI) ülke kodlarıyla yapılandırılması gerekir.</p>

13.3 802.11h Düzenleyici Etki Alanı Kontrolü

Tablo 13.2 IEEE 802.11h Standardı

Alan	Açıklama
<i>IEEE 802.11h</i>	<p>Yönetim Kullanıcı Arabirimi IEEE 802.11h düzenleyici etki alanı kontrolünün AP'de etkin olup olmadığını gösterir. IEEE 802.11h, son kullanıcı Yönetici tarafından devre dışı bırakılamaz. Aşağıdaki ayrıntılar yalnızca bilgi amaçlı verilmiştir.</p> <p>IEEE 802.11h, 5 GHz bant için belirli düzenleyici etki alanlarının karşılanmasında gerekli olan iki hizmeti sunan bir standarttır. Bu iki hizmet şunlardır: İletim Gücü Kontrolü (TPC) ve Dinamik Frekans Seçimi (DFS).</p> <ul style="list-style-type: none">TPC, 5 GHz bantta çalışan Telsiz Yerel Alan Ağlarının (RLAN'lar) verici gücü kontrolünü kullanmasını gerektirir. İzin verilen her kanal için düzenleyici maksimum aktarım çıkış gücüne ve azaltma gereksinimlerine uymayı da içerir. Bunun sonucunda da uydu servisleriyle olan parazit azalır.DFS, 5 GHz bantta çalışan RLAN'ların radar sistemleriyle ortak kanalda çalışmasını önleyecek bir mekanizma uygulamalarını ve mevcut kanalların aynı biçimde kullanımını sağlamasını gerektirir. <p>Not: AP, minimum 802.11h standardı gerektiren bir ülkede kullanılmak üzere yapılandırıldıysa 802.11h otomatik olarak etkinleştirilir. Bu standart, şu an yalnızca Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) kategorisindeki ülkeler tarafından istenmektedir. 802.11h Japonya için de etkinleştirilir.</p>

AP Geliştirici için IEEE **802.11h** standardıyla ilgili dikkate alınması gereken pek çok önemli nokta vardır:

- 802.11h, yalnızca 802.11a bandında çalışır. 802.11b ve 802.11g için gerekli değildir.
- 802.11h'nin etkin olduğu bir etki alanında çalışıyorsanız BSS kanal seçimi her zaman "Otomatik"tir. Başka bir kanal yapılandırılmış olsa bile bu kanal yoksayılır ve otomatik kanal seçimi geçerli olur.
- 802.11h etkinleştirildiğinde ilk başlatma süresi en az altmış saniye artar. Bu süre, seçili kanalın radar parazitine karşı taranması için gereken minimum süredir.
- 802.11h kullanımdayken WDS bağlantıları kurmak zor olabilir. Bunun sebebi, WDS bağlantısındaki iki AP'nin çalışan kanallarının, kanal kullanımına ve radar parazitine bağlı olarak sürekli değişebilecek olmasıdır. WDS, yalnızca her iki AP'nin de aynı kanalda çalıştığı durumlarda çalışır. WDS hakkında daha fazla bilgi için bkz. Bölüm 20: "Kablosuz Dağıtım Sistemi".

13.4 Telsiz Arabirimini Yapılandırma

Telsiz arabirimi, Kanal ve **802.11** modlarını Tablo 13.3'te açıklandığı gibi ayarlamanıza olanak sağlar.



Not: İki telsizli bir AP'de bu telsiz arabirimi ayarlarını hem Telsiz Arabirimi Bir hem de Telsiz Arabirimi İki için yapılandırmanız gerekir.

Tablo 13.3 Telsiz Arabirimi Ayarları

Alan	Açıklama
<i>MAC Addresses (Shown on two-radio AP only) (MAC Adresleri [Yalnızca iki telsizli AP'lerde görüntülenir])</i>	<p>Arabirimin Ortam Erişim Denetimi (MAC) Adreslerini belirtir.</p> <p>Telsiz Arabirimi Bir (Dahili/Konuk) ve Telsiz Arabirimi İki (Dahili/Konuk) MAC adresleri yalnızca iki telsizli AP'lerde görüntülenir.</p> <p>MAC adresi, bir arabirimi ağa tanıtan herhangi bir cihazın kalıcı ve benzersiz donanım adresidir. MAC adresi üretici tarafından atanır. MAC adresini değiştiremezsiniz. Arabiriminin benzersiz bir tanımlayıcısı olduğu için burada bilgi amaçlı değinilmiştir.</p>

Tablo 13.3 Telsiz Arabirimi Ayarları (Devamı)

Alan	Açıklama
<i>Mode (Mod)</i>	<p><i>Mod</i>, telsiz tarafından kullanılan <i>Fiziksel Katman (PHY)</i> standardını tanımlar.</p> <p>9160 G2 Kablosuz Ağ Geçidi cihazının tek ya da iki telsizli, tek ya da çift bant erişim noktaları türleri vardır. Modun yapılandırma seçenekleri sahip olduğunuz ürüne göre farklılık gösterir.</p> <p>Tek Bant AP: Tek Bant AP için şu modlardan birini seçin:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g <p>Çift Bant AP: Çift Bant AP için her Telsiz Arabirimine bir mod olacak şekilde aşağıdaki modlardan birini seçin:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g• IEEE 802.11a <p>Tek ya da Çift Telsizli AP: Çift telsizli bir AP'niz varsa her iki telsiz arabirimi için de bir IEEE 802.11 modu seçin. (Tek telsizli AP'lerde yalnızca bir telsiz arabirimi vardır.)</p>
<i>Channel (Kanal)</i>	<p><i>Kanalı</i> seçin. Kanalların menzili ve varsayılan kanal telsiz arabiriminin <i>Modu</i> tarafından belirlenir.</p> <p>Kanal telsizin alma/verme için kullandığı telsiz spektrumu kısmını tanımlar. Her mod, spektrumun Federal İletişim Komisyonu (FCC) ya da Uluslararası Telekomünikasyon Birliği (ITU-R) gibi ulusal ve uluslararası otoriteler tarafından nasıl lisanslandığına bağlı olarak pek çok kanal sunar.</p> <p>Varsayılan ayar, başlangıçta en az meşgul kanalı seçen Auto'dur (Otomatik).</p>

13.5 "Dahili" Kablosuz LAN Ayarlarını Yapılandırma

Dahili Ayarlar, dahili *Kablosuz LAN*'ın (WLAN) *MAC* Adresini (salt okunur) ve Ağ Adını (*SSID* olarak da bilinir) Tablo 13.4'te anlatıldığı gibi açıklar.

Tablo 13.4 Kablosuz LAN Ayarları

Alan	Açıklama
<i>MAC Address</i> (<i>MAC Adresi</i>)	<p>Bu erişim noktasının Dahili arabiriminin MAC adresini gösterir. Bu alan salt okunurdur, değiştirilemez.</p> <p>Bu erişim noktası fiziksel olarak tek bir cihaz olsa da, ağ üzerinde her biri benzersiz MAC Adreslerine sahip iki ya da daha fazla düğümle gösterilebilir. Bu da, tek bir erişim noktası için <i>Temel Hizmet Kümesi Tanımlayıcıları (BSSID)</i> kullanılarak yapılır.</p> <p>"Dahili" erişim noktası için görüntülenen MAC adresleri, "Dahili" arabirimin BSSID'leridir.</p> <p>İki telsizli AP'lerde, Dahili arabirimde her telsiz için bir tane olmak üzere iki MAC adresi görüntülenir.</p>
<i>Wireless Network Name (SSID)</i> (<i>Kablosuz Ağ Adı</i>)	<p>Dahili WLAN'ın .SSID'sini girin.</p> <p><i>Hizmet Kümesi Tanımlayıcısı (SSID)</i>, en çok 32 karakterden oluşan ve bir kablosuz yerel alan ağını benzersiz biçimde tanımlayan alfanümerik bir dizedir. <i>Ağ Adı</i> olarak da bilinir. SSID'de kullanılacak karakterlerle ilgili bir kısıtlama yoktur.</p>

13.6 "Konuk" Ağ Kablosuz Ayarlarını Yapılandırma

Konuk Ayarları, *Konuk Ağının MAC* Adresini (salt okunur) ve kablosuz ağ adını (*SSID*) Tablo 13.5'te anlatıldığı gibi açıklar. Bir erişim noktasının iki farklı ağ adıyla (SSID) yapılandırılması, 9160 G2 Kablosuz Ağ Geçidi cihazındaki Konuk arabiriminden faydalanmanıza olanak sağlar. Daha fazla bilgi için bkz. Bölüm 14: "Konuk Erişimini Ayarlama".

Tablo 13.5 Konuk Ağ Kablosuz Ayarları

Alan	Açıklama
<i>MAC Address (MAC Adresi)</i>	<p>Bu erişim noktasının Konuk arabiriminin MAC adresini gösterir. Bu alan salt okunurdur, değiştirilemez.</p> <p>Bu erişim noktası fiziksel olarak tek bir cihaz olsa da, ağ üzerinde her biri benzersiz MAC Adreslerine sahip iki ya da daha fazla düğümle gösterilebilir. Bu da, tek bir erişim noktası için <i>Temel Hizmet Kümesi Tanımlayıcıları (BSSID)</i> kullanılarak yapılır.</p> <p>"Konuk" erişim noktası için görüntülenen MAC adresleri, "Konuk" arabiriminin BSSID'leridir.</p> <p>İki telsizli AP'lerde, Konuk arabiriminde her telsiz için bir tane olmak üzere iki MAC adresi görüntülenir.</p>
<i>Wireless Network Name (SSID) (Kablosuz Ağ Adı)</i>	<p><i>Konuk ağının SSID'sini girin.</i></p> <p><i>Hizmet Kümesi Tanımlayıcısı (SSID)</i>, en çok 32 karakterden oluşan ve bir kablosuz yerel alan ağını benzersiz biçimde tanımlayan alfanümerik bir dizedir. <i>Ağ Adı</i> olarak da bilinir. SSID'de kullanılacak karakterlerle ilgili bir kısıtlama yoktur.</p> <p>Konuk ağı için dahili SSID'den farklı ve "konuk" ağı olduğu kolayca anlaşılabilen bir SSID sağlayın.</p>

13.7 Kablosuz Ayarlarını Güncelleme

Kablosuz ayarlarını güncellemek için:

1. 802.11 Settings (802.11 Ayarları) sayfasına gidin.
2. Kablosuz ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

14.1 Konuk Arabirimini Anlama	155
14.2 Konuk Arabirimini Yapılandırma	155
14.2.1 Sanal Bir LAN'da Konuk Ağı Yapılandırma	156
14.2.2 Karşılama Ekranını (Giriş Portalı) Yapılandırma	157
14.3 Konuk Ağını İstemci Olarak Kullanma	157
14.4 Dağıtım Örneği	158

Kullanıma hazır *Konuk Arabirimi*, izole bir ağa kontrollü konuk erişimi sağlamak için 9160 G2 Kablosuz Ağ Geçidi cihazını yapılandırmanızı sağlar. Aynı erişim noktasını biri güvenli "Dahili" LAN, diğeri genel "Konuk" ağı olmak üzere iki farklı kablosuz ağ olarak işlev görecektir ve yayın yapacak şekilde yapılandırabilirsiniz. Konuk istemciler konuk ağına kullanıcı adı ve şifre olmadan erişebilir. Konuklar oturum açtıklarında bir konuk *Karşılama* ekranı ("*giriş portalı*" olarak da bilinir) ile karşılaşır.

14.1 Konuk Arabirimini Anlama

Konuk bağlantısı için benzersiz parametreler belirleyebilir ve *konuk* istemcilerini ağı daha hassas olan diğer alanlarından ayırabilirsiniz.



Önemli: *Konuk ağında herhangi bir güvenlik yoktur, yalnızca düz metin güvenlik modu kullanılabilir.*

Aynı zamanda, güvenlik duvarının ötesindeki korunan bilgilere tam erişim sağlayan ve erişim için güvenli oturum açma bilgileri ve sertifikalar gerektiren güvenli bir *dahili* ağ yapılandırabilirsiniz (konuk ağıyla aynı erişim noktasını kullanarak).

9160 G2 Kablosuz Ağ Geçidi cihazının Yönetim Web sayfalarında konuk arabirimi yapılandırma seçeneklerini uygun biçimde ayarlayarak VLAN'lar içeren tek bir ağ ile 9160 G2 Kablosuz Ağ Geçidi için bir Konuk arabirimi yapılandırabilirsiniz. (Bu tür konuk arabirimlerinin yapılandırılmasıyla ilgili ayrıntılı bilgi için bkz. "Sanal Bir LAN'da Konuk Ağı Yapılandırma", sayfa 156).



Notlar: *Bu yöntem, 9160 G2 Kablosuz Ağ Geçidi'nde yerleşik olarak bulunan birden fazla BSSID ve Sanal LAN (VLAN) teknolojilerinden yararlanır. Dahili ve Konuk ağları, aynı erişim noktasında olan ve her biri Kablosuz arabirimde farklı ağ adlarına (SSID) ve Kablolu arabirimde farklı VLAN Kimliklerine sahip birden fazla BSSID olarak uygulanır.*

İki telsizli erişim noktalarında Konuk Yönetimi ve Oturum Açma ayarları hem Telsiz 1 hem de Telsiz 2 için geçerlidir.

14.2 Konuk Arabirimini Yapılandırma

9160 G2 Kablosuz Ağ Geçidi cihazında Konuk Arabirimini yapılandırmak için aşağıdaki adımları uygulayın:

1. Erişim noktasını, aşağıdaki "Sanal Bir LAN'da Konuk Ağı Yapılandırma" bölümünde anlatıldığı gibi *sanal olarak* ayrı iki ağ olacak şekilde yapılandırın.
2. "Karşılama Ekranını (Giriş Portalı) Yapılandırma", sayfa 157'da anlatıldığı gibi, konuk giriş portalı için konuk *Karşılama* ekranını ayarlayın.



Not: Konuk Arabirimi ayarları, kümedeki erişim noktaları arasında paylaşılmaz. Bu ayarlar Yönetim sayfalarında her erişim noktası için ayrı ayrı yapılandırılmalıdır. Geçerli kümenin üyesi olan bir erişim noktasının Yönetim Web sayfasına gitmek için, geçerli AP'nin Cluster, Access Points (Küme, Erişim Noktaları) sayfasındaki **IP Adresi** bağlantısına tıklayın. Hangi ayarların kümeyle paylaşıldığı, hangilerinin paylaşılmadığı hakkında daha fazla bilgi için bkz. “Hangi Ayarlar Küme Yapılandırmasının Bir Parçası Olarak Paylaşılır, Hangileri Paylaşılmaz?”, sayfa 57.

14.2.1 Sanal Bir LAN'da Konuk Ağı Yapılandırma



Notlar: Sanal LAN (VLAN) ağlarında Konuk ve Dahili ağlar yapılandırabilmeniz için, kullandığınız anahtar ve DHCP sunucusunun VLAN'ları desteklemesi gerekir.

Bir önkoşul olarak, IEEE 802.1Q standardında açıklandığı gibi VLAN etiketli paketleri kullanabilmek için anahtar üzerinde bir bağlantı noktası yapılandırın.

Konuk Karşılama Ekranı ayarları, kümedeki erişim noktaları arasında paylaşılır. Bu ayarları bir erişim noktası için güncellediğinizde, yeni yapılandırma kümedeki diğer erişim noktalarıyla paylaşılır. Hangi ayarların kümeyle paylaşıldığı, hangilerinin paylaşılmadığı hakkında daha fazla bilgi için bkz. “Hangi Ayarlar Küme Yapılandırmasının Bir Parçası Olarak Paylaşılır, Hangileri Paylaşılmaz?”, sayfa 57.

Sanal LAN'larda Dahili ve Konuk ağları yapılandırmak için şu adımları izleyin:

1. Erişim noktasındaki ağ bağlantı noktası ile LAN arasında tek bir kablolu bağlantı kullanın. (Bu bağlantı noktasının VLAN etiketli paketleri kullanabilecek şekilde yapılandırıldığından emin olun).
2. VLAN'larda Dahili ve Konuk ağları için Bölüm 12: “Ethernet (Kablolu) Arabİrİmİ” bölümlerinde anlatıldığı gibi Ethernet (kablolu) Ayarlarını yapılandırın. (“Sanal Konuk Ağı Belirleme”, sayfa 139'da anlatıldığı gibi Konuk Erişimini etkinleştirip *For Internal and Guest access, use two: VLANs* [Dahili ve Konuk ağları için iki VLAN kullan] seçeneğini belirleyin).
3. Bölüm 13: “Kablosuz Arabİrİmİnİ Ayarlama” bölümünde anlatıldığı gibi hem Dahili hem de Konuk ağları için telsiz arabirimi ayarları ve ağ adları (SSID) girin.
4. Konuk başlangıç ekranını “Karşılama Ekranını (Giriş Portalı) Yapılandırma”, sayfa 157'da anlatıldığı gibi yapılandırın.

14.2.2 Karşılama Ekranını (Giriş Portalı) Yapılandırma

Konuk istemcilerin bir web tarayıcıyı açtıklarında ya da web'de gezinmeye çalıştıklarında görecekleri bir Karşılama ekranı ayarlayabilir ya da mevcut ekranı değiştirebilirsiniz. Giriş portalını ayarlamak için aşağıdaki adımları izleyin:

1. *Manage > Guest Login* (Yönet > Konuk Olarak Oturum Açma) sekmesine gidin.

Şekil 14.1 Konuk Olarak Oturum Açma Ekran Ayarları

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

Modify guest welcome screen settings

Guest User Welcome Screen ☒ Enabled ☐ Disabled

Welcome Screen Text

Thank you for using wireless Guest Access as provided by this 9160 wireless AP. Upon clicking "Accept", you will gain access to our wireless guest network. This network allows

Update

2. Karşılama ekranını etkinleştirmek için **Enabled** (Etkin) seçeneğini belirleyin.
3. *Welcome Screen Text* (Karşılama Ekranı Metni) alanına, konuk istemcilerin giriş portalına girdiklerinde görmelerini istediğiniz metin mesajını girin.
4. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

14.3 Konuk Ağını İstemci Olarak Kullanma

Konuk ağı yapılandırıldıktan sonra istemciler konuk ağına şu şekilde erişebilir:

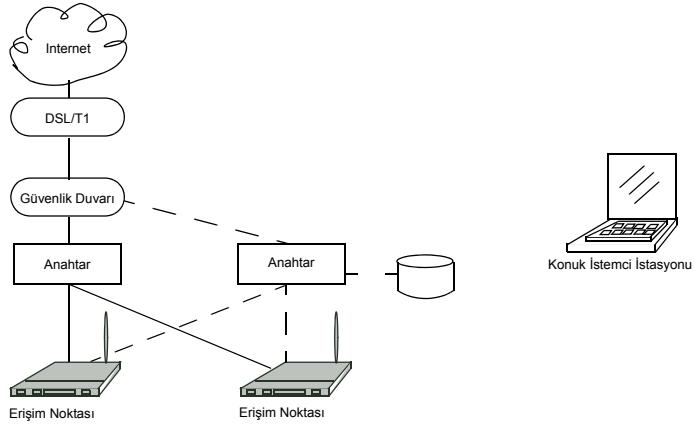
1. Konuk istemci kapsama alanına girer ve kablosuz ağlar için tarama yapmaya başlar.

2. Konuk ağı, konuk SSID'sinin Konuk arabirimi Yönetim Web sayfasında nasıl belirtildiğine bağlı olarak ya Konuk SSID'sini ya da benzer bir adı kullanarak kendini gösterir.
3. Konuk istemci Konuk SSID'sini seçer.
4. Konuk istemci bir Web tarayıcı açar ve Konuk Karşılama ekranını görür.
5. Konuk Karşılama ekranında istemcinin tıklayarak devam etmesini sağlayan bir düğme bulunur.
6. Konuk istemci artık "konuk" ağını kullanabilir.

14.4 Dağıtım Örneği

Şekil 14.2'de kesik çizgiler konuk ağına özel bağlantıları göstermektedir. Tüm erişim noktaları ve bağlantılar (konuklar dahil) aynı 9160 G2 Kablosuz Ağ Geçidi Yönetim Web sayfalarından yönetilir.

Şekil 14.2 Konuk Ağına Özel Bağlantılar



15.1 Sanal Kablosuz Ağ Ayarlarına Gitme.	161
15.2 VLAN'ları Yapılandırma	161
15.3 Ayarları Güncelleme	163

Aşağıdaki bölümler Sanal LAN'lardaki (VLAN'lar) birden fazla kablosuz ağın nasıl yapılandırıldığını anlatmaktadır.

15.1 Sanal Kablosuz Ağ Ayarlarına Gitme

VLAN'larda birden fazla ağ kurmak için *Manage > VWN* (Yönet > VWN) sekmesine gidin ve ilgili alanları aşağıda anlatıldığı gibi güncelleyin.

Şekil 15.1 VWN Ayarları

VWN	Enabled	VLAN ID	SSID	Broadcast SSID	Security
1	<input checked="" type="checkbox"/>		Virtual Wireless Network 1	<input checked="" type="checkbox"/>	None
2	<input checked="" type="checkbox"/>		Virtual Wireless Network 2	<input checked="" type="checkbox"/>	None

Update

15.2 VLAN'ları Yapılandırma



Not: VLAN'larda ek ağlar yapılandırmak için önce Ethernet Ayarları sayfasında Sanal Kablosuz Ağlar'ı etkinleştirmeniz gerekir. Bkz. "Sanal Kablosuz Ağlar", sayfa 140.



Önemli: VLAN'ları yapılandırdığınızda erişim noktasıyla bağlantınızı yitirebilirsiniz. Öncelikle, kullandığınız anahtarın ve DHCP sunucusunun IEEE802.1Q standardına uygun şekilde VLAN'ları desteklediğini doğrulayın. VLAN'ları yapılandırdıktan sonra anahtardaki Ethernet kablosunu etiketli paket (VLAN) bağlantı noktasına fiziksel olarak yeniden bağlayın. Ardından Yönetim Web sayfaları aracılığıyla yeni IP adresine yeniden bağlanın. (Gerekirse VLAN ve DHCP yapılandırmalarıyla ilgili altyapı destek yöneticisine danışın.)

Tablo 15.1 Sanal Kablosuz Ağ Ayarları

Alan	Açıklama
<i>Virtual Wireless Network (Sanal Kablosuz Ağ)</i>	En fazla 6 adet VWN yapılandırabilirsiniz.
<i>Enabled (Etkin)</i>	<p>Yapılandırılmış bir ağı etkinleştirebilir ya da devre dışı bırakabilirsiniz.</p> <ul style="list-style-type: none">Belirtilen ağı etkinleştirmek için ilgili VWN'nin yanındaki <i>Enabled</i> (Etkin) onay kutusunu işaretleyin.Belirtilen ağı devre dışı bırakmak için ilgili VWN'nin yanındaki <i>Enabled</i> (Etkin) onay kutusunun işaretini kaldırın. <p>Belirtilen ağı devre dışı bırakırsanız girdiğiniz VLAN kimliğini yitirirsiniz.</p>
<i>VLAN ID (VLAN Kimliği)</i>	<p>Dahili VLAN için 1 - 4094 arası bir sayı belirleyin.</p> <p>Bu eylem, erişim noktasının VLAN etiketli DHCP istekleri göndermesine yol açar. Anahtar ve DHCP sunucusu VLAN IEEE 802.1Q çerçevelerini desteklemelidir. Erişim noktası DHCP sunucusuna erişebilmelidir.</p> <p>VLAN ve DHCP yapılandırmalarıyla ilgili Yöneticiye danışın.</p>
<i>SSID</i>	<p>Kablosuz ağ için karakter dizesi olarak bir ad girin. Bu ad, bu ağıdaki tüm erişim noktaları için geçerlidir. Daha fazla erişim noktası eklediğinizde erişim noktaları bu SSID'yi paylaşır.</p> <p>Hizmet Kümesi Tanımlayıcı (SSID), en fazla 32 karakterden oluşan alfanümerik bir dizedir.</p> <p>Not: Yönettiğiniz AP'ye kablosuz istemci olarak bağlanırsanız SSID'yi sıfırlamanız AP bağlantısını yitirmenize yol açar. Bu yeni ayarı kaydettikten sonra yeni SSID'ye tekrar bağlanmanız gerekir.</p>

Tablo 15.1 Sanal Kablosuz Ağ Ayarları (Devamı)

Alan	Açıklama
<i>Broadcast SSID (SSID Yayını)</i>	<p>Broadcast SSID (SSID Yayını) onay kutusunu işaretleyerek <i>Broadcast SSID</i> ayarını seçin.</p> <p>Erişim noktası varsayılan olarak uyarı anonslarındaki <i>Hizmet Kümesi Tanımlayıcısını</i> (SSID) yayınlar (izin verir).</p> <p>İstasyonların erişim noktanızı otomatik olarak keşfetmemesi için bu yayını kaldırabilirsiniz (engelleyebilirsiniz). AP'nin SSID yayını kaldırıldığında ağ adı, istemci istasyonundaki <i>Mevcut Ağlar Listesinde</i> görülmez. İstemcinin bu AP'ye bağlanabilmesi için doğrulama isteyen öğede yapılandırılan ağ adını tam olarak bilmesi gerekir.</p> <p>Not: Burada ayarladığınız SSID Yayını, özel olarak bu Sanal Ağ (Bir ya da İki) içindir. Diğer ağlar hali hazırda yapılandırılmış olan güvenlik modlarını kullanmaya devam eder.</p> <ul style="list-style-type: none">• <i>Ethernet Settings</i> [Ethernet Ayarları] sayfasında yapılandırılan orijinal Dahili ağınız <i>Security</i> (Güvenlik) kısmında ayarlanan SSID Yayını kullanır.• Herhangi bir Konuk ağı yapılandırılırsa SSID Yayınına her zaman izin verilir.
<i>Security (Güvenlik)</i>	<p>Bu VLAN için <i>Güvenlik Modu</i> seçin. Aşağıdakilerden birini seçin:</p> <ul style="list-style-type: none">• Yok (Düz metin)• Statik WEP• WPA Kişisel <p>Not: Burada ayarladığınız Güvenlik Modu özel olarak bu Sanal Ağ içindir. Diğer ağlar hali hazırda yapılandırılmış olan güvenlik modlarını kullanmaya devam eder.</p> <ul style="list-style-type: none">• <i>Ethernet Settings</i> [Ethernet Ayarları] sayfasında yapılandırılan orijinal Dahili ağınız <i>Security</i> (Güvenlik) kısmında ayarlanan Güvenlik modunu kullanır.• Herhangi bir Konuk ağı yapılandırılırsa güvenlik modunu her zaman "None" (Yok) olarak ayarlayın.

15.3 Ayarları Güncelleme

VLAN ayarlarını güncellemek için:

1. *VWN* sekmesine gidin.
2. VLAN ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

802.11 TELSİZ AYARLARINI YAPILANDIRMA

16

16.1 Telsiz Ayarlarını Anlama	167
16.2 Telsiz Ayarlarına Gitme	167
16.3 Telsiz Ayarlarını Yapılandırma	169
16.4 Ayarları Güncelleme	173

Aşağıdaki bölümler, 9160 G2 Kablosuz Ağ Geçidi cihazındaki 802.11 Telsiz Ayarlarının nasıl yapılandırıldığını anlatmaktadır:

16.1 Telsiz Ayarlarını Anlama

Telsiz ayarları doğrudan erişim noktasındaki telsiz cihazının davranışını ve fiziksel ortamla olan etkileşimini, yani AP'nin hangi tip elektromanyetik dalgaları nasıl yaydığını kontrol eder. Telsizin açık ya da kapalı olmasını, telsiz frekansı (RF) yayın kanalını, uyarı aralığını (AP uyarı aktarımları arasındaki süre), aktarım gücünü, telsizin çalıştığı IEEE 802.11 modunu ve daha pek ayarı belirleyebilirsiniz.

9160 G2 Kablosuz Ağ Geçidi, tek telsizli, çift bant bir erişim noktası olarak yapılandırılmış şekilde gelir.

Erişim noktası şu modlarda yayın yapabilir:

- IEEE **802.11b** modu.
- IEEE **802.11g** modu.
- IEEE **802.11a** modu.
- Atheros Turbo 5 GHz.
- Atheros Dynamic Turbo 5 GHz.
- Atheros Turbo 2,4 GHz.
- Atheros Dynamic Turbo 2,4 GHz.
- Uzun Menzil.



Önemli: *Psion Teklogix mobil bilgisayarlar, Atheros Turbo modlarını desteklemez. Gereksiz telsiz yükünü önlemek için Turbo modunun kullanılması önerilmez.*

IEEE modu diğer telsiz ayarlarıyla birlikte “Telsiz Ayarlarına Gitme”, sayfa 167 ve “Telsiz Ayarlarını Yapılandırma”, sayfa 169 bölümlerinde anlatıldığı gibi yapılandırılır.

16.2 Telsiz Ayarlarına Gitme

Telsiz ayarlarını belirlemek için *Manage > 802.11 Advanced Settings* (Yönet > 802.11 Gelişmiş Ayarları) sekmesine gidin. Burada açılan *Radio Settings* (Telsiz Ayarları) sayfasında ilgili alanları Tablo 16.1, sayfa 169'da açıklandığı gibi güncelleyin.

Şekil 16.1 Telsiz Ayarları Yapılandırmasına Genel Bakış

Basic Settings	Modify radio settings
User Management	
Cluster	Status <input checked="" type="radio"/> On <input type="radio"/> Off
Access Points	Mode <input type="text" value="IEEE 802.11g"/>
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	
Hosts	
802.1Q	

Super AG ☐ Enabled ☒ Disabled

Extended Range ☐ Enabled ☒ Disabled

Channel

Beacon Interval (Msec, Range: 20 - 2000)

DTIM Period (Range: 1-255)

Fragmentation Threshold (Range: 256-2346, Even Numbers)

RTS Threshold (Range: 0-2347)

Maximum Stations (Range: 0-2007)

Transmit Power Percent

Rate Supported Basic

54 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
48 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
36 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
24 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Broadcast/Multicast Rate Limiting

Rate Limit (packets per second)

Rate Limit Burst (packets per second)

16.3 Telsiz Ayarlarını Yapılandırma

Tablo 16.1 Telsiz Ayarları

Alan	Açıklama
<i>Radio (Telsiz)</i>	<p>9160 G2 Kablosuz Ağ Geçidi cihazının tek ve iki telsizli erişim noktası türleri vardır.</p> <p>Tek Telsizli AP: 9160 G2 Kablosuz Ağ Geçidi cihazının tek telsizli versiyonuna sahipseniz Telsiz sekmesinde bu alan bulunmaz.</p> <p>İki Telsizli AP: 9160 G2 Kablosuz Ağ Geçidi cihazının iki telsizli versiyonuna sahipseniz Telsiz 1 ya da Telsiz 2'yi belirleyin. İki telsizli bir AP'de, bu sekmede yer alan diğer ayarlar, bu alanda seçilen telsiz için geçerlidir. Ayarları iki telsiz için de yapılandırdığınızdan emin olun.</p>
<i>Status (On/Off) (Durum [Açık/Kapalı])</i>	<p>On (Açık) ya da Off (Kapalı) seçeneğine tıklayarak telsizin açık mı yoksa kapalı mı olmasını istediğinizi belirtin.</p>
<i>Mode (Mod)</i>	<p><i>Mod</i>, telsiz tarafından kullanılan <i>Fiziksel Katman (PHY)</i> standardını tanımlar.</p> <p>9160 G2 Kablosuz Ağ Geçidi cihazının tek ya da çift bant erişim noktası türleri vardır.</p> <p>Tek Bant AP: Tek Bant erişim noktası için şu modlardan birini seçin:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g <p>Çift Bant AP: Çift Bant erişim noktası için şu modlardan birini seçin:</p> <ul style="list-style-type: none">• IEEE 802.11b• IEEE 802.11g• IEEE 802.11a <p>Not: İki telsizli bir AP'niz varsa yukarıdaki Telsiz alanında Telsiz 1 ya da Telsiz 2'nin seçili olduğuna bağlı olarak farklı modlar kullanılabilir.</p> <p><i>Telsiz modunu seçtiğinizde o modun uygun Temel ya da Destekli Hızları otomatik olarak seçilir. (Bu tablonun devamında sayfa 172'de Hız Gruplarının açıklamasına bakın.)</i></p>
<i>Super AG (Süper AG)</i>	<p>Süper AG'nin etkinleştirilmesi bir telsiz modunda (IEEE 802.11b, g, a vb.) telsiz verimini artırarak daha iyi bir performans sağlar. Süper AG etkinleştirildiğinde erişim noktası aktarımlarının daha fazla bant genişliği kullanacağını unutmayın.</p> <ul style="list-style-type: none">• Süper AG'yi etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.• Süper AG'yi devre dışı bırakmak için Disabled (Devre Dışı) seçeneğine tıklayın.


Tablo 16.1 Telsiz Ayarları (Devamı)

Alan	Açıklama
<i>Extended Range (Uzun Menzil)</i>	<p>Atheros Extended Range (XR), daha uzun mesafede düşük hızlı trafik uygulamanın özel bir yöntemidir. XR etkin istemcilerde ve erişim noktalarında görünmez ve 802.11g ile 802.11a modlarında 802.11 standardıyla birlikte çalışabilecek şekilde tasarlanmıştır. 802.11b, Atheros Turbo</p> <p>5 GHz veya Atheros Dynamic Turbo 5 GHz'de Atheros XR desteği bulunmaz.</p> <p>Atheros XR'in etkinleştirilmesi istemcinizin ve erişim noktanızın çalışabileceği menzili genişletir.</p> <ul style="list-style-type: none">• Uzun Menzili etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.• Uzun Menzili devre dışı bırakmak için Disabled (Devre Dışı) seçeneğine tıklayın. <p>IEEE 802.11b, Atheros Turbo 5 GHz ya da Atheros Dynamic Turbo 5 GHz donanım modunu seçtiğinizde bu seçenek kullanılabilir olmayacaktır. Atheros XR, bu donanım modları tarafından desteklenmez.</p>
<i>Channel (Kanal)</i>	<p>Kanal, telsizin alma/verme için kullandığı telsiz spektrumu kısmını tanımlar. Kanalların menzili ve varsayılan kanallar telsiz arabiriminin Modu tarafından belirlenir.</p> <p>Modların çoğu için varsayılan ayar Auto'dur (Otomatik). Sinyal gücüne, trafik yüklerine vs. göre en iyi kanal seçeneklerini otomatik olarak algıladığı için otomatik modu önerilen moddur. Ancak 1-11 arası kanallardan (1 ve 11 dahil) istediğinizi seçebilirsiniz.</p>
<i>Beacon Interval (Uyarı Aralığı)</i>	<p>Uyarı çerçeveleri, kablosuz ağların varlığını duyurmak için erişim noktası tarafından düzenli aralıklarla iletilir. Varsayılan olarak her 100 milisaniyede bir (ya da her 10 saniyede bir) uyarı anonsu gönderilir.</p> <p><i>Uyarı Aralığı</i> değeri milisaniye cinsinden ayarlanır. 20 - 2000 arası bir değer girin.</p>
<i>DTIM Period (DTIM Süreci)</i>	<p><i>Teslim Trafiği Bilgi Haritası (DTIM)</i> mesajı, bazı Uyarı aralıklarında yer alan bir unsurdur. Düşük güç modunda uyuyan istemci istasyonlarından hangilerinin erişim noktası arabelleğinde alınmayı bekleyen verileri olduğunu belirtir.</p> <p>Burada belirlediğiniz DTIM süreci, bu erişim noktası tarafından sunulan istemcilerin AP arabelleğinde alınmayı bekleyen veri olup olmadığını ne sıklıkta kontrol etmesi gerektiğini belirtir.</p> <p>Verilen aralıkta (1 - 255) bir DTIM süreci belirleyin.</p> <p>Ölçme işlemi uyarılarla yapılır. Örneğin, bunu 1'e ayarladığınızda istemciler her uyarıda AP'de bekleyen veri olup olmadığını kontrol eder. 2'ye ayarladığınızda istemciler iki uyarıda bir kontrol eder. 10'a ayarladığınızda istemciler on uyarıda bir kontrol eder.</p>

Tablo 16.1 Telsiz Ayarları (Devamı)

Alan	Açıklama
<i>Fragmentation Threshold</i> (Bölme Eşiği)	<p>Çerçeve boyutu eşiğini bayt olarak ayarlamak için 256 ile 2346 arası bir sayı belirleyin.</p> <p><i>Bölme eşiği</i> ağ üzerinden aktarılan paketlerin (çerçevelerin) boyutunu sınırlama yöntemidir. Paketlerin biri burada ayarlanan bölme eşiğini aşarsa bölme işlevi etkinleştirilir ve paket birden çok 802.11 çerçevesi olarak gönderilir.</p> <p>Aktarılmakta olan paket eşiğe eşit ya da eşikten küçükse bölme işlevi kullanılmaz.</p> <p>Eşiği en yüksek değere (2346 bayt) ayarlamak bölme işlevini etkin biçimde devre dışı bırakır.</p> <p>Bölme işlevi hem çerçeveleri ekstra olarak bölme ve yeniden birleştirme işlerini gerektirdiğinden hem de ağdaki mesaj trafiğini artırdığından dolayı daha fazla ek yük içerir. Ancak bölme işlevi düzgün biçimde yapılandırıldığında ağ performansının ve güvenilirliğinin <i>geliştirilmesine</i> yardımcı olabilir.</p> <p>Daha küçük çerçeveler göndermek (daha düşük bölme eşikleri kullanarak) mikrodalga fırınlarla olduğu gibi bazı parazit sorunlarının giderilmesinde yardımcı olabilir.</p> <p>Bölme işlevi, varsayılan olarak offtur (kapalı). Herhangi bir telsiz parazitinden şüphelenmediğiniz sürece bölme işlevini kullanmamanızı öneriyoruz. Her parçaya uygulanan ek başlık ağdaki ekstra yükü artırır ve verimi büyük oranda düşürebilir.</p>
<i>RTS Threshold (RTS Eşiği)</i>	<p>0 ile 2347 arasında bir RTS Eşiği değeri belirleyin.</p> <p>RTS eşiği, aktarımı (RTS) göndermek için isteğin paket boyutunu belirler. Bu da, özellikle çok istemcili erişim noktalarındaki trafik akışının kontrol edilmesine yardımcı olur.</p> <p>Düşük bir eşik değeri belirlerseniz RTS paketleri daha sık gönderilir. Bu şekilde daha fazla bant genişliği kullanılır ve paketin verimi azalır.</p> <p>Öte yandan, daha fazla RTS paketi göndermek, yoğun bir ağda ya da elektromanyetik parazitlerin olduğu ağlarda oluşabilecek parazit ve çökmelerden kurtulmaya yardımcı olabilir.</p>
<i>Maximum Stations</i> (Maksimum İstasyon Sayısı)	<p>Bu AP'ye tek seferde erişmesine izin verilen maksimum istasyon sayısını belirleyin.</p> <p>0 - 2007 arası bir değer girebilirsiniz.</p>

Tablo 16.1 Telsiz Ayarları (Devamı)

Alan	Açıklama
<i>Transmit Power</i> (Aktarım Gücü)	<p>Bu erişim noktasının aktarım gücünü ayarlamak için yüzde olarak bir değer girin.</p> <p>Varsayılan ayar, erişim noktasının gücünün yüzde 100'ünü kullanarak aktarım yapmasıdır.</p> <p> Öneriler:</p> <ul style="list-style-type: none">• Çoğu durumda varsayılan ayarın korunmasını ve aktarım gücünün yüzde 100 olarak kalmasını öneriyoruz. Varsayılan ayar, erişim noktasına maksimum yayın menzili sunduğundan ve gerek duyulan AP sayısını azalttığından dolayı daha uygun ve etkili bir ayardır.• Ağ kapasitesini artırmak için AP'leri birbirine daha yakın yerleştirin ve aktarım gücü değerini azaltın. Bu sayede AP'ler arasındaki bindirme ve parazit azalır. Zayıf kablosuz sinyallerinin ağınızın fiziksel olarak dışına yayılması ihtimali daha az olduğundan düşük aktarım gücü ayarı, ağınızın daha güvenli olmasını sağlar.
<i>Rate Sets</i> (Hız Grupları)	<p>Erişim noktasının desteklemesini istediğiniz aktarım hızı gruplarını ve erişim noktasının bildirmesini istediğiniz temel hız gruplarını işaretleyin.</p> <p>Hızlar Mb/sn cinsinden gösterilir.</p> <ul style="list-style-type: none">• Supported Rate Sets (Desteklenen Hız Grupları) erişim noktasının desteklediği hızları belirtir. Birden fazla hız seçebilirsiniz (bir hızı seçmek ya da seçimi kaldırmak için onay kutusuna tıklayın). AP, hata oranları ve istemci istasyonlarının AP'den uzaklığı gibi faktörleri temel alarak en uygun hızı otomatik olarak seçer.• Basic Rate Sets (Temel Hız Grupları) ağdaki diğer AP'ler ve istemci istasyonlarıyla iletişim kurma gibi amaçlarla erişim noktasının ağa bildireceği hızı belirtir. Bir AP yayınının desteklenen hız gruplarının bir alt setine sahip olması genellikle daha etkilidir. <p>Hem "b" hem de "g" istemcilerini desteklemek için telsiz modunu IEEE 802.11g olarak değiştirin. Web Kullanıcı Arabirimi, hem "b" hem de "g" istemcilerinin bağlanmasına izin veren varsayılan Hız Grubunu otomatik olarak seçer.</p> <p>Yalnızca "g" istemcilerini desteklemek için telsiz modunu IEEE 802.11g olarak değiştirin. Web Kullanıcı Arabirimi otomatik olarak varsayılan Hız Grubunu seçer. Ardından Temel Hız olarak 24, 12 ve 6'yı ekleyin. "b" istemcileri bu hızları desteklemediği için bu durum, "b" istemcilerin bağlanmasını önler ancak standart gereği bu hızları desteklemesi gereken "g" istemcilerinin bağlanmasına izin verir.</p> <p>Daha fazla bilgi için bu tablonun üst kısımlarında sayfa 169'da yer alan <i>Mode</i> (Mod) bölümünü okuyun.</p>

Tablo 16.1 Telsiz Ayarları (Devamı)

Alan	Açıklama
<i>Enable Broadcast/Multicast Rate Limiting (Yayın/Çoklu Gönderim Hızı Sınırlamasını Etkinleştir)</i>	<p>Çoklu gönderim ve yayın hız sınırlamasının etkinleştirilmesi, ağda aktarılan paket sayısını sınırlar ve ağın toplam performansını artırır.</p> <p>Bazı protokoller, bir ağdaki düğümlerin çoğunun ilgilenmediği trafik için çoklu gönderim ve yayın paketleri kullanır. Diğer makineler için ARP istekleri, DHCP ya da BOOTP mesajları örnek olarak gösterilebilir. Bazı protokollerde, hız sınırı kontrolü ayarlandığında ağda aktarılan fazla paketlerin sayısı sınırlanmış olur. Genellikle filtrelenen herhangi bir trafik daha sonra yeniden aktarılır ve herhangi bir soruna yol açmaz.</p> <ul style="list-style-type: none">• Çoklu Gönderim ve Yayın Hızı Sınırlamasını etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.• Çoklu Gönderim ve Yayın Hızı Sınırlamasını devre dışı bırakmak için Disabled (Devre Dışı Bırak) seçeneğine tıklayın. <p><i>Çoklu Gönderim/Yayın Hızı Sınırlaması</i> seçeneği, varsayılan olarak devre dışıdır. Siz Çoklu Gönderim ve Yayın Hızı Sınırlamasını etkinleştirilene kadar şu alanlar devre dışıdır.</p>
<i>Broadcast/Multicast Rate Limit (Çoklu Gönderim ve Yayın Hızı Sınırı)</i>	<p>Çoklu gönderim ve yayın trafiği için ayarlamak istediğiniz hız sınırını girin. Sınır, saniye başına 1 paketten fazla, 50 paketten az olmalıdır. Bu hız sınırının altında kalan trafikler her zaman uyum sağlar ve uygun bir hedefe aktarılır.</p> <p>Varsayılan ve maksimum hız sınırı, saniyede 50 pakettir.</p>
<i>Broadcast/Multicast Rate Limit Burst (Çoklu Gönderim ve Yayın Hızı Sınır Artışı)</i>	<p>Hız sınırı artışı ayarlamak, tüm trafik hız sınırını aşmadan önce ne kadar trafik artışı olabileceğini belirler. Bu artış sınırı, bir ağda ayarlanan hız sınırının üzerinde belirli aralıklarla artış olmasına izin verir.</p> <p>Varsayılan ve maksimum hız sınırı artışı, saniyede 75 pakettir.</p>

16.4 Ayarları Güncelleme

Telsiz ayarlarını güncellemek için:

1. 802.11 Advanced Settings (802.11 Gelişmiş Ayarlar) sekmeli sayfaya gidin.
2. Telsiz ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.



*Not: 9160 G2 Kablosuz Ağ Geçidi'nin iki telsizli türünü kullanıyorsanız hem Telsiz 1'in hem de Telsiz 2'nin bu sekmede yapılandırıldığını unutmayın. Görüntülenen ayarlar, Radio (Telsiz) alanında (sekmedeki ilk alan) seçtiğiniz telseze bağlı olarak ya Telsiz 1 ya da Telsiz 2 için geçerlidir. Ayarları telsizlerden biri için yapılandırdığınızda **Update** (Güncelle) seçeneğine tıkladıktan sonra diğer telsizi seçin ve yapılandırın. Diğer telsiz için ikinci kez yaptığınız yapılandırma ayarlarından sonra **Update** (Güncelle) seçeneğine tıkladığınızdan emin olun.*

17.1 MAC Filtreleme Ayarlarına Gitme	177
17.2 MAC Filtreleme Ayarlarını Kullanma	178
17.3 Ayarları Güncelleme	178

Ortam Erişim Denetimi (MAC) adresi, ağın her bir düğümünü benzersiz biçimde tanımlayan bir donanım adresidir. Tüm IEEE 802 ağ cihazları ortak bir 48 bit MAC adresi formatı kullanır. Bu adres, FE:DC:BA:09:87:65 örneğinde olduğu gibi genellikle iki nokta işaretiyle ayrılan onaltılık düzendeki 12 haneden oluşur. Kablosuz istemci tarafından kullanılan her kablosuz ağ arabirim kartının (*NIC*) benzersiz bir MAC adresi vardır.

MAC Filtering (MAC Filtreleme) özelliğini açıp onaylanan MAC adreslerini listeleyerek istemcinin kablosuz ağınıza erişimini kontrol edebilirsiniz. MAC Filtreleme açıkken yalnızca MAC adresi listede yer alan istemciler ağa erişebilir.

Aşağıdaki bölümler 9160 G2 Kablosuz Ağ Geçidi cihazında MAC adresi filtrelemenin nasıl kullanılacağını açıklamaktadır.

17.1 MAC Filtreleme Ayarlarına Gitme

MAC adresiyle filtrelemeyi etkinleştirmek için *Manage > MAC Filtering* (Yönet > MAC Filtreleme) sekmesine gidin ve ilgili alanları aşağıda gösterilen şekilde güncelleyin.

Şekil 17.1 MAC Filtreleme Ayarları

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Configure MAC Filtering of client stations

Filter

☐ Allow only stations in list

☒ Block all stations in list

Stations List

10:10:10:10:14:44

Remove

[] : [] : [] : [] : [] : [] Add

Update

17.2 MAC Filtreleme Ayarlarını Kullanma

Bu sayfa, *Ortam Erişim Denetimi* (MAC) adreslerini kullanarak 9160 G2 Kablosuz Ağ Geçidi cihazına erişimi kontrol etmenizi sağlar. Filtreyi nasıl ayarladığınıza bağlı olarak MAC adresleri listelenen istemci istasyonlarının erişimine *izin verebilir* ya da bu istemcilerin erişimini *engelledebilirsiniz*.

Konuk arabiriminde, **MAC** Filtreleme ayarları iki **BSS** için de geçerlidir.

İki telsizli AP'de, MAC Filtreleme ayarları iki telsiz için de geçerlidir.

Tablo 17.1 MAC Filtreleme Ayarları

Alan	Açıklama
<i>Filter (Filtre)</i>	MAC Adresi <i>Filtresini</i> ayarlamak için aşağıdaki radyo düğmelerinden birine tıklayın: <ul style="list-style-type: none">Allow only stations in the list (Yalnızca listedeki istasyonlara izin ver)Block all stations in list (Listedeki tüm istasyonları engelle)
<i>Stations List (İstasyon Listesi)</i>	İstasyon Listesine MAC adresi eklemek için altta bulunan metin kutusuna istasyonun 48 bit MAC adresini yazdıktan sonra Add (Ekle) düğmesine tıklayın. MAC Adresi İstasyon Listesine eklenir. İstasyon Listesinden MAC adresi silmek için 48 bit MAC adresini seçin ve ardından Remove (Kaldır) düğmesine tıklayın. Filtreyi nasıl ayarladığınıza bağlı olarak listedeki istasyonların AP'ye erişmesine izin verilir ya da erişimleri engellenir.

17.3 Ayarları Güncelleme

MAC ayarlarını güncellemek için:

1. *MAC Filtering* (MAC Filtreleme) sekmesine gidin.
2. MAC ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

18.1 Yük Dengelemeyi Anlama	181
18.1.1 Yük Dengesizliğini Tanımlama: Kapasitesinden Fazla ya da Az Çalışan Erişim Noktaları	181
18.1.2 Kullanım Sınırlamaları ve İstemci İlişkilerini Belirleme	181
18.1.3 Yük Dengeleme ve Hizmet Kalitesi (QoS)	182
18.2 Yük Dengeleme Ayarlarına Gitme	182
18.3 Yük Dengelemeyi Yapılandırma	183
18.4 Ayarları Güncelleme	184

9160 G2 Kablosuz Ağ Geçidi, kablosuz istemci bağlantılarını birden fazla erişim noktasına dengeli biçimde dağıtmanızı sağlar. Yük dengelemeyi kullanarak ağınızdaki bir erişim noktasının orantısız bir kablosuz trafik yükü taşıdığı için performansında düşüşün yaşandığı senaryoları önlemiş olursunuz.

Aşağıdaki bölümlerde kablosuz ağınızda yük dengelemeyi nasıl yapılandıracağınız anlatılmaktadır.

18.1 Yük Dengelemeyi Anlama

Yük dengeleme ayarları da 9160 G2 Kablosuz Ağ Geçidi cihazındaki yapılandırma ayarlarının çoğunda olduğu gibi kümelenen erişim noktaları arasında paylaşılır.



Not: Bazı durumlarda, sürekli olarak kapasitesinden fazla çalışan yalnızca bir erişim noktası için sınırlamalar koymak isteyebilirsiniz. Bağımsız modda çalışan belirli bir erişim noktası için ona özel ayarlar belirleyebilirsiniz. (Bkz. “Kümelemeyi Anlama”, sayfa 56 ve “Erişim Noktası Yönetimine Gitme”, sayfa 55.)

18.1.1 Yük Dengesizliğini Tanımlama: Kapasitesinden Fazla ya da Az Çalışan Erişim Noktaları

Birden fazla erişim noktasının İstemci İlişkileri verisi ile Alma/Verme verilerinin karşılaştırılması, sürekli ve orantısız bir şekilde kablosuz trafik yükünün büyük bir kısmını taşıyan erişim noktalarını belirlemenizi sağlar. Bu durum, bir erişim noktasının konum yerleştirme ya da diğer faktörlerden dolayı ağdaki istemcilerin çoğuna en güçlü sinyali ilettiğinde gerçekleşebilir. Bu erişim noktası, en fazla istemci talebini alırken diğer erişim noktaları varsayılan olarak çoğu zaman eylemsiz kalır.

Kapasitesinden fazla çalışan AP'lerin daha yüksek "Çalışma" oranlarına, kapasitesinden az çalışan AP'lerin ise daha yüksek "Eylemsiz Kalma" oranlarına sahip olduğunu gösteren İstemci İlişkileri verileri ve Alma/Verme istatistikleriyle kablosuz trafiği yüklerinin erişim noktaları arasındaki dengesiz dağılımı açıkça görülebilir. Kapasitesinden daha fazla trafik yükü taşıyan AP'lerde aşırı yükten dolayı yavaş veri hızı ya da düşük alma/verme oranı gibi sorunlar yaşanabilir.

18.1.2 Kullanım Sınırlamaları ve İstemci İlişkilerini Belirleme

Ağ AP kullanımındaki dengesizlikleri ortadan kaldırmak için yük dengelemeyi etkinleştirebilir, kullanım oranlarına ve erişim noktası başına izin verilen istemci ilişkisi sayısına sınırlama getirebilirsiniz.

18.1.3 Yük Dengeleme ve Hizmet Kalitesi (QoS)

Yük dengeleme, *IP Üzerinden Ses* (VoIP) gibi zaman açısından duyarlı olan, kablosuz ağdaki hava dalgalarına zamanında erişim ve bant genişliği konusunda diğer uygulamalarla yarışan uygulamalar için *Hizmet Kalitesi* (QoS) sunulmasına da katkı sağlar. Ağınızı QoS'ye göre yapılandırma konusunda daha fazla bilgi için bkz. Bölüm 19: “Hizmet Kalitesi (QoS)”.

18.2 Yük Dengeleme Ayarlarına Gitme

Administration (Yönetim) kullanıcı arabiriminde *Manage > Load Balancing* (Yönet > Yük Dengeleme) sekmesine gidin ve ilgili alanları bir sonraki bölümde anlatıldığı gibi güncelleyin.

Şekil 18.1 Yük Dengeleme Ayarları

Basic Settings	Modify load balancing settings
User Management	Load Balancing <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Cluster	Utilization for No New Associations <input type="text" value="0"/> (Percent, 0 disables)
Access Points	Utilization for Disassociation <input type="text" value="0"/> (Percent, 0 disables)
Sessions	Station Threshold for Disassociation <input type="text" value="0"/> Range 1 - 2007, 0 disables.
Channel Management	<input type="button" value="Update"/>
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	

18.3 Yük Dengelemeyi Yapılandırma

Yük dengelemeyi yapılandırmak için **Load Balancing** (Yük Dengeleme) seçeneğini *etkinleştirin* ve erişim noktası belirlenen kullanım oranına ulaştığında tetiklenecek sınırlama ve davranışları ayarlayın.



Notlar: İstemcilerin AP ile ilişkisi kesildiği durumlarda bile, menzilde başka bir erişim noktası varsa ağ, istemci istasyonlarına kesintisiz hizmet sunmaya devam eder; böylece istemciler ağa yeniden bağlanabilir. İstemcilerin normalde bağlı oldukları AP'ye ve alt ağıdaki diğer AP'lere otomatik olarak bağlanmayı denemesi gerekir. Bir AP ile ilişkisi kesilen istemcilerin aynı alt ağıdaki başka bir AP'ye sorunsuz bir şekilde geçiş yapması gerekir.


Yük Dengeleme ayarları, AP yükünün tamamına uygulanır. Konuk erişimi etkinleştirildiğinde ayarlar hem Dahili hem de Konuk ağlarına uygulanır.

İki telsizli erişim noktalarında Yük Dengeleme ayarları iki telsize de uygulanır ancak her telsizin yükü ayrı hesaplanır ve hem Dahili hem de Konuk ağını içerir (Konuk erişimi etkinleştirildiğinde).

Tablo 18.1 Yük Dengeleme Ayarları

Alan	Açıklama
<i>Load Balancing</i> (Yük Dengeleme)	<p>Bu erişim noktasında yük dengelemeyi etkinleştirmek için Enable (Etkinleştir) seçeneğine tıklayın.</p> <p>Bu erişim noktasında yük dengelemeyi devre dışı bırakmak için Disable (Devre dışı bırak) seçeneğine tıklayın.</p>
<i>Utilization for No New Associations</i> (Yeni İlişkileri Kısıtlayan Kullanım Oranı)	<p>Kullanım oranı sınırlamaları, kablosuz bant genişliği kullanımıyla ilgilidir.</p> <p>Yeni istemci ilişkilerinin kabul edilmesinin ne zaman sonlandırılacağını belirlemek amacıyla bu erişim noktası için yüzde olarak bant genişliği kullanım oranı sınırı belirleyin.</p> <p>Kullanım oranı, bu erişim noktası için belirlenen sınırı aştığında bu erişim noktasında yeni istemci ilişkilerine izin verilmez.</p> <p>Bu alanı 0 olarak belirlediğinizde kullanım oranına bakılmaksızın tüm yeni ilişkilere izin verilir.</p>

Tablo 18.1 Yük Dengeleme Ayarları (Devamı)

Alan	Açıklama
<i>Utilization for Disassociation</i> (Mevcut İlişkileri Sonlandıran Kullanım Oranı)	<p>Kullanım oranı sınırlamaları, kablosuz bant genişliği kullanımıyla ilgilidir.</p> <p>Mevcut istemcilerin ilişkisinin ne zaman sonlandırılacağını belirlemek amacıyla bu erişim noktası için yüzde olarak bant genişliği kullanım oranı sınırı belirleyin.</p> <p>Kullanım oranı, belirlenen sınırı aştığında bu erişim noktasıyla ilişkili olan istemcinin ilişkisi kesilir.</p> <p>Bu alanı 0 olarak belirlediğinizde kullanım oranına bakılmaksızın mevcut istemcilerin ilişkisi hiçbir zaman kesilmez.</p>
<i>Stations Threshold for Disassociation</i> (İlişki Kesme İçin İstasyon Eşiği)	<p>İlişki kesme için "istasyon eşiği" olarak bir istemci istasyon sayısı belirleyin. Herhangi bir zamanda AP ile ilişkili istemci istasyonu sayısı burada belirlediğiniz sayıya eşit ya da bu sayıdan küçükse</p> <p><i>Utilization for Disassociation</i> (Mevcut İlişkileri Sonlandıran Kullanım Oranı) değerine bakılmaksızın hiçbir istasyonun ilişkisi kesilmez.</p> <p>Teorik olarak, izin verilen maksimum istemci istasyonu sayısı 2007'dir.</p> <p> Maksimum istasyon sayısını 30-50 arası bir sayı olarak belirlemenizi öneriyoruz. Bant genişliğinin tüm AP istemcileri tarafından paylaşıldığı düşünüldüğünde bu aralıktaki istasyon sayısı, erişim noktasında makul bir yük olmasını sağlar.</p>

18.4 Ayarları Güncelleme

Yük dengeleme ayarlarını güncellemek için:

1. *Load Balancing* (Yük Dengeleme) sekmesine gidin.
2. Yük dengeleme ayarlarını gerekli şekilde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

19.1 QoS'i Anlama	187
19.1.1 QoS ve Yük Dengeleme	187
19.1.2 802.11e ve WMM Standartları Desteği	187
19.1.3 QoS Kuyukları ve Trafik Akışını Koordine Etme Parametreleri	188
19.1.3.1 QoS Kuyukları ve Paketlerdeki Hizmet Türleri (ToS)	188
19.1.3.2 Veri Çerçevelerinin EDCF Kontrolü ve Çerçeveler Arası Karar Verme Aralığı	190
19.1.3.3 Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi	191
19.1.3.4 Daha İyi Performans İçin Paket Artırma	191
19.1.3.5 İstemci İstasyonları İçin Aktarım Olanığı (TXOP) Aralığı	192
19.1.4 802.1p ve DSCP Etiketleri	192
19.1.4.1 VLAN Önceliği	193
19.1.4.2 DSCP Önceliği	194
19.2 QoS Kuyuklarını Yapılandırma	194
19.2.1 AP EDCA Parametrelerini Yapılandırma	196
19.2.2 Wi-Fi Multimedyaı Etkinleştirme/Devre Dışı Bırakma	198
19.2.3 İstasyon EDCA Parametrelerini Yapılandırma	198
19.3 Ayarları Güncelleme	200

Hizmet Kalitesi (**QoS**), *IP Üzerinden Ses* (VoIP); diğer ses, video ve medya akışı türleri ve standart 9160 G2 Kablosuz Ağ Geçidi üzerinden IP verisi gibi farklı kablosuz trafiklerinin daha fazla verim ve daha iyi performans sunması için birden fazla kuyrukta parametreler belirlemenizi sağlar.

Aşağıdaki bölümlerde 9160 G2 Kablosuz Ağ Geçidi cihazında Hizmet Kalitesi kuyruklarının nasıl yapılandırıldığı anlatılmaktadır.

19.1 QoS'i Anlama

Fazla sayıdaki istemcinin hava dalgalarına erişme denemelerinin neden olduğu ağ tıkanıklığı ve günün yoğun bir anında bant genişliği için yarışan yüksek trafik hacmi, QoS'i etkileyen ana faktörlerdir. Yoğun, aşırı yüklü bir ağın hizmet kalitesindeki düşüş, en belirgin olarak *IP Üzerinden Ses* (VoIP) ve medya akışı gibi zaman açısından duyarlı uygulamalarda kendini gösterir.

QoS'teki değişikliklerden daha az etkilenen tipik veri dosyalarından farklı olarak Video, VoIP ve medya akışı istikrarlı bir hızda belirli bir sırada gönderilmeli ve Paket aktarımları arasında minimum bekleme süresi olmalıdır. Hizmet kalitesinden ödün verilirse ses ya da video bozulur.

19.1.1 QoS ve Yük Dengeleme

Yük dengeleme (bkz. Bölüm 18: “Yük Dengeleme”) ve QoS tekniklerini birlikte kullanarak zaman açısından duyarlı uygulamalar için yoğun bir ağda bile yüksek kaliteli hizmet sunabilirsiniz. Yük dengeleme, trafik yükünü erişim noktalarına daha uygun bir biçimde dağıtma yöntemidir. QoS, tek bir erişim noktasındaki farklı kablosuz trafiği türleri için aktarım önceliklerini temel alarak bant genişliği ve ağ erişimini paylaştırma yöntemidir.

19.1.2 802.11e ve WMM Standartları Desteği

QoS, paylaşılan ağ bağlantılarındaki veri akışlarını kontrol etmek için kullanılan çeşitli teknolojileri ifade eder. **IEEE 802.11e** işlem grubu, kablosuz ağlardaki aktarım kalitesi ve hizmet kullanılabilirliği için bir QoS standardı tanımlama sürecindedir. QoS, ağ tıkanıklığını en aza indirerek; Sapma, Gecikme ve Paket Kaybı faktörlerini sınırlayarak; zaman açısından duyarlı ya da kritik önem taşıyan uygulamalar için ayrılan bant genişliğini destekleyerek ve kanal erişimi için kablosuz trafiğine öncelik vererek daha iyi ağ hizmeti sağlamak için tasarlanmıştır.

Tüm IEEE **802.11** çalışma grubu standartlarında olduğu gibi amaç, farklı şirketlerden gelen bileşenlerin birlikte çalışmasını sağlayacak bir QoS özelliklerini uygulama standardı sunmaktır.

9160 G2 Kablosuz Ağ Geçidi, **802.11e** özelliklerinin bir alt grubunun uygulamaları olan *Kablosuz Multimedya (WMM)* teknik özellikleri ve *Kablosuz Multimedya (WMM)* standartlarına dayanan bir QoS sunar.

Hem erişim noktaları hem de kablosuz istemciler (dizüstü bilgisayarlar, tüketici elektroniği ürünleri) WMM etkin olabilir.

19.1.3 QoS Kuyrukları ve Trafik Akışını Koordine Etme Parametreleri

9160 G2 Kablosuz Ağ Geçidi cihazındaki QoS seçeneklerini yapılandırma işlemi, farklı kablosuz trafiği türleri için mevcut kuyruklarda parametreler ayarlamayı içerir. Gönderilen medya gerekliliklerini temel alarak her kuyruktaki paket aktarımları için farklı minimum ve maksimum bekleme süreleri yapılandırabilirsiniz. Kuyruklar Ses, Video, multimedya ve kritik önem taşıyan uygulamalar için otomatik olarak minimum aktarım bekleme süresi sağlar ve standart IP verileri için en iyi çaba parametrelerine dayanır.

Örneğin, zaman açısından duyarlı Ses, Video ve multimedya verilerine etkin olarak daha yüksek aktarım önceliği verilirken (kanallar arası daha düşük bekleme süresi) zaman açısından daha az duyarlı ancak genellikle daha fazla veri içeren diğer uygulamalar ve standart IP verilerinin daha uzun bekleme sürelerini tolere etmesi beklenir.

9160 G2 Kablosuz Ağ Geçidi, IEEE Kablosuz Multimedya (WMM) standardını temel alarak QoS uygular. Linux tabanlı kuyruk sınıfları paketleri etiketlemek ve birden fazla kuyruk oluşturmak için kullanılır. Sağlanan kuyruklar, iletilen veri türüne göre dahili önceliklendirme ve yönlendirme sunar.

Yönetim Kullanıcı Arabirimi, kuyruklarda parametre yapılandırmanız için bir yöntem sunar.

19.1.3.1 QoS Kuyrukları ve Paketlerdeki Hizmet Türleri (ToS)

9160 G2 Kablosuz Ağ Geçidi cihazındaki QoS, **IP** paketi başlığındaki Hizmet Türü (**ToS**) ile ilişkili **WMM** bilgisinden yararlanır. Ağ üzerinden gönderilen her IP paketinin başlığında verinin nasıl önceliklendirilmesi ve ağ üzerinden iletilmesi gerektiğini belirten bir ToS alanı bulunur. ToS alanı 3 - 7 bit arası bir değerden oluşur. Her bit bu verinin farklı bir yönünü ya da öncelik derecesini ve diğer meta bilgileri (düşük bekleme süresi, yüksek verim, yüksek güvenilirlik, düşük maliyet vb.) temsil eder.

Örneğin, büyük miktarlardaki verileri tek seferde iletebilme özelliği FTP için kritik önem taşıdığından FTP veri paketlerine yönelik ToS'nin maksimum verime ayarlanma ihtimali yüksektir. Bu durumda etkileşimli geri bildirim alınması güzel olur ancak çok gerekli değildir. Minimum bekleme süresi VoIP veri paketlerinin kalitesi ve performansı için kritik bir faktör olduğundan bu paketler minimum bekleme süresine ayarlanır.

Erişim noktası, AP'den geçen tüm paketlerin başlıklarındaki ToS alanını inceler. Paketin ToS alanında yer alan değere bağlı olarak AP, öncelikli şekilde iletilmesi için paketi kuyruklardan birine atar. Bu süreç QoS'i kasten yapılandırıp yapılandırmamanızdan bağımsız olarak otomatik bir şekilde gerçekleşir.

Hey kuyruk farklı bir veri türüyle ilişkilendirilir. Aktarım sırasında kullanılan kuyruk, ilişkili öncelikler ve parametreler şöyledir:

- Veri 0 (Ses). En yüksek öncelikli kuyruk, minimum bekleme süresi. IP Üzerinden Ses (VoIP) gibi zaman açısından duyarlı veriler otomatik olarak bu kuyruğa gönderilir.
- Veri 1 (Video). Yüksek öncelikli kuyruk, minimum bekleme süresi. Video ve diğer medya akışları gibi zaman açısından duyarlı veriler otomatik olarak bu kuyruğa gönderilir.
- Veri 2 (En İyi Çaba). Orta derecede öncelikli kuyruk, orta derecede verim ve bekleme süresi. En standart IP verileri bu kuyruğa gönderilir.
- Veri 3 (Arka plan). En düşük öncelikli kuyruk, yüksek verim. Maksimum verim gerektiren ve zaman açısından duyarlı olmayan yığın halindeki veriler (örneğin FTP verileri) bu kuyruğa gönderilir.

Daha yüksek öncelikli bir kuyruktaki bulunan paketler daha düşük öncelikli bir kuyruktaki paketlerden daha önce iletilir. Kuyruktaki "Veri 0" ve "Veri 1" olarak etiketlenmiş etkileşimli veriler her zaman ilk olarak gönderilir. "Veri 2" etiketli en iyi çaba verileri ikinci olarak, "Veri 3" etiketli arka plan (yığın) verileri en son olarak gönderilir. Düşük öncelikli kuyrukların (trafik sınıfı) her biri, yüksek trafik sınıfları gönderildikten sonra artı kalan bant genişliğini kullanır. Erişim noktasını her zaman meşgul edecek yeteri kadar etkileşimli veriniz varsa düşük öncelikli trafik hiçbir zaman gönderilmez.

Yönetim kullanıcı arabirimindeki QoS ayarlarını kullanarak erişim noktası tarafından istemciye ya da istemciden erişim noktasına gönderilen her kuyruğa nasıl davranılacağını belirleyen *Gelişmiş Dağıtılmış Kanal Erişimi* (EDCA) parametrelerini yapılandırabilirsiniz.



Not: Kablosuz trafiği şu şekilde ilerler:

- Erişim noktasından istemci istasyonuna doğru aşağı akış.
- İstemci istasyonundan erişim noktasına doğru yukarı akış.
- Erişim noktasından ağa doğru yukarı akış.
- Ağdan erişim noktasına doğru aşağı akış.

WMM etkinken 9160 G2 Kablosuz Ağ Geçidi'ndeki QoS ayarları yukarıda belirtilenlerin ilk ikisini, yani erişim noktasından istemci istasyonuna (AP EDCA parametreleri) doğru olan aşağı akış trafiği ve istasyondan erişim noktasına (istemci EDCA parametreleri) doğru olan yukarı akış trafiğini etkiler.

WMM devre dışyken halen AP'den istemci istasyonuna (AP EDCA parametreleri) doğru olan aşağı akış üzerinde parametre oluşturabilirsiniz.

Trafik akışının diğer aşamaları (ağa gelen ve ağdan giden akışlar) AP'deki QoS ayarlarının kontrolünde değildir.

19.1.3.2 Veri Çerçevelerinin EDCF Kontrolü ve Çerçeveler Arası Karar Verme Aralığı

Veriler 802.11 kablosuz ağları üzerinden *çerçeveler* halinde iletilirler. *Çerçeve*, kablosuz bir ağda iletilmek üzere paketlenmiş bazı açıklayıcı meta bilgilerin yanında ayrı bir veri grubundan oluşur.



Not: Çerçeve, kavram olarak Paket ile benzerlik gösterir. Paketler Ağ katmanında (OSI modelinde 3. katman) çalışırken çerçeveler Veri-Bağlantı katmanında (OSI modelinde 2. katman) çalışır.

Her çerçevede kaynak ve hedef MAC adresi, protokol versiyonlu bir kontrol alanı, çerçeve türü, çerçeve sekans numarası, çerçeve gövdesi (iletilecek gerçek bilgiyle birlikte) ve hata algılama için çerçeve kontrolü sekansı vardır.

802.11 standardı kablosuz altyapısının yönetimi, denetimi ve veri aktarımı için çeşitli *çerçeve türleri* tanımlar. 802.11 çerçeve türleri şunlardır: (1) *yönetim çerçeveleri*, (2) *kontrol çerçeveleri* ve (3) *veri çerçeveleri*. Kablosuz altyapısının kullanılabilirliğini yöneten ve kontrol eden yönetme ve kontrol çerçeveleri aktarım sırasında otomatik olarak daha yüksek önceliğe sahiptir.

802.11e, hangi çerçevelerin uygun kanallara erişeceğini belirlemek ve farklı veri türlerinin aktarımı için bekleme sürelerini koordine etmek için *çerçeveler arası aralığı* kullanır.

Yönetim ve kontrol çerçeveleri veri aktarımı için minimum süre, yani *kısa çerçeveler arası aralık* (SIF) kadar bekler. Bu bekleme süreleri altyapı desteği olarak 802.11'de dahili şekilde bulunur ve yapılandırılmaz.

9160 G2 Kablosuz Ağ Geçidi, *Gelişmiş Dağıtım Koordinasyonu İşlevini (EDCF) 802.11e* standardında tanımlandığı şekilde destekler. **DCF** standardının iyileştirilmiş versiyonu olan ve **CSMA/CA** protokolüne dayanan EDCF, *veri çerçeveleri* arasındaki çerçeveler arası aralığı (IFS) tanımlar. Veri çerçeveleri aktarımdan önce çerçeveler arası karar verme aralığı (AIFS) olarak tanımlanan bir süre boyunca bekler.

Bu parametre yapılandırılabilir.



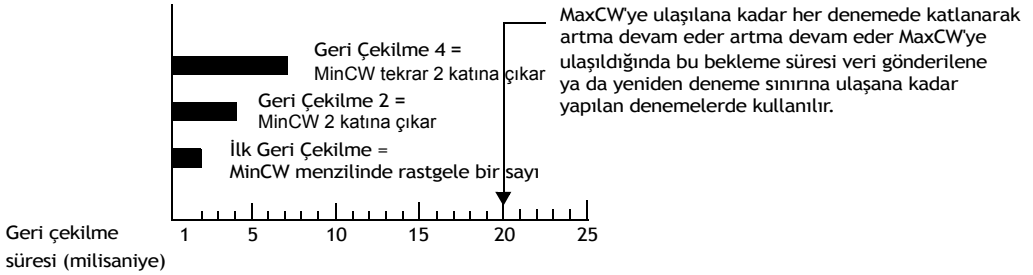
Not: Veri çerçevelerini AIFS'te göndermek daha yüksek öncelikli yönetim ve kontrol çerçevelerinin SIF'lere daha önce gönderilmesini sağlar.

AIFS, birden fazla erişim noktasının aynı anda veri göndermemesini, bunun yerine bir kanal boşalana kadar beklemesini sağlar.

19.1.3.3 Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi

Bir erişim noktası ortamın kullanımda (meşgul) olduğunu algılayarsa belirtilen kanala tekrar erişmeye çalışmadan önce bekleyeceği süreyi belirlemek için DCF *rastgele geri çekilme* zamanlayıcısını kullanır. Her erişim noktası yeniden denemeler arasında rastgele bir süre bekler. Bekleme süresi (ilk başta *Minimum Çatışma Penceresi* olarak belirtilen bir aralıktaki rastgele bir değer) belirli bir sınıra kadar (*Maksimum Çatışma Penceresi*) katlanarak artar. Birden fazla AP'nin ortama aynı anda eriştiği ve eş zamanlı olarak veri aktarmayı denediği durumlarda rastgele bekleme süresi, çarpışmaların çoğunu engeller. Bir ağda ne kadar fazla etkin kullanıcınız varsa geri çekilme zamanlayıcısının çarpışma ve yeniden aktarmaların sayısını azaltma konusunda o kadar fazla performans kazancı olur.

Şekil 19.1 DCF Rastgele Geri Çekilme Zamanlayıcısı



Erişim noktası tarafından kullanılan rastgele geri çekilme, yapılandırılabilen bir parametredir. Rastgele bekleme süresini açıklamak için "Minimum Çatışma Penceresi" (MinCW) ve "Maksimum Çatışma Penceresi" (MaxCW) tanımlanmıştır.

- *Minimum Çatışma Penceresi* olarak belirlenen değer, ilk rastgele geri çekilme bekleme süresi aralığının en üst sınırıdır. Rastgele geri çekilmeden kullanılan sayı ilk başta 0 ile Minimum Çatışma Penceresinde tanımlanan sayı arasında rastgele bir sayıdır.
- İlk rastgele geri çekilme süresi veri çerçevesi başarıyla aktarılmadan önce biterse erişim noktası yeniden deneme sayacını artırır ve rastgele geri çekilme penceresinin değerini iki katına çıkarır. *Maksimum Çatışma Penceresi* olarak belirlenen değer, bu rastgele geri çekilmeyi iki katına çıkarma işlemi için en üst sınırdır. İki katına çıkarma işlemi veri çerçevesi gönderilene ya da Maksimum Çatışma Penceresi boyutuna ulaşılan kadar devam eder.

19.1.3.4 Daha İyi Performans İçin Paket Artırma

9160 G2 Kablosuz Ağ Geçidi, veri verimini ve kablosuz ağ üzerinden aktarım hızını artıran *paket artırma* teknolojisi tabanlı 802.11e'yi içerir. Paket artırma, başlık bilgisi ekstra yükü olmadan birden çok paketin aktarılmasını sağlar. Bu sayede ağ hızı ve veri verimi artar. İzin verilen paket artırma boyutu (maksimum artırma uzunluğu) yapılandırılabilen bir parametredir.

19.1.3.5 İstemci İstasyonları İçin Aktarım Olanağı (TXOP) Aralığı

Aktarım Olanağı (TXOP), bir Wi-Fi Multimedya (WMM) istemci istasyonunun kablosuz ortam (WM) üzerinde aktarım başlatma hakkına sahip olduğu zaman aralığıdır.

19.1.4 802.1p ve DSCP Etiketleri

IEEE **802.1p**, IEEE 802 standardının bir uzantısıdır ve QoS sağlamadan sorumludur. 802.1p'nin temel amacı veri bağlantısı/MAC katmanındaki ağ trafiğine öncelik vermektir. 802.1p, çoklu gönderim trafiğini filtreleme özelliği sunarak 2. katmanla anahtarlanmış ağları geçmemesini sağlar. Öncelik verme şeması için etiketleme çerçevelerini kullanır. 2. katman anahtarlarının bu standartla uyumlu olması için gelen LAN paketlerini ayrı trafik sınıfları olarak gruplayabilmesi gerekir.

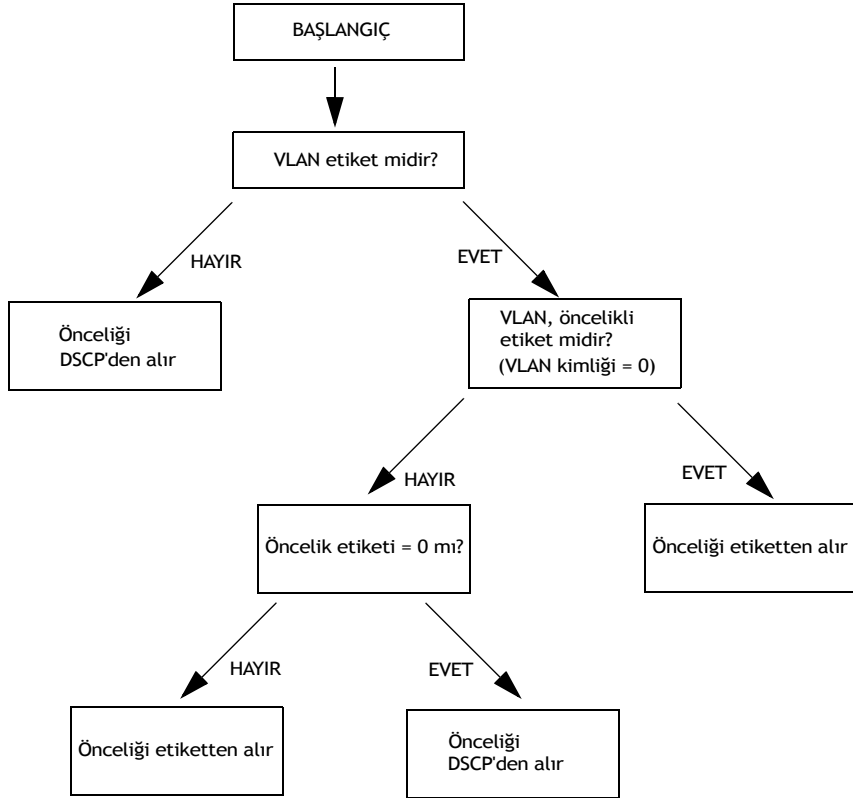
802.1p başlığı, paketlerin çeşitli trafik sınıflarına ayrılmasını sağlayan üç bitlik önceliklendirme alanı içerir. Sekiz tane öncelik seviyesi tanımlanmıştır. En yüksek öncelik olan yedi, ağ için kritik önem taşıyan trafiğe (sese) gidebilir. Daha yüksek önceliğe sahip paketler her zaman ilk olarak aktarılır. Yüksek öncelikli paketlerin aktarımı devam ediyorsa düşük öncelikli paketler aktarılmaz; yüksek öncelikli paketler başarıyla aktarılanlara kadar kuyrukta bekletilirler. En düşük öncelik seviyesi sıfırdır; bu değer varsayılan en iyi çaba olarak kullanılır ve herhangi bir değer ayarlanmadığında otomatik olarak açılır.



Not: QoS ve WMM etkinleştirilmeden 802.1p'nin çalışmayacağını unutmayın. WMM'nin hem AP'de hem de AP'ye bağlanan istemcide etkinleştirilmiş olması gerekir.

Şekil 19.2'deki akış şeması, ağda etiketlerin alınışını ve trafiğe öncelik verilen durumları gösterir.

Şekil 19.2 Ağ Trafikinin Önceliklendirilmesi



19.1.4.1 VLAN Önceliği

Tablo 19.1, öncelik etiketlerini ve bir VLAN etiketinden aldıkları ilişkili değerleri gösterir.

Tablo 19.1 VLAN Etiket Öncelikleri

VLAN Kimliği Etiketi	Öncelik
0 - varsayılan DHCP değeri	En İyi Çaba
1	Arka plan
2	Arka plan
3	En İyi Çaba

Tablo 19.1 VLAN Etiket Öncelikleri (Devamı)

VLAN Kimliği Etiketi	Öncelik
4	Video
5	Video
6	Ses
7	Ses

19.1.4.2 DSCP Önceliği

Tablo 19.2 DSCP değerlerini, ilişkili kimliği ve öncelik seviyesini gösterir.

Tablo 19.2 DSCP Etiket Öncelikleri

Kimlik Etiketi	Öncelik	DSCP Değeri
0 - varsayılan DHCP değeri	En İyi Çaba	0
1	Arka plan	16
2	Arka plan	8
3	En İyi Çaba	24
4	Video	32
5	Video	40
6	Ses	48
7	Ses	56

19.2 QoS Kuyruklarını Yapılandırma

QoS kuyrukları ayarlamak için *Services > QoS* (Hizmetler > QoS) sekmesine gidin ve ayarları aşağıda anlatıldığı gibi yapılandırın.

Şekil 19.3 Hizmet Kalitesi (QoS) Ayarları

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Modify QoS queue parameters

Queue

AIFS

cwMin

cwMax

Max. Burst

Data 0 (Voice)

1

3

7

1.5

Data 1 (Video)

1

7

15

3.0

Data 2 (Best Effort)

3

15

63

0

Data 3 (Background)

7

15

1023

0

AP EDCA parameters

Wi-Fi Multimedia (WMM)

Enabled

Disabled

Queue

AIFS

cwMin

cwMax

TXOP Limit

Data 0 (Voice)

2

3

7

47

Data 1 (Video)

2

7

15

94

Data 2 (Best Effort)

3

15

1023

0

Data 3 (Background)

7

15

1023

0

Station EDCA parameters

Update

9160 G2 Kablosuz Ağ Geçidi cihazında Hizmet Kalitesinin (**QoS**) yapılandırılması işlemi, farklı kablosuz trafiği türleri için mevcut kuyruklarda parametre ayarlama ve aktarım için (*Çatışma Penceresi* aracılığıyla) etkili biçimde minimum ve maksimum bekleme süreleri belirlemeyi içerir. Burada açıklanan ayarlar yalnızca erişim noktasındaki veri aktarma davranışları için geçerlidir; istemci istasyonundaki veri aktarma davranışları için geçerli değildir.



Not: Konuk arabiriminde QoS kuyruk ayarları, bütün olarak erişim noktası yükü (iki BSS birlikte) için geçerlidir.

İki telsizli bir erişim noktasında bu ayarlar iki telsiz için de geçerlidir ancak her telsiz trafiğinin kuyruğu farklıdır. (Aşağıda belirtildiği gibi konuk trafiği bir istisnadır.)

Dahili ve Konuk ağ trafiikleri her telsizde her zaman aynı kuyruğu kullanır. Bu durum hem tek telsizli hem de iki telsizli AP'ler için geçerlidir.

Erişim noktasındaki QoS, IP paket başlığındaki Hizmet Türüyle (ToS) ilgili mevcut bilgilerden yararlanır. Erişim noktası, AP'den geçen tüm paketlerin başlıklarındaki ToS alanını inceler. Paketin ToS alanında yer alan değere bağlı olarak AP, öncelikli şekilde iletilmesi için paketi kuyruklardan birine atar. Her kuyruk farklı bir veri türüyle ilişkilendirilir. Erişim noktasından gönderildiğinde her kuyruğa nasıl davranılacağını belirleyen parametreler yapılandırılabilir.

Hizmet Kalitesi yapılandırma şunları içerir:

- “AP EDCA Parametrelerini Yapılandırma”, sayfa 196.
- “Wi-Fi Multimedya Etkinleştirme/Devre Dışı Bırakma”, sayfa 198.
- “Ayarları Güncelleme”, sayfa 200.

19.2.1 AP EDCA Parametrelerini Yapılandırma

AP Gelişmiş Dağıtılmış Kanal Erişimi (EDCA) Parametreleri erişim noktasından istemci istasyonuna doğru akan trafiği etkiler.

Tablo 19.3 AP EDCA Parametreleri

Alan	Açıklama
<i>Queue (Kuyruk)</i>	<p>Kuyruklar AP'den istasyona aktarılan farklı veri türlerine göre tanımlanır:</p> <p>Veri 0 (Ses)</p> <p>Yüksek öncelikli kuyruk, minimum bekleme süresi. VoIP ve medya akışları gibi zaman açısından duyarlı veriler otomatik olarak bu kuyruğa gönderilir.</p> <p>Veri 1 (Video)</p> <p>Yüksek öncelikli kuyruk, minimum bekleme süresi. Zaman açısından duyarlı video verileri otomatik olarak bu kuyruğa gönderilir.</p> <p>Veri 2 (En İyi Çaba)</p> <p>Orta derecede öncelikli kuyruk, orta derecede verim ve bekleme süresi. En standart IP verileri bu kuyruğa gönderilir.</p> <p>Veri 3 (Arka plan)</p> <p>En düşük öncelikli kuyruk, yüksek verim. Maksimum verim gerektiren ve zaman açısından duyarlı olmayan yığın halindeki veriler (örneğin FTP verileri) bu kuyruğa gönderilir.</p> <p>Daha fazla bilgi için bkz. “QoS Kuyrukları ve Trafik Akışını Koordine Etme Parametreleri”, sayfa 188.</p>

Tablo 19.3 AP EDCA Parametreleri (Devamı)

Alan	Açıklama
<i>AIFS</i> (<i>Inter-Frame Space</i>) (<i>Çerçeveler Arası Aralık</i>)	<p>Çerçeveler Arası Karar Verme Aralığı (AIFS) veri çerçeveleri için bekleme süresi (milisaniye cinsinden) belirler.</p> <p>AIFS için geçerli değerler 1 - 255 arasındır.</p> <p>Daha fazla bilgi için Veri Çerçevelerinin DCF Kontrolü ve Çerçeveler Arası Aralık bölümüne bakın.</p> <p>Daha fazla bilgi için bkz. "Veri Çerçevelerinin EDCF Kontrolü ve Çerçeveler Arası Karar Verme Aralığı", sayfa 190.</p>
<i>cwMin</i> (<i>Minimum Contention Window</i>) (<i>Minimum Çatışma Penceresi</i>)	<p>Bu parametre bir aktarımın yeniden denenmesi için gereken ilk rastgele geri çekilme bekleme süresini ("pencere") belirleyen algoritmanın girişidir.</p> <p><i>Minimum Çatışma Penceresinde</i> belirtilen değer, ilk rastgele geri çekilme bekleme süresinin belirlendiği aralığın üst sınırıdır (milisaniye cinsinden).</p> <p>İlk rastgele sayı, 0 ile burada belirtilen sayı arasında olacaktır.</p> <p>İlk rastgele geri çekilme bekleme süresi, veri çerçevesi gönderilmeden önce dolarsa yeniden deneme sayacı artar ve rastgele geri çekilme değeri (penceresi) iki katına çıkar. Rastgele geri çekilme değeri Maksimum Çatışma Penceresinde tanımlanan sayıya ulaşana kadar ikiye katlanma devam eder.</p> <p>"cwmin" için geçerli değerler şunlardır: 1, 3, 7, 15, 31, 63, 127, 255, 511 ya da 1023.</p> <p>Daha fazla bilgi için bkz. "Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi", sayfa 191.</p>
<i>cwMax</i> (<i>Maksimum Çatışma Penceresi</i>)	<p><i>Maksimum Çatışma Penceresinde</i> belirtilen değer, rastgele geri çekilme değerinin ikiye katlanması için belirlenen üst sınırdır (milisaniye cinsinden). İki katına çıkarma işlemi veri çerçevesi gönderilene ya da Maksimum Çatışma Penceresi boyutuna ulaşılan kadar devam eder.</p> <p>Maksimum Çatışma penceresi boyutuna ulaşıldığında izin verilen maksimum yeniden deneme sayısına ulaşılana kadar yeniden deneme işlemleri devam eder.</p> <p>"cwmax" için geçerli değerler şunlardır: 1, 3, 7, 15, 31, 63, 127, 255, 511 ya da 1023.</p> <p>Daha fazla bilgi için bkz. "Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi", sayfa 191.</p>

Tablo 19.3 AP EDCA Parametreleri (Devamı)

Alan	Açıklama
<i>Max. Burst Length</i> (Maksimum Artırma Uzunluğu)	Yalnızca AP EDCA Parametresi (Maksimum Artırma Uzunluğu yalnızca erişim noktasından istemci istasyonuna doğru akan trafik için geçerlidir.) Bu değer, kablosuz ağda paket artışı için izin verilen Maksimum Artırma Uzunluğunu (milisaniye cinsinden) belirtir. <i>Paket artışı</i> , başlık bilgisi olmadan iletilen birden çok çerçeveden oluşan bir koleksiyondur. Azalan yük, daha fazla verim alınmasını ve daha iyi bir performans elde edilmesini sağlar. Maksimum artırma uzunluğu için geçerli değerler 0,0 ile 999,9 arasındadır. Daha fazla bilgi için bkz. "Daha İyi Performans İçin Paket Artırma", sayfa 191.

19.2.2 Wi-Fi Multimedya Etkinleştirme/Devre Dışı Bırakma

Wi-Fi MultiMedya (WMM), varsayılan olarak erişim noktasında etkinleştirilmiştir. WMM etkinken QoS önceliklendirme ve kablosuz ortam erişiminin koordinasyonu açıktır. WMM etkinken 9160 G2 Kablosuz Ağ Geçidi cihazındaki QoS ayarları, erişim noktasından istemci istasyonuna (AP EDCA parametreleri) doğru olan *aşağı akış* trafiği ve istasyondan erişim noktasına (istasyon EDCA parametreleri) doğru olan *yukarı akış* trafiğini kontrol eder.

WMM'nin devre dışı bırakılması, istasyon EDCA parametrelerinin istasyondan erişim noktasına doğru olan *yukarı akış* trafiği üzerindeki QoS kontrolünü devre dışı bırakır.

WMM devre dışıyken halen erişim noktasından istemci istasyonuna (AP EDCA parametreleri) doğru olan *aşağı akış* üzerinde parametre oluşturabilirsiniz.

- WMM uzantılarını devre dışı bırakmak için **Disabled** (Devre Dışı) seçeneğine tıklayın.
- WMM uzantılarını etkinleştirmek için **Enabled** (Etkin) seçeneğine tıklayın.

19.2.3 İstasyon EDCA Parametrelerini Yapılandırma

İstasyon Gelişmiş Dağıtılmış Kanal Erişimi (EDCA) Parametreleri istemci istasyonundan erişim noktasına doğru olan trafik akışını etkiler.

Tablo 19.4 İstasyon EDCA Parametreleri

Alan	Açıklama
<i>Queue (Kuyruk)</i>	<p>Kuyruklar istasyondan AP'ye aktarılan farklı veri türlerine göre tanımlanır:</p> <p>Veri 0 (Ses)</p> <p>En yüksek öncelikli kuyruk, minimum bekleme süresi. VoIP ve medya akışları gibi zaman açısından duyarlı veriler otomatik olarak bu kuyruğa gönderilir.</p> <p>Veri 1 (Video)</p> <p>En yüksek öncelikli kuyruk, minimum bekleme süresi. Zaman açısından duyarlı video verileri otomatik olarak bu kuyruğa gönderilir.</p> <p>Veri 2 (En İyi Çaba)</p> <p>Orta derecede öncelikli kuyruk, orta derecede verim ve bekleme süresi. En standart IP verileri bu kuyruğa gönderilir.</p> <p>Veri 3 (Arka plan)</p> <p>En düşük öncelikli kuyruk, yüksek verim. Maksimum verim gerektiren ve zaman açısından duyarlı olmayan yığın halindeki veriler (örneğin FTP verileri) bu kuyruğa gönderilir.</p> <p>Daha fazla bilgi için bkz. "QoS Kuyrukları ve Trafik Akışını Koordine Etme Parametreleri", sayfa 188.</p>
<i>AIFS (Inter-Frame Space) (Çerçeveler Arası Aralık)</i>	<p><i>Çerçeveler Arası Karar Verme Aralığı (AIFS) veri çerçeveleri</i> için bekleme süresi (milisaniye cinsinden) belirler.</p> <p>Daha fazla bilgi için Veri Çerçevelerinin DCF Kontrolü ve Çerçeveler Arası Aralık bölümüne bakın.</p> <p>Daha fazla bilgi için bkz. "Veri Çerçevelerinin EDCF Kontrolü ve Çerçeveler Arası Karar Verme Aralığı", sayfa 190.</p>
<i>cwMin (Minimum Contention Window) (Minimum Çatışma Penceresi)</i>	<p>Bu parametre bir aktarımın yeniden denenmesi için gereken ilk rastgele geri çekilme bekleme süresini ("pencere") belirleyen algoritmanın girişidir.</p> <p><i>Minimum Çatışma Penceresinde</i> belirtilen değer, ilk rastgele geri çekilme bekleme süresinin belirlendiği aralığın üst sınırıdır (milisaniye cinsinden).</p> <p>İlk rastgele sayı, 0 ile burada belirtilen sayı arasında olacaktır.</p> <p>İlk rastgele geri çekilme bekleme süresi, veri çerçevesi gönderilmeden önce dolarsa yeniden deneme sayacı artar ve rastgele geri çekilme değeri (penceresi) iki katına çıkar. Rastgele geri çekilme değeri Maksimum Çatışma Penceresinde tanımlanan sayıya ulaşana kadar ikiye katlanma devam eder.</p> <p>Daha fazla bilgi için bkz. "Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi", sayfa 191.</p>

Tablo 19.4 İstasyon EDCA Parametreleri (Devamı)

Alan	Açıklama
<i>cwMax</i> (Maksimum Çatışma Penceresi)	<p>Maksimum Çatışma Penceresinde belirtilen değer, rastgele geri çekilme değerinin ikiye katlanması için belirlenen üst sınırdır (milisaniye cinsinden). İki katına çıkarma işlemi veri çerçevesi gönderilene ya da Maksimum Çatışma Penceresi boyutuna ulaşılan kadar devam eder.</p> <p>Maksimum Çatışma penceresi boyutuna ulaşıldığında izin verilen maksimum yeniden deneme sayısına ulaşılan kadar yeniden deneme işlemleri devam eder.</p> <p>Daha fazla bilgi için bkz. "Rastgele Geri Çekilme ve Minimum/Maksimum Çatışma Penceresi", sayfa 191.</p>
<i>TXOP Limit</i> (TXOP Sınırı)	<p>Yalnızca İstasyon EDCA Parametresi (TXOP Sınırı yalnızca istemci istasyonundan erişim noktasına doğru alan trafik için geçerlidir.)</p> <p>Aktarım Olanakı (TXOP), bir WME istemci istasyonunun kablosuz ortam (WM) üzerinde aktarım başlatma hakkına sahip olduğu zaman aralığıdır.</p> <p>Bu değer istemci istasyonlarının milisaniye cinsinden Aktarım Olanakını (TXOP), yani bir WMM istemci istasyonunun kablosuz ortam üzerinde aktarım başlatma hakkına sahip olduğu zaman aralığını belirtir.</p>

19.3 Ayarları Güncelleme

QoS ayarlarını güncellemek için:

1. *QoS* sekmesine gidin.
2. QoS ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

20.1 Kablosuz Dağıtım Sistemini Anlama	203
20.1.1 WDS'yi Uzak Kablolulu LAN'ları Birleştirmek İçin Kullanma	203
20.1.2 WDS İle Ağ Kapsamını Kablolulu Kapsama Alanının Ötesine Taşıma	204
20.1.3 Yedekleme Bağlantıları Oluşturmak İçin WDS'yi Kullanma.	205
20.2 WDS Bağlantılarıyla İlgili Güvenlik Hususları.	205
20.2.1 Statik WEP Veri Şifrelemeyi Anlama.	206
20.2.2 WPA (PSK) Veri Şifrelemeyi Anlama	206
20.3 WDS Ayarlarını Yapılandırma	207
20.3.1 WDS Bağlantısı Yapılandırma Örneği	209
20.4 Ayarları Güncelleme	210

9160 G2 Kablosuz Ağ Geçidi cihazı, Kablosuz Dağıtım Sistemi (**WDS**) kullanarak birden fazla erişim noktasını bağlamanızı sağlar. WDS, erişim noktalarının birbirleriyle kablosuz olarak iletişim kurmasını sağlar. Bu özellik, gezici istemciler için ve birden fazla kablosuz ağ yönetirken sorunsuz bir deneyim sağlama konusunda kritik bir önem taşır. Ayrıca ihtiyaç duyulan kablo sayısını azaltarak ağ altyapısını basitleştirir.

Aşağıdaki bölümler 9160 G2 Kablosuz Ağ Geçidi cihazında WDS'nin nasıl yapılandırıldığını açıklamaktadır.

20.1 Kablosuz Dağıtım Sistemini Anlama

Kablosuz Dağıtım Sistemi (WDS), Genişletilmiş Hizmet Kümesi (ESS) oluşturmak için Temel Hizmet Kümeleri (BSS) olarak bilinen erişim noktalarını kablosuz olarak bağlayan bir teknolojidir.

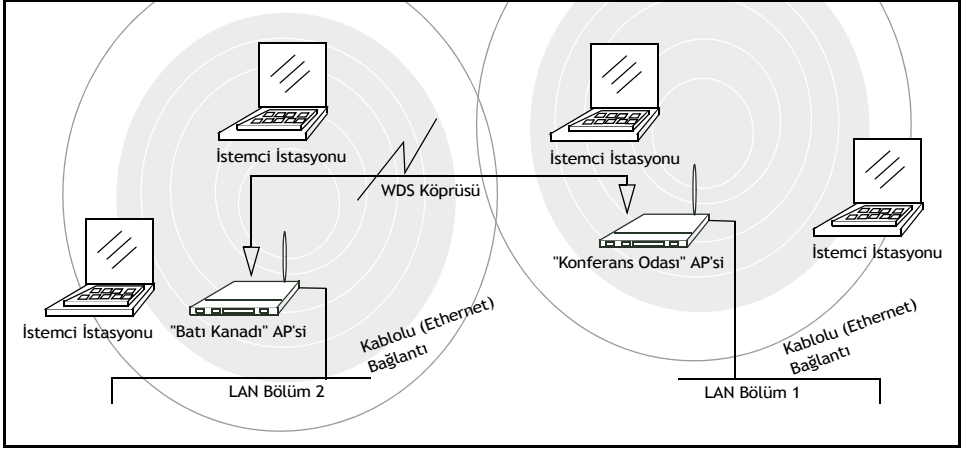


Not: BSS, birden fazla BSSID özelliğinin tek erişim noktalarını iki ya da daha fazla erişim noktası gibi gösterdiği durumlar dışında, genellikle bir erişim noktasına (tek AP'li kablosuz "ağ" olarak yerleştirilen) karşılık gelir. Bu gibi durumlarda erişim noktası birden fazla benzersiz BSSID'ye sahiptir.

20.1.1 WDS'yi Uzak Kablolu LAN'ları Birleştirmek İçin Kullanma

Bir **ESS**'de (birden çok erişim noktasından oluşan bir ağ) her erişim noktası, tek bir erişim noktasının kapsayamayacağı kadar büyük bir alanın bir bölümünde hizmet verir. Tek bir **LAN** oluşturmak amacıyla uzak Ethernet'leri birleştirmek için WDS'yi kullanabilirsiniz. Örneğin, ağa Ethernet ile bağlı olan erişim noktalarınızdan biri Konferans Odasındaki (LAN Bölüm 1) birden fazla istemci istasyonuna, diğeri ise Batı Kanadı ofislerindeki (LAN Bölüm 2) istasyonlara hizmet veriyor olsun. Konferans Salonundaki ve Batı Kanadındaki erişim noktalarını, bu iki alandaki istemcilere yönelik tek bir ağ oluşturmak için WDS bağlantısıyla birleştirebilirsiniz (bkz. Şekil 20.1, sayfa 204).

Şekil 20.1 Birleştirilen Uzak Kablolu LAN'lar

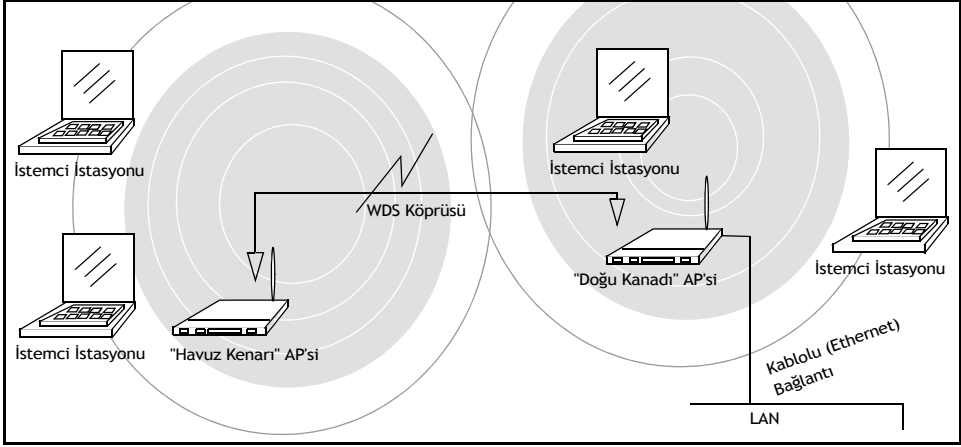


20.1.2 WDS ile Ağ Kapsamını Kablolu Kapsama Alanının Ötesine Taşıma

ESS, kablolanmanın zor, masraflı ya da verimsiz olduğu alanlarda ağın kapsama alanını genişletebilir.

Örneğin, ağa Ethernet ile bağlı olan ve bir alanda (bu örnekte "Doğu Kanadında") birden fazla istemci istasyonuna hizmet sunan ancak kapsama alanı dışındaki istasyonlara ulaşamayan bir ağınız olduğunu düşünelim. Ayrıca uzak alana Ethernet kablosu döşemenin çok zor ya da çok masraflı olduğunu varsayalım. İkinci grup istasyonun olduğu bölgenin (Şekil 20.1.3, sayfa 205'teki örneğe göre "Havuz Kenarının") yakınına ikinci bir erişim noktası yerleştirip WDS bağlantısıyla bu iki AP'yi birleştirerek bu sorunu çözebilirsiniz. Bu sayede uzak istasyonlara ulaşmak için ekstra bir erişim noktası sağlayarak ağınızı kablosuz olarak genişletebilirsiniz (bkz. Şekil 20.1.3, sayfa 205).

Şekil 20.2 Kapsamı Kablolu Kapsama Alanının Ötesine Taşınan Ağ



20.1.3 Yedekleme Bağlantıları Oluşturmak İçin WDS'yi Kullanma

WDS köprülemenin bir diğer kullanım amacı yedekleme bağlantıları oluşturmaktır. *Yayılan Ağaç Protokolü (STP)*, 9160 G2 Kablosuz Ağ Geçidi cihazında otomatik olarak etkinken WDS, ağdaki erişim noktaları arasında yedekleme yolları yapılandırmak için kullanılabilir. Örneğin, iki erişim noktası arasında hem Ethernet aracılığıyla birincil bir yola, hem de WDS bağlantısı aracılığıyla ikincil (yedek) bir kablosuz yola sahip olabilirsiniz. Ethernet bağlantısı kesilirse STP, yedek kablosuz yolu etkinleştirerek ağ haritasını yeniden yapılandırır ve ağın sorunlu kısmını etkili biçimde onarır.

20.2 WDS Bağlantılarıyla İlgili Güvenlik Hususları

WDS bağlantıları için birkaç güvenlik ayarı yapmak önemlidir. WDS bağlantısına, bağlantıdaki AP'ye uygulanan güvenlik ayarından bağımsız olarak bir güvenlik modu ayarlayabilirsiniz. Örneğin, güvenliği AP1'de **Yok**, AP2'de **WEP** olarak ayarlayabilirsiniz. İki ayar birbirinden farklı olmasına rağmen WDS bağlantısı için Yok ya da WEP güvenlik ayarından birini seçebilirsiniz. Bu kural için tek istisna, WPA'dır (PSK). WPA (PSK) güvenlik ayarı, yalnızca AP1'in ve AP2'nin WPA Kişisel ya da WPA Kurumsal güvenlik ayarlarından birine ayarlı olduğu durumlarda WDS bağlantısında ayarlanabilir.

20.2.1 Statik WEP Veri Şifrelemeyi Anlama

Statik *Kablolu Eş Değer Gizlilik (WEP)*, 802.11 kablosuz ağlar için bir veri şifreleme protokolüdür. Belirli bir WDS bağlantısındaki erişim noktalarının ikisi de aynı güvenlik ayarıyla yapılandırılmalıdır. Statik WEP'te veri şifreleme için ya statik 64 bit (40 bit gizli anahtar + 24 bit başlatma vektörü [IV]) ya da 128 bit (104 bit gizli anahtar + 24 bit IV) Paylaşılan Anahtar olarak belirtilir.

Statik *WEP*'i WDS bağlantısında (köprüsünde) etkinleştirebilirsiniz. WEP etkinleştirildiğinde WDS bağlantısındaki iki erişim noktası arasındaki tüm veri alışverişi sizin sağladığınız sabit bir WEP anahtarıyla şifrelenir.

Statik WEP, istemci istasyonlarına sunulan diğer güvenlik modlarının seviyesinde etkili bir veri koruması sağlamaz. Statik WEP'i güvenli kablosuz trafiği için kullanılan bir *LAN*'da kullanıyorsanız ağınızı riske atıyorsunuz demektir. Bu yüzden dahili ağınızdaki tüm WDS bağlantılarında WPA (PSK) şifrelemeyi kullanmanızı öneririz. Ağınızdaki veri trafiğinin güvenlik riskinden kaygı duyuyorsanız Statik WEP tabanlı WDS'yi Dahili ağdaki erişim noktalarını birleştirmek için kullanmayın. WPA (PSK) hakkında daha fazla bilgi için aşağıdaki “WPA (PSK) Veri Şifrelemeyi Anlama” bölümüne bakın.

Farklı güvenlik modlarının verimliliği hakkında daha fazla bilgi için bkz. Bölüm 10: “Güvenliği Yapılandırma”. Bu konu ayrıca daha az duyarlı veri trafiği için kullanılan Konuk ağındaki AP'den istasyona trafik akışı için şifrelenmemiş güvenlik modunun kullanımını da kapsamaktadır.

20.2.2 WPA (PSK) Veri Şifrelemeyi Anlama

Wi-Fi Korumalı Erişim (Önceden Paylaşılan Anahtar) ya da WPA (PSK), Statik WEP'ten daha güçlü bir güvenlik biçimidir. Önceden “WPA-Ev” olarak bilinen WPA (PSK), köprülenen bağlantıdaki AP'ler arasında paylaşılan bir şifre olan önceden paylaşılmış bir şifre kullanarak çalışır. WPA (PSK), uygulaması karmaşık ve masraflı olan RADIUS kimlik doğrulama altyapısına gerek duymadan gelişmiş bir 802.11 kablosuz güvenliği sunar.

WPA (PSK) şifreleme paylaşılan bir anahtarı temel aldığından, WDS bağlantısındaki iki AP de aynı anahtarla ayarlanmalıdır, aksi halde iletişim kurmaları ve bilgi paylaşımları mümkün değildir.



Not: Güvenlik sebebiyle WDS köprüsündeki paylaşılan anahtarları düzenli aralıklarla değiştirmenizi öneririz.

Farklı güvenlik modlarının verimliliği hakkında daha fazla bilgi için bkz. Bölüm 10: “Güvenliği Yapılandırma”.

20.3 WDS Ayarlarını Yapılandırma

Bu erişim noktasından diğerlerine doğru olan veri trafiğinin ayrıntılarını belirtmek için *Manage > WDS* (Yönet > WDS) sekmesine gidin ve ilgili alanları aşağıda anlatıldığı gibi güncelleyin.



Not: Şekil 20.3, iki telsizli AP'ler için WDS ayarları sayfasını gösterir. Tek telsizli AP'lerin Yönetim Web sayfası biraz daha farklı görünür.

Şekil 20.3 Kablosuz Dağıtım Sistemi Ayarları

Basic Settings	Configure WDS bridges to other access points
User Management	Local Address 00:08:A2:01:4B:56
Cluster	Remote Address <input type="text"/>
Access Points	Encryption None (Plain-text) ▼
Sessions	
Channel Management	Remote Address <input type="text"/>
Wireless Neighborhood	Encryption None (Plain-text) ▼
Security	
Status	Remote Address <input type="text"/>
Interfaces	Encryption None (Plain-text) ▼
Events	
Transmit/Receive	Remote Address <input type="text"/>
Client Associations	Encryption None (Plain-text) ▼
Neighboring Access Points	
Manage	Remote Address <input type="text"/>
Ethernet Settings	Encryption None (Plain-text) ▼
802.11 Settings	
802.11 Advanced Settings	<input type="button" value="Update"/>
VWN	
WDS	
Guest Login	

Aşağıdaki notlar **WDS** yapılandırmasıyla ilgili bazı önemli talimatları özetlemektedir. WDS yapılandırmasına başlamadan önce lütfen notların tamamını okuyun.



Not: WDS'yi kullanırken WDS bağlantısına katılan her iki erişim noktasında da WDS ayarlarını yapılandırdığınızdan emin olun.

Bir erişim noktası çiftinin arasında yalnızca bir WDS bağlantınız olabilir. Bunun anlamı, uzak bir MAC adresi belirli bir erişim noktası için yalnızca bir kez WDS sayfasında görünebilir.

WDS bağlantısına katılan erişim noktalarının ikisi de aynı Telsiz kanalında olmalı ve aynı IEEE 802.11 modunu kullanmalıdır. (Telsiz modunu ve kanalı yapılandırma hakkında bilgi için bkz. Bölüm 16: “802.11 Telsiz Ayarlarını Yapılandırma”.)

802.11h kullanımdayken WDS bağlantıları kurmak zor olabilir. Bkz. “802.11h Düzenleyici Etki Alanı Kontrolü”, sayfa 148.

Bu erişim noktasındaki WDS'yi yapılandırmak için veri transferi yapılacak ve bu AP'ye bilgi gönderecek her AP'yi açıklayın. Tüm hedef AP'leri için Tablo 20.1'de gösterildiği gibi açıklamalar gereklidir.

Tablo 20.1 Hedef Erişim Noktası Ayarları

Alan	Açıklama
<i>Local Address</i> (Yerel Adres)	<p>Bu erişim noktası için Ortam Erişim Denetimi (MAC) adreslerini belirtir.</p> <p>MAC adresi, bir arabirimi ağa tanıtan herhangi bir cihazın kalıcı ve benzersiz donanım adresidir. MAC adresi üretici tarafından atanır. MAC adresini değiştiremezsiniz. Erişim noktasının ya da arabirimin benzersiz bir tanımlayıcısı olduğu için burada bilgi vermek amacıyla değinilmiştir.</p> <p>Tek Telsizli AP:</p> <p>Tek telsizli bir erişim noktasında, WDS ayarları sayfasının üst kısmında tek bir MAC adresi görüntülenir. Tek telsizli AP için görüntülenen adres, bu telsiz AP'sinin MAC adresidir. AP, dışarıdaki diğer ağlar tarafından bu adresle bilinir.</p> <p>İki Telsizli AP:</p> <p><i>Yerel Adres</i>, iki telsizli bir AP'deki her WDS bağlantısı için seçilen telsizin (WLAN0'da Telsiz 1 ya da WLAN1'de Telsiz 2) dahili arabiriminin MAC adresini yansıtır.</p>
<i>Remote Address</i> (Uzak Adres)	<p>Hedef erişim noktasının (verilerin gönderileceği ya da "aktarılabacağı" ve alınacağı erişim noktası), başka bir deyişle WDS köprüsü oluşturduğunuz AP'nin MAC adresini belirtin.</p> <p><i>Remote Address</i> (Uzak Adres) alanının sağındaki ok işaretine tıklayarak ağdaki tüm kullanılabilir MAC Adreslerini ve ilgili SSID'lerini görebilirsiniz. Listedeki uygun MAC adresini seçin.</p> <p>Not: Açılır listede görüntülenen SSID, hedef erişim noktası için doğru MAC Adresini tanımlamanıza yardımcı olur. Bu SSID, WDS bağlantısı için ayarladığınız ayrı bir SSID'dir. Bu iki SSID aynı değere ve ada sahip değildir (ve olmamalıdır).</p>

Tablo 20.1 Hedef Erişim Noktası Ayarları (Devamı)

Alan	Açıklama
<i>Encryption (Şifreleme)</i>	<p>WDS bağlantısında güvenlik sorunlarından endişe etmiyorsanız herhangi bir şifreleme türü ayarlayabilirsiniz. Güvenlikle ilgili endişeleriniz varsa Statik WEP ya da WPA (PSK)'dan birini seçebilirsiniz.</p> <p>Not: Burada kullanabileceğiniz şifreleme türleri <i>Security (Güvenlik)</i> sayfasında belirlediğiniz ayarlara bağlıdır. WPA (PSK) seçeneği yalnızca <i>Security (Güvenlik)</i> sekmeli sayfada modu WPA Personal (WPA Kişisel) ya da WPA Enterprise (WPA Kurumsal) olarak ayarladığınız zaman WDS sayfasında kullanılabilir bir seçenek olarak görüntülenir.</p> <p>None (Plain Text) (Yok [Düz metin]): Şifrelemeyi None (Yok) olarak ayarladığınızda WDS köprüsündeki AP'ler arasında gönderilen veri şifrelenmez; düz metin olarak gönderilir.</p> <p>WEP: Kablolü Eş Değer Gizlilik (WEP) şifrelemenin WDS bağlantısında etkinleştirilmesini isteyip istemediğinizi belirtin. Kablolü Eş Değer Gizlilik (WEP), 802.11 kablosuz ağlar için bir veri şifreleme protokolüdür. WDS bağlantısındaki erişim noktalarının ikisi de aynı güvenlik ayarıyla yapılandırılmalıdır. Statik WEP'te veri şifreleme için statik 64 bit (40 bit gizli anahtar + 24 bit başlatma vektörü [IV]) ya da 128 bit (104 bit gizli anahtar + 24 bit IV) Paylaşılan Anahtar olarak belirtilir. WEP güvenliği hakkında daha fazla bilgi için bkz. "Statik WEP", sayfa 103.</p> <p>WPA (PSK): WPA (PSK) şifrelemenin WDS bağlantısında etkinleştirilmesini isteyip istemediğinizi belirtin. Wi-Fi Korumalı Erişim Önceden Paylaşılan Anahtar, WPA (PSK) WEP'ten daha güvenli bir şifreleme biçimidir. WPA (PSK) şifrelemeyi kullanırken ağınızdaki her AP'nin aynı benzersiz anahtarla ayarlanmalıdır, aksi halde birbirleriyle iletişim kuramazlar.</p> <p>WPA (PSK) seçeneği yalnızca <i>Security (Güvenlik)</i> sekmeli sayfada modu WPA Personal (WPA Kişisel) ya da WPA Enterprise (WPA Kurumsal) olarak ayarladığınız zaman WDS sayfasında kullanılabilir bir seçenek olarak görüntülenir. Güvenlik hakkında daha fazla bilgi için bkz. "Kablosuz Ağlardaki Güvenlik Sorunlarını Anlama", sayfa 93.</p> <p>WPA (PSK) güvenliği hakkında daha fazla bilgi için bkz. "WPA Kişisel", sayfa 111.</p>

20.3.1 WDS Bağlantısı Yapılandırma Örneği

WDS'yi kullanırken WDS bağlantısındaki her iki erişim noktasında da WDS ayarlarını yapılandırdığınızdan emin olun. Örneğin "MyAP1" ve "MyAP2" adlı iki erişim noktası arasında bir WDS bağlantısı oluşturmak için aşağıdakileri yapın:

1. MyAP1'in IP adresini Web tarayıcının adres çubuğuna URL şeklinde aşağıdaki gibi yazarak MyAP1'in Yönetim Web sayfasını açın:

<http://ErişimNoktasınınIPAdresi>

ErişimNoktasınınIPAdresi, MyAP1'in adresidir.

2. MyAP1 Yönetim Web sayfasında *WDS* sekmesine gidin.

MyAP1'nin (şu an görüntülediğiniz erişim noktasının) MAC adresi, sayfanın üst kısmında "Local Address" (Yerel Adres) şeklinde görüntülenir.

3. MyAP2 ile veri alışverişi yapmak için bir WDS arabirimi yapılandırın.

MyAP2'nin MAC adresini "Remote Address" (Uzak Adres) olarak yazın ve ağı (konuk ya da dahili), güvenliği vb. özellikleri belirtmek için geri kalan alanları doldurun. Ayarları kaydedin (**Update** [Güncelle] düğmesine basın).

4. Modu ve MyAP1'in yayın yapmasını istediğiniz telsiz kanalını ayarlamak ya da doğrulamak için Yönetim Web sayfalarındaki telsiz ayarlarına (*Manage > 802.11 Advanced Settings* [Yönet > 802.11 Gelişmiş Ayarlar]) gidin.

Bağlantıda yer alan MyAP1 ve MyAP2 erişim noktalarının aynı moda ayarlanması ve aynı kanalda aktarım yapması gerektiğini unutmayın.

Bu örnekte, IEEE 802.11b Modunu kullandığımızı ve Kanal 6'da yayın yaptığımızı varsayalım. (Modu ve Kanalı, Radio (Telsiz) sekmesindeki açılır menüden seçtik.)

5. Şimdi aynı adımları MyAP2 için tekrarlayalım:

- MyAP2'nin IP adresini bir URL'de kullanarak MyAP2'nin Yönetim Web sayfalarını açın.
- MyAP2 Yönetim Web sayfasında *WDS* sekmesine gidin. (MyAP2'nin MAC adresi "Local Address" [Yerel Adres] olarak görüntülenecektir).
- MyAP1'in MAC adresinden başlayarak MyAP1 ile veri alışverişi yapmak üzere bir WDS arabirimi yapılandırın.
- MyAP2'nin telsiz ayarlarına giderek MyAP1 ile aynı modda olduğunu ve aynı kanalda yayın yaptığını doğrulayın. (Bu örnekte, Mod 802.11b ve Kanal 6'dır.)
- **Update** (Güncelle) düğmesine tıklayarak ayarları kaydettiğinizden emin olun.

20.4 Ayarları Güncelleme

WDS ayarlarını güncellemek için:

1. *WDS* sekmesine gidin.
2. WDS ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

21.1 SNMP Ayarlarını Anlama.	213
21.2 SNMP Ayarlarına Gitme	214
21.3 SNMP Ayarlarını Yapılandırma.	215
21.3.1 SNMP Tuzaklarını Yapılandırma	217
21.3.2 SNMP Ayarlarını Güncelleme	218

Aşağıdaki bölümler 9160 G2 Kablosuz Ağ Geçidi Kurumsal-Yönetici API'da SNMP ve ilgili ayarların nasıl yapılandırılacağını açıklar:

21.1 SNMP Ayarlarını Anlama

Basit Ağ Yönetimi Protokolü (SNMP) ağ araçlarıyla ilgili bilgileri kaydetme, saklama ve paylaşmayla ilgili bir standart tanımlar. SNMP ağ yönetimini, sorun gidermeyi ve bakımı kolaylaştırır.

SNMP ile yönetilen bir ağın temel bileşenleri şunlardır: yönetilen cihazlar, SNMP araçları ve bir yönetim sistemi. Araçlar Yönetim Bilgi Tabanlarında (MIB'ler) cihazlarıyla ilgili bilgileri saklar ve istendiğinde bu bilgileri SNMP yöneticisine verir. Yönetilen cihazlar; erişim noktası baz istasyonları, yönlendiriciler, anahtarlar, köprüler, hub'lar, sunucular ve yazıcılar gibi ağ düğümleri olabilir.

9160 G2 Kablosuz Ağ Geçidi; HP OpenView ya da Devicescape Wireless Operations Center gibi ağ yönetim sistemlerine sorunsuzca entegre olmak için SNMP tarafından yönetilen bir cihaz olarak işlev görebilir.

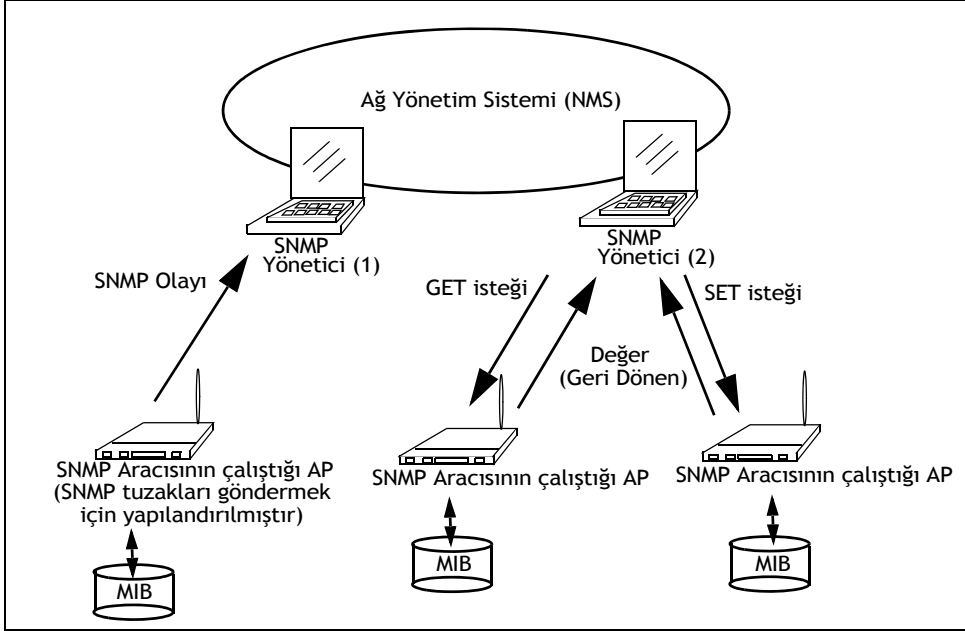
MIB'ler, bir ağdaki sanal veritabanında bulunan nesne veya dosya koleksiyonlarıdır. SNMP, MIB'den bilgi almak için belirli komut ve sorgular kullanır.

9160 G2 Kablosuz Ağ Geçidi şu standart SNMP MIB'leri destekler:

- Köprü MIB 802.1d (RFC 1493).
- SNMPv2 MIB (RFC 3418).
- IEEE Std 802.11 MIB (taban).
- Arabirim Grubu MIB (RFC 2233).
- Yeni IEEE 802.11k MIB'ye dayanan iki özel MIB (Kablosuz MIB ve Sistem MIB'si). Bu MIB'ler sırasıyla 9160 G2 Kablosuz Ağ Geçidi istemci ilişkisi listesi ve AP algılama tablosuyla ilgili bilgi sağlar. Özel Sistem MIB'si sistemi yeniden başlatma ve ürün yazılımı yükseltme gibi bakım işlevleri sağlar.

9160 G2 Kablosuz Ağ Geçidi SNMP tuzaklarını da destekler. Şekil 21.1, SNMP'nin ağda nasıl çalıştığını açıklar.

Şekil 21.1 Ağda Çalışan SNMP



21.2 SNMP Ayarlarına Götme

SNMP ayarlarını yapılandırmak için *Services > SNMP* (Hizmetler > SNMP) sekmesine gidin ve alanları aşağıda anlatıldığı gibi güncelleyin.

Şekil 21.2 SNMP Ayarlarına Genel Bakış

Basic Settings	Modify SNMP Settings	
User Management		
Cluster	SNMP <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Access Points	Read-only community name (for permitted GETs) <input type="text" value="public"/>	
Sessions	Port number the SNMP agent will listen to <input type="text" value="161"/>	
Channel Management	Allow SNMP SET requests <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Wireless Neighborhood	Read-write community name (for permitted SETs) <input type="text" value="protected"/>	
Security	Restrict the source of SNMP requests to only the designated hosts or subnets <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Status	Hostname or subnet of Network Management System <input type="text" value="Değer (Geri Dönen)"/>	
Interfaces	Trap Destinations	
Events	Community name for traps <input type="text" value="trapcommunity"/>	
Transmit/Receive	Enabled <input checked="" type="checkbox"/> Hostname <input type="text" value="one.traphost.com"/>	
Client Associations	<input checked="" type="checkbox"/> <input type="text" value="two.traphost.com"/>	
Neighboring Access Points	<input type="checkbox"/> <input type="text"/>	
Manage	<input type="button" value="Update"/>	
Ethernet Settings		
802.11 Settings		
802.11 Advanced Settings		
VWN		
WDS		
Guest Login		
MAC Filtering		
Load Balancing		
Services		
QoS		
Time		
SNMP		

21.3 SNMP Ayarlarını Yapılandırma

SNMP araçlarının başlama/durma denetimi, ortak şifre yapılandırması, MIB'lere erişim ve SNMP tuzağı yerlerinin yapılandırılması aşağıda açıklandığı şekilde 9160 G2 Kablosuz Ağ Geçidi aracılığıyla sağlanmaktadır.

Tablo 21.1 SNMP Ayarları

Alan	Açıklama
<i>SNMP Enabled/Disabled (SNMP Etkin/Devre Dışı)</i>	<p>SNMP'yi ağıınızda etkinleştirmeyi ya da devre dışı bırakmayı seçebilirsiniz. SNMP, varsayılan olarak devre dışıdır.</p> <ul style="list-style-type: none">• SNMP'yi etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.• SNMP'yi devre dışı bırakmak için Disabled (Devre Dışı) seçeneğine tıklayın. <p>Not: SNMP'yi etkinleştirmedeniz SNMP sayfasındaki diğer tüm alanlar devre dışı kalır.</p>
<i>Read-only community name for permitted GETs (İzin verilen GET'ler için salt okunur ortak ad)</i>	<p>Salt okunur bir ortak ad girin.</p> <p>SNMPv2c'de tanımlandığı gibi ortak ad, ağda veri isteğinde bulunacak makineleri yalnızca SNMP araçları olacak şekilde kısıtlamak için kullanılan basit bir kimlik doğrulama mekanizması işlevi görür. Ad, şifre işlevi görür ve gönderen şifreyi biliyorsa isteğin gerçek olduğu varsayılır.</p> <p>Ortak ad herhangi bir alfanümerik formatta olabilir.</p>
<i>Port number the SNMP agent will listen to (SNMP aracısının dinleyeceği port numarası)</i>	<p>SNMP araçları varsayılan olarak yalnızca bağlantı noktası 161'den gelen istekleri dinler. Ancak, aracının başka bir bağlantı noktasını dinlemesi için bu ayarı yapılandırabilirsiniz.</p> <p>SNMP araçlarının istekler için dinlemesini istediğiniz bağlantı noktasının numarasını girin.</p>
<i>Allow SNMP SET Requests (SNMP SET İsteklerine İzin Ver)</i>	<p>SNMP SET isteklerine izin verip vermemeyi seçebilirsiniz.</p> <p>SET isteklerini etkinleştirmek, ağdaki makinelerin AP'deki yapılandırılmış aracıya SET istekleri gönderebilmesi anlamına gelir.</p> <p>Not: SET istekleri özel Sistem MIB'siyle sınırlıdır.</p> <ul style="list-style-type: none">• SNMP SET isteklerini etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın.• SNMP SET isteklerini devre dışı bırakmak için Disabled (Devre Dışı) seçeneğine tıklayın.
<i>Read-write community name for permitted SETs (İzin verilen GET'ler için okuma-yazma özellikli ortak ad)</i>	<p>SNMP SET isteklerini etkinleştirdiyseiz okuma-yazma özellikli bir ortak ad ayarlayabilirsiniz.</p> <p>Ortak ad ayarlamak şifre ayarlamaya benzer. Yalnızca kendilerini bu ortak adla tanımlayan makinelerden gelen istekler kabul edilecektir.</p> <p>Ortak ad herhangi bir alfanümerik formatta olabilir.</p>

Tablo 21.1 SNMP Ayarları (Devamı)

Alan	Açıklama
<i>Restrict the source of SNMP requests to only the designated hosts or subnets (SNMP isteği kaynağını yalnızca belirlenen ana bilgisayar ve alt ağlar olacak şekilde sınırla)</i>	<p>İzin verilen SNMP isteklerinin kaynaklarını sınırlayabilirsiniz.</p> <ul style="list-style-type: none">İzin verilen SNMP isteklerinin kaynaklarını sınırlamak için Enabled (Etkin) seçeneğine tıklayın.SNMP isteği gönderen her kaynağa izin vermek için Disabled (Devre Dışı) seçeneğine tıklayın.
<i>Hostname or subnet of Network Management System (Ağ Yönetim Sisteminin Ana Bilgisayar Adı ya da Alt Ağı)</i>	<p>Yönetilen cihazlara GET ve SET istekleri gönderebilen makinelerin DNS ana bilgisayar adını ve alt ağını belirtin.</p> <p>Bu özellik, ortak adla birlikte SNMP ayarlarında bir güvenlik seviyesi sağlar. SNMP aracı yalnızca burada belirtilen ana bilgisayar adından ya da alt ağdan gelen istekleri kabul eder.</p> <p>Bir alt ağ belirlemek için <i>AddressRange/MaskLength</i> (AdresAralığıMaskeUzunluğu) formatında bir veya daha fazla alt ağ adres aralığı girin (<i>AddressRange</i> [AdresAralığı], bir IP adresidir, <i>MaskLength</i> [MaskeUzunluğu] ise maske bitlerinin sayısını ifade eder). "NetAddress/NetMask"(NetAdresi/NetMaskesi) ve "NetAddress/MaskLength" (NetAdresi/MaskeUzunluğu) formatlarının ikisi de desteklenir. IP Adresi ya da Ana Bilgisayar Adı için bağımsız ana bilgisayarlar sağlanabilir. Örneğin; 192.168.1.0/24 aralığını girdiğinizde bu aralık, 192.168.1.0 adresli bir alt ağ ve 255.255.255.0 uzunluğunda bir alt ağ maskesi belirlir.</p> <p>Adres aralığı, belirtilen NMS'in alt ağını belirlemek için kullanılır. Yalnızca bu aralıktaki IP adresine sahip makineler, yönetilen cihazda GET ve SET istekleri yürütebilir. Yukarıdaki örneğe göre, adresleri 192.168.1.1 ile 192.168.1.254 arasında olan makineler, cihazda SNMP komutları yürütebilir. (Bir alt ağ aralığında .0 son ekiyle belirtilen adres, her zaman alt ağ adresi için, .255 ile belirtilen adres de her zaman yayın adresi için ayrılır).</p> <p>Başka bir örnek: 10.10.1.128/25 aralığını girdiğinizde IP adresi 10.10.1.129 ile 10.10.1.254 arasında olan makineler, yönetilen cihazlarda SNMP istekleri yürütebilir. Bu örnekte, 10.10.1.128, ağ adresi; 10.10.1.255 ise yayın adresidir. 126 adres belirlenebilir.</p>

21.3.1 SNMP Tuzaklarını Yapılandırma

SNMP Tuzakları, SNMP yönetilen cihazlarından (9160 G2 Kablosuz Ağ Geçidi gibi) belirli ana bilgisayarlara giden mesajların asenkron iletişimini sağlar. Bir Ağ Yönetim Sistemi (NMS), bir ağda yer alan çok sayıda cihazdan sorumluyorsa ağdaki her cihazın periyodik olarak sorgulanması pratik bir yöntem değildir. AP'de SNMP olay tuzakları etkinleştirildiğinde her bir cihaz, SNMP Yöneticilerine ya da NMS'teki diğer belirli ana bilgisayarlara ağ arabirimlerinin artması/azalması, istemcilerin erişim noktasıyla ilişkilenebilir ya da kimlik doğrulamayla ilgili başarısız denemeleri, sistem gücünün artması/azalması ve ağ tipolojisindeki değişiklikler gibi bazı ağ olaylarıyla ilgili doğrudan mesaj gönderebilir.

SNMP tuzakları, gereksiz SNMP isteklerini ortadan kaldırarak ağ kaynaklarında tasarruf sağlar. Ayrıca SNMP Yöneticilerinin ağlarında sorun giderme işlemlerini daha kolay yapmasına yardımcı olur. Örneğin, bir SNMP yöneticisi pek çok cihazı destekleyen ve her bir cihazın çok sayıda nesnesinin olduğu büyük bir ağdan sorumluysa tüm cihazlardaki her bir nesneden bilgi istemek pratik bir yöntem değildir. Yönetilen cihazdaki her aracı için en iyi çözüm, yöneticiyi olağan dışı olaylar konusunda bilgilendirmektir. Bilgilendirme işlemi, olayla ilgili bir tuzak gönderilerek yapılır. Yönetici, olayla ilgili bilgi aldıktan sonra aksiyon alıp almamaya ve hangi aksiyonları alacağına karar verebilir.

Tablo 21.2 SNMP Tuzak Ayarları

Alan	Açıklama
<i>Community name for traps</i> (Tuzaklar için ortak ad)	SNMP tuzaklarıyla ilişkili global ortak dizeyi girin. Cihazdan gönderilen tuzaklar ortak ad olarak bu dizeyi sağlar.
<i>Hostname</i> (Ana Bilgisayar Adı)	SNMP tuzakları göndermek istediğiniz bilgisayarın DNS ana bilgisayar adını girin. DNS ana bilgisayar adına örnek: snmptraps.teklogix.com SNMP tuzakları SNMP aracısından rastgele gönderildiğinden tuzakların tam olarak nereye gönderileceğinin belirlenmesi yerinde olur. Uygun ana bilgisayar adının yanındaki Enabled (Etkin) onay kutusunu seçtiğinizden emin olun.

21.3.2 SNMP Ayarlarını Güncelleme

SNMP ayarlarını güncellemek için:

1. *SNMP* sekmesine gidin.
2. SNMP ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

9160 G2'NİN BAZ İSTASYONU OLARAK KULLANILMASI

22

22.1 Genel Bakış	221
22.2 Telsiz Protokolleri	222
22.2.1 Ayarlanabilir Sorgulama/Çatışma Protokolü	222
22.3 Dar Bant Menüleri	222
22.3.1 Dar Bant Telsiz Yapılandırma Ayarları	222
22.3.1.1 RA1001A Telsiz Parametreleri	224
22.3.2 Bağlantı Seçenekleri	225
22.3.3 Bağlantı Seçenekleri: Baz İstasyonu Modu.	225
22.3.3.1 Sorgulama Protokolü Parametreleri	227
22.3.3.2 Telsiz Parametreleri	229
22.3.4 Bağlantı Seçenekleri: RRM Modu	231
22.4 Bağlantı Menüleri	231
22.4.1 Baz İstasyonu Yapılandırma Ayarları	233
22.4.2 RRM Grupları Yapılandırma Ayarları	234
22.4.2.1 RRM Grupları	236
22.4.2.2 Sorgulama Protokolü Parametreleri	237
22.4.2.3 Telsiz Parametreleri	239
22.4.2.4 Grup Parametreleri	240
22.4.2.5 Uzak Telsiz Modülleri	241
22.4.3 Telsiz Bağlantısı Özellikleri Yapılandırma Ayarları	241
22.4.3.1 Telsiz Bağlantısı Özellikleri	243
22.4.3.2 Otomatik Telsiz Adresleri	244
22.4.3.3 Otomatik Terminal Numarası	245
22.4.4 Ana Bilgisayarlar Menüsü	246
22.4.4.1 9010 Yapılandırma.	249

22.1 Genel Bakış

9160 G2 Kablosuz Ağ Geçidi, mobil bilgisayarlarla iletişimi sağlamak için bir telsiz bağlantısı ve Psion Teklogix özel protokollerini kullanarak kablolu veya kablosuz bir Baz İstasyonu ya da Uzak Telsiz Modülü (RRM) olarak kullanılabilir (bkz. "Telsiz Protokolleri", sayfa 222).

9160 G2, kablolu bir baz istasyonu olarak kullanıldığında Ayarlanabilir Sorgulama/Çatışma Protokolünü (sayfa 222) kullanarak kablosuz mobil bilgisayarlarla iletişim kurabilir ve ağ denetleyicisine bir ağ üzerinden bağlanır.

9160 G2, kablosuz bir baz istasyonu olarak kullanıldığında 802.11 WDS'yi kullanarak kablosuz baz istasyonu ve mobil bilgisayarlarla iletişim kurabilir.

RRM olarak kullanıldığında ise, 9160 G2'nin mobil bilgisayarlarla olan telsiz bağlantısının çalışması ve zamanlaması, doğrudan zaman çoklama telsiz protokolü kullanan bir ağ denetleyicisi tarafından kontrol edilir (aşağıdaki "Zaman Çoklama ve Hücrel Geçiş" bölümüne bakın). Ağ denetleyicisine bir ağ üzerinden bağlanır.

Zaman Çoklama ve Hücrel Geçiş

Telsiz bağlantısıyla çalışmanın iki yöntemi vardır. İlk yöntem *hücrel geçiş* tir. Kavram olarak cep telefonu sistemleriyle benzerlik gösterir. Burada, her bir baz istasyonu farklı bir telsiz kanalı kullanır. Mobil bilgisayarlar telsiz bağlantısını izler ve otomatik olarak en iyi telsiz sinyali alan kanala geçer. Ana bilgisayar, bu hücrel geçiş özelliğini göremez.

İkinci yöntem *zaman çoklamadır*. Burada, sitedeki tüm Uzak Telsiz Modülü (RRM) baz istasyonları aynı kanalı kullanır. Ağ denetleyicisi, bir UDP/IP ağı üzerinden sorgulama sekanslarını koordine ederek RRM'lerin aynı anda veri aktarımı yapmamasını sağlar. Ana bilgisayar, bu zaman çoklama özelliğini de göremez. Zaman çoklama, işlem hızı düşük olan siteler için uygundur.

Hücrel geçiş ve zaman çoklama, tek bir Psion Teklogix sisteminde birleştirilebilir: Bir site, her bir kanalı ve kanallar arasında hücrel geçişi kullanan pek çok gruplanmış zaman çoklamalı baz istasyonu ile birlikte iki ya da daha fazla kanalda çalışabilir.

Operatör, bu durumların hepsinde herhangi bir iletişim kaybı olmadan tüm sitede rahatlıkla gezinebilir. Psion Teklogix sistemi, baz istasyonları arasındaki kanal değişimini ve geçişleri kullanıcıyı uyarmadan gerçekleştirir.

Baz istasyonu ya da RRM olarak çalışırken *Configuration Main Menu* (Yapılandırma Ana Sayfası) ekranındaki *Base Station Configuration* (Baz İstasyonu Yapılandırması) sayfalarında yer alan parametreler, ileriki bölümlerde açıklandığı gibi uygun şekilde ayarlanmalıdır.

Ayrıca, uygun telsiz ve ana bilgisayar parametreleri de uygulanmalıdır. Telsiz parametreleri Bölüm 22.3.1'de açıklandığı gibi *Dar Bant* telsizlerin *Radio* (Telsiz) sayfalarında yer alır. Ana bilgisayar parametreleri "Kısım 22.4.4 Ana Bilgisayarlar Menüsü", sayfa 246'da açıklanmıştır.



Not: 9160 G2 ana parametreleri, ilk önce Bölüm 4: “Kurulum ve Başlatma İçin Hızlı Adımlar” ve Bölüm 5: “Temel Ayarları Yapılandırma” bölümlerinde açıklandığı gibi ayarlanmalıdır. RF protokolleriyle ilgili ayrıntılı bilgi için aşağıdaki bölümlere bakın.

22.2 Telsiz Protokolleri

RF protokolleri, bir telsiz kanalının kullanımını etkili biçimde paylaşarak mobil bilgisayarların baz istasyonlarıyla iletişim kurmasına olanak sağlar. Psion Teklogix sistemleri, iki RF protokolünden birini kullanır: Psion Teklogix Ayarlanabilir Sorgulama/Çatışma Protokolü ya da tescilsiz IEEE 802.11 protokolü.

9160 G2, baz istasyonu ya da RRM olarak kullanılırken Ayarlanabilir Sorgulama/Çatışma protokolünü kullanır. 9160 G2, baz istasyonu ve 802.11 erişim noktalarının eş zamanlı çalışmasını destekler.

22.2.1 Ayarlanabilir Sorgulama/Çatışma Protokolü

Ayarlanabilir Sorgulama/Çatışma protokolü, her zaman 19,2 kb/sn kadar baud hızına sahip Dar Bant telsiz sistemlerinde kullanılır ve daha yüksek hızlarda Geniş Spektrum sistemlerinde de kullanılabilir.

Bu protokolle çalışan mobil bilgisayarlar, 9160 G2'den sorgu almıyorlarsa veri aktarımı yapmazlar. Mobil bilgisayarlar genellikle toplu olarak sorgulanırlar. Her sorgunun ardından mobil bilgisayar grupları, sorguları yanıtlayabilecekleri yanıt pencerelerine atanırlar. Herhangi bir "çarşıma" meydana gelirse (birden fazla mobil bilgisayar bir pencerede yanıt göndermeye çalışırsa) sorgulamayı yapan 9160 G2 bölünür ve çarşıyan mobil bilgisayarlar çarşıma olmadan yanıt gönderene kadar grubu yeniden atar.

Bu protokolün ayarlanabilir özellikleri, yanıt penceresinin yüksek veya düşük RF trafik durumlarına olanak sağlayacak ve belirli bir mobil bilgisayarın göndereceği ya da alacağı çok fazla verisi olduğunda verilerin uzun süre kuyrukta bekletilmesini önleyecek şekilde ayarlanmasına olanak sağlar.

Ayarlanabilir sorgulama/çatışmayı kullanan sistemler, hücrel seçeneğini kullanarak mobil bilgisayar operatörlerinin kapsama alanlarından geçerken kesintisiz bir iletişim sunarak sitenin içinde gezinebilmesini sağlar.

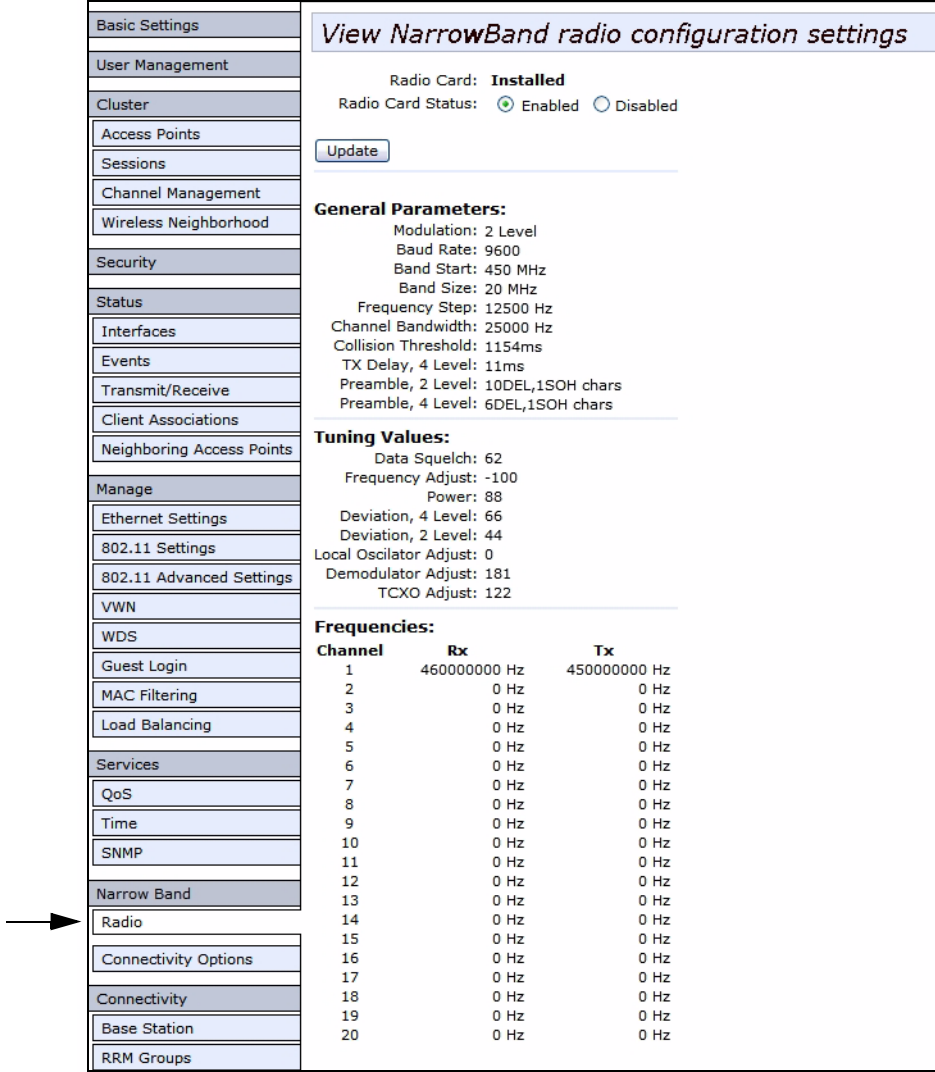
Hücrel baz istasyonu etkin değilse operatörün bir baz istasyonu kapsama alanından diğerine her geçişinde, mobil bilgisayarın ekranında "RESET: Press Enter" (SIFIRLA: ENTER tuşuna basın) mesajı görüntülenir.

22.3 Dar Bant Menüleri

22.3.1 Dar Bant Telsiz Yapılandırma Ayarları

Narrow Band (Dar Bant) menü seçeneklerinden *Radio* (Telsiz) alt menüsünü seçtiğinizde 9160 G2, ayarlanmış olduğu çalışma modunun (baz istasyonu ya da RRM) *Dar Bant Telsiz Yapılandırma Ayarlarını* görüntüler. Görüntülenen sayfa 9160 G2'nin durumunu ayarlamaya ve RA1001A telsiz kartının kalıcı iletişim ayarlarını almanıza olanak sağlar.

Şekil 22.1 Dar Bant Telsiz Ayarlarına Genel Bakış



View NarrowBand radio configuration settings

Radio Card: **Installed**
Radio Card Status: ☒ Enabled ☐ Disabled
[Update](#)

General Parameters:
Modulation: 2 Level
Baud Rate: 9600
Band Start: 450 MHz
Band Size: 20 MHz
Frequency Step: 12500 Hz
Channel Bandwidth: 25000 Hz
Collision Threshold: 1154ms
TX Delay, 4 Level: 11ms
Preamble, 2 Level: 10DEL,1SOH chars
Preamble, 4 Level: 6DEL,1SOH chars

Tuning Values:
Data Squelch: 62
Frequency Adjust: -100
Power: 88
Deviation, 4 Level: 66
Deviation, 2 Level: 44
Local Oscillator Adjust: 0
Demodulator Adjust: 181
TCXO Adjust: 122

Frequencies:

Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

Radio Card Status (Telsiz Kartı Durumu)

Bu parametre, Dar Bant Telsizi **etkinleştirir** ya da **devre dışı bırakır**. Bu kart, test amaçlı olarak hiçbir telsiz parazitinin olmaması gerektiğinde geçici olarak **devre dışı bırakılabilir**. Bu değişikliği uygulamak için **Update** (Güncelle) düğmesine basın.

22.3.1.1 RA1001A Telsiz Parametreleri

Narrow Band Radio Configuration Settings (Dar Bant Telsiz Ayarları) sayfası, RA1001A Dar Bant telsiz için *General* (Genel), *Frequencies* (Frekanslar) ve *Tuning Values* (Ayarlama Değerleri) parametrelerini görüntüler. Bu üretici ayarları yapılandırılmaz. Ayarlar, aşağıdaki şekillerde gösterilmiştir.

Şekil 22.2 RA1001A Telsiz Parametreleri

General Parameters:
Modulation: 2 Level
Baud Rate: 9600
Band Start: 450 MHz
Band Size: 20 MHz
Frequency Step: 12500 Hz
Channel Bandwidth: 25000 Hz
Collision Threshold: 1154ms
TX Delay, 4 Level: 11ms
Preamble, 2 Level: 10DEL,1SOH chars
Preamble, 4 Level: 6DEL,1SOH chars

Şekil 22.3 RA1001A Telsiz Ayarlama Değerleri

Tuning Values:
Data Squelch: 62
Frequency Adjust: -100
Power: 88
Deviation, 4 Level: 66
Deviation, 2 Level: 44
Local Oscillator Adjust: 0
Demodulator Adjust: 181
TCXO Adjust: 122

Şekil 22.4 RA1001A Telsiz Frekansları

Frequencies:		
Channel	Rx	Tx
1	460000000 Hz	450000000 Hz
2	0 Hz	0 Hz
3	0 Hz	0 Hz
4	0 Hz	0 Hz
5	0 Hz	0 Hz
6	0 Hz	0 Hz
7	0 Hz	0 Hz
8	0 Hz	0 Hz
9	0 Hz	0 Hz
10	0 Hz	0 Hz
11	0 Hz	0 Hz
12	0 Hz	0 Hz
13	0 Hz	0 Hz
14	0 Hz	0 Hz
15	0 Hz	0 Hz
16	0 Hz	0 Hz
17	0 Hz	0 Hz
18	0 Hz	0 Hz
19	0 Hz	0 Hz
20	0 Hz	0 Hz

22.3.2 Bağlantı Seçenekleri

Bu alt menüyü seçtiğinizde görüntülenen sayfa, baz istasyonu ya da RRM modu için 9160 G2'nin çalıştırma seçeneklerini ayarlamanızı sağlar.

22.3.3 Bağlantı Seçenekleri: Baz İstasyonu Modu

Baz istasyonu çalışma moduna ayarlanan 9160 G2'nin *Connectivity Options* (Bağlantı Seçenekleri) alt menüsüne girdiğinizde Sorgulama Protokolü ve Telsiz Parametreleri görüntülenir.

Şekil 22.5 Sorgulama Protokolü ve Telsiz Parametrelerine Genel Bakış

Set Operating Mode and view Polling Protocol or RRM settings	
Basic Settings	
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	

Operating Mode:	Base Station Base Station RRM
Auto-Startup:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Shared Channel:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Polling Protocol Parameters:	
Number of Poll Windows:	3 (Range 2..4)
Size of Poll Windows:	8 (Range 5..32)
Maximum Message Segment Size:	100 (Range 32..116)
Number of Retries:	3 (Range 1..7)
Collision Size:	6 (Range 3..10)
Free Window Factor:	0 (Range 0..7)
Message Mode Limit:	4 (Range 0..7)
Callsign Period:	0 (Range 0..60)
Callsign String:	Teklogix (Max 10 letters or digits)
Radio Parameters:	
Sync Delay:	22 (Range 3..45)
Remote Tx On:	13 (Range 3..60)
Active Channel:	1 (Range 1..20)
<input type="button" value="Update"/>	

Operating Mode (Çalışma Modu)

Bu parametre, 9160 G2'nin çalışma modunu **Base Station** (Baz İstasyonu) ya da **RRM** olarak ayarlamanızı sağlar.

Auto-Startup (Otomatik Başlama)

Bu parametre, 9160 G2 yeniden başlatıldığında sorgulamayı hemen **etkinleştirir**. Otomatik **Başlama devre dışı bırakıldığında** 9160 G2, sorgulama işlemi ağ denetleyicisinden başlatılana kadar bekler.

Shared Channel (Paylaşılan Kanal)

Paylaşılan Kanal, devlet tarafından sunulan gereksinimleri sağlamak için yalnızca Hollanda'da kullanılır. **Etkinleştirildiğinde** sorgulama için zamanlama kısıtlamaları getirir. Her 2 saniyelik sorgulamanın ardından 0,5 saniyelik bir sessizlik olur (bu süre içinde sorgulama yapılmaz).

Ayrıca, kanalda başka bir taşıyıcı algılanırsa 9160 G2, veri yolu boşalana kadar telsiz aktarımını durdurur.

22.3.3.1 Sorgulama Protokolü Parametreleri

Polling Protocol Parameters:		
Number of Poll Windows:	<input type="text" value="3"/>	(Range 2..4)
Size of Poll Windows:	<input type="text" value="8"/>	(Range 5..32)
Maximum Message Segment Size:	<input type="text" value="100"/>	(Range 32..116)
Number of Retries:	<input type="text" value="3"/>	(Range 1..7)
Collision Size:	<input type="text" value="6"/>	(Range 3..10)
Free Window Factor:	<input type="text" value="7"/>	(Range 0..7)
Message Mode Limit:	<input type="text" value="4"/>	(Range 0..7)
Callsign Period:	<input type="text" value="0"/>	(Range 0..60)
Callsign String:	<input type="text" value="Teklogix"/>	(Max 10 letters or digits)

Number of Poll Windows (Sorgulama Pencerelerinin Sayısı)

Bu parametre, 9160 G2'nin kullanacağı sorgulama penceresi sayısını tanımlar. Bu parametreye atanan değer, kullanılan mobil bilgisayar ve telsiz bağlantı protokolü sayısına bağlıdır. Tablo 22.1, *Sorgulama Penceresi Sayısı* parametresine atanan değer nasıl belirlendiğini gösterir.

Tablo 22.1 Sorgulama Pencerelerinin Sayısı - Hücresel Protokol

Mobil Bilgisayar Sayısı	Minimum Pencere Sayısı
1-16	2
17-81	3
82-256	4

Size of Poll Windows (Sorgulama Pencerelerinin Boyutu)

Bu parametreye atanan değer, normal bir sorgulama penceresinde 9160 G2 ile mobil bilgisayarın birbirlerine gönderebilecekleri en büyük mesajı belirler. Pencerenin boyutu **5 - 32** karakter uzunluğundaki mesajları gösterecek şekilde her yerinden ayarlanabilir.

Büyük pencereler sorgulama süresini artırır ve yanıt süresini de artırabilir. Küçük pencereler mesaj sayısını ve uzun mesaj sorgulamalarını artırır, ayrıca yanıt süresini de artırabilir.



Önemli: *"Hücresel" modunda bu parametrenin minimum değeri 8'dir.*

Maximum Message Segment Size (Maksimum Mesaj Bölümü Boyutu)

Bu parametre, mesaj modundayken *mobil bilgisayara* ya da uzun mesaj modundayken *mobil bilgisayardan* gönderilebilecek en büyük mesajı belirler. 9160 G2 baz istasyonunda bu parametre için girilen değer, ağ yöneticisi ya da 9160 G2 mini denetleyicide girilen değere eşit veya o değerden büyük olmalıdır. Bu parametre için izin verilen aralık 32-116 karakterdir. (Uzun mesajlar birkaç paket halinde gönderilir). Varsayılan değer **100**'dür.

Number of Retries (Yeniden Deneme Sayısı)

Bu parametre, mobil bilgisayardan herhangi bir bilgilendirme alınmadığında 9160 G2'nin bir mesajı kaç kez yeniden göndermeyi deneyeceğini belirler. (Eksik mesajlar mesaj kuyruğunun sonuna döndüğünden bu yeniden denemelerin art arda sorgulamalarla gerçekleşmesi gerekmez.) Tüm yeniden denemeler gerçekleştikten sonra mobil bilgisayarın "çevrimdışı" olduğu bildirilir. 9160 G2, mobil bilgisayar "çevrimiçi" olduğunu bildirene kadar mobil bilgisayara herhangi bir mesaj aktarmaz. İzin verilen değer, **1 - 7** arasındır.

Collision Size (Çarpışma Boyutu)

Bu parametre, telsiz bağlantısındaki rastgele bir gürültünün, mobil bilgisayarlar arasında gerçekleşen bir çarpışma olarak yorumlanması ihtimalini azaltır. 9160 G2, çarpışmaları gereksiz yere ortadan kaldırırsa yanıt süresi artar.

Çarpışma Boyutu, bir hata mesajından (CRC, kayıp CD vb.) önce alınan karakter sayısına bir üst sınır getirir. Bu parametre değeri sekizse telsiz bağlantısında görüntülenen bir hata mesajından önceki sekiz ya da daha az karakter, gürültü olarak değerlendirilir. Sekizden fazla karakter varsa çarpışma olarak değerlendirilir. Kabul edilen değer aralığı **3 - 10**'dur.

Free Window Factor (Boş Pencere Faktörü)

Bu parametrede girilen değer, "boş pencere modu"nun kullanılıp kullanılmayacağını belirler. Boş pencere modunda, başka bir pencereye atanmayan tüm mobil bilgisayarlar boş pencereyi kullanabilir.

Bu parametreye **0** (sıfır) değerinin girilmesi, boş pencere modunu **devre dışı** bırakır. Bu parametre değerinin artırılması, mesajın boş pencerede aktarılma ihtimalini artırır.

Message Mode Limit (Mesaj Modu Sınırı)

Bu parametre, mesaj modu sorgulaması başlamadan önce aktarım için kuyruğa alınması gereken mesajların üst limitini tanımlar. Kabul edilen değer aralığı **0 - 7**'dir (0, mesaj modunu **devre dışı bırakır**).



Not: Mobil bilgisayar ve geçmiş olayların sayısı da, mesaj modunu başlatıp başlatmamayı belirleyen algoritmanın bir parçasıdır.

Callsign Period (Çağrı İşareti Süreci)

Çağrı işareti, sesli bir Mors kodu sinyali olarak periyodik biçimde iletilir. Bu parametre, çağrı işareti iletimleri arasındaki zaman aralığını dakika cinsinden belirtir. Kabul edilen değer aralığı **0 - 60**'tır. Federal kuruluşlar, Industry Canada ve ABD Federal İletişim Komisyonu, her sistemin 15 dakikada bir kendi tanımlayıcı çağrı işaretini iletmelerini gerektirir.

Çağrı işaretinin gerekli olmadığı ülkelerde bu parametrenin **0**'a ayarlanması, çağrı işaretlerinin iletilmesini önleyerek mobil bilgisayarlarda daha kısa sorgulama zaman aşımı süresi ve daha hızlı kanal değiştirme olanağı sunar.

Callsign String (Çağrı İşareti Dizesi)

Bu dize maksimum **10** karakter uzunluğunda olabilir. Tüm karakterler sayı ya da harf olmalıdır. "DE" (kimden) ön eki, iletilen çağrı işaretinin başına eklenir.

22.3.3.2 Telsiz Parametreleri

Radio Parameters:	
Sync Delay:	<input type="text" value="18"/> (Range 3..45)
Remote Tx On:	<input type="text" value="4"/> (Range 3..60)
Active Channel:	<input type="text" value="1"/> (Range 1..20)

Sync Delay (Senkronizasyon Bekleme Süresi)



Önemli: *Telsiz protokolü zamanlaması iyice anlaşılmadan bu parametrenin fabrika ayarları değiştirilmemelidir.*

Sync Delay (Senkronizasyon Bekleme Süresi), baz istasyonu aktarımı ile ilk yanıt penceresi arasındaki gecikmeyi karakter süresi cinsinden belirtir. Bu parametreye atanan değer, sistemdeki diğer baz istasyonları ve mobil bilgisayarlarla uyumlu olmalıdır. RA1001A telsizinin iki ya da dört seviyeli modülasyonu vardır ve bu modülasyonlarla sırasıyla 4800 bp/sn ve 9600 bp/sn ya da 9600 bp/sn ve 19.200 bp/sn baud hızı sunar.

İki seviyeli modülasyona sahip, 9600 baud hızında çalışan dar bant bir telsiz için varsayılan ayar **23**'tür.

Dört seviyeli modülasyona sahip, 19.200 baud hızında çalışan dar bant bir telsiz için varsayılan ayar **31**'dir.

Remote Txon (Uzak Txon)

Remote Txon (Uzak Txon), telsizin mobil bilgisayarlarda (uzak) açılma zamanını sağlar. Gerçek veri elde edilene kadar telsize gönderilecek doldurma karakteri sayısını belirtir. Bu parametre karakter sürelerine dayandığından karakter sayısı telsiz bağlantısının baud hızına bağlıdır.

Remote Txon parametresine atanan değer, tüm mobil bilgisayarlar ve baz istasyonu ekipmanlarıyla tutarlı olmalıdır. İzin verilen değer aralığı **3 - 60**'tır.



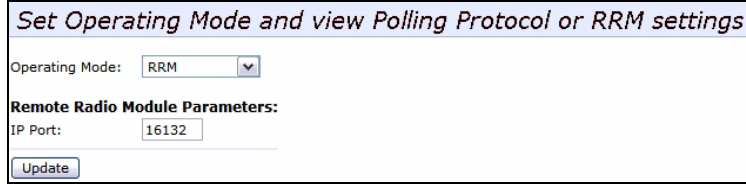
Önemli: *Telsiz protokolü zamanlaması anlaşılmadan bu parametrenin fabrika ayarları değiştirilmemelidir.*

Active Channel (Etkin Kanal)

Bu parametre, 9160 G2'nin çalışan telsiz kanalını belirler. Bu da, kanalın mobil bilgisayarlar tarafından yapılan kanal aramasında görünmesini sağlar. Seçilen kanal, *Narrow Band Radio Configuration Settings* (Dar Bant Telsiz Yapılandırma Ayarları) sayfasında belirtildiği gibi frekanslarla yapılandırılan kanallardan biri olmalıdır. İlişkili kanal ve frekansların listesi için bkz. Şekil 22.4, sayfa 225.

22.3.4 Bağlantı Seçenekleri: RRM Modu

RRM çalışma moduna ayarlanan bağımlı bir 9160 G2'nin *Connectivity Options* (Bağlantı Seçenekleri) alt menüsüne girdiğinizde 9160 G2, RRM parametrelerini görüntüler.



Set Operating Mode and view Polling Protocol or RRM settings

Operating Mode: RRM

Remote Radio Module Parameters:

IP Port: 16132

Update

IP Port (IP Bağlantı Noktası)

Bu parametre, RRM bağımlı birimi olarak çalışan 9160 G2'nin dinleme bağlantı noktası sayısını girmenize olanak sağlar. Bağlantı noktası sayısı **1024 - 32.767** arasında olabilir.



Önemli: *Buraya girilen bağlantı noktası sayısı, ağ denetleyicisinin RRM yapılandırmasında bu 9160 G2 için girilen bağlantı noktası sayısı ile aynı olmalıdır.*

22.4 Bağlantı Menüleri

9160 G2 Kablosuz Ağ Geçidi, çeşitli ana bilgisayar platformları kullanarak mobil bilgisayarlarla kablosuz baz istasyonları arasındaki iletişimden ve bir ağ denetleyicisinden (Psion Teklogix 9500 İletişim Sunucusu ya da 9160 G2 Kablosuz Ağ Geçidi) faydalanan bir baz istasyonu ya da uzak telsiz modülü (RRM) olarak çalışabilir. Alternatif olarak ağ denetleyici, Psion Teklogix SDK (işleyici) kullanan bir ana bilgisayar olabilir.

Ayrıca 9160 G2, ağdaki başka bir 9160 G2'nin bağımlı baz istasyonu olarak da kullanılabilir.

Şekil 22.6 Baz İstasyonu Yapılandırması

Basic Settings	View Base Station configuration settings
User Management	
Cluster	Slave Base Stations:
Access Points	Number of configured Slave Base Stations: 0
Sessions	Base Station Number: 1
Channel Management	Status: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Wireless Neighborhood	Description: Unnamed Base Station
Security	IP Address: 0.0.0.0 Port: 16100
Status	Message Size: 100 (Range 32..116)
Interfaces	Auto-Startup: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Events	
Transmit/Receive	To Restore Default Configuration...
Client Associations	Click "Default" to re-load the default configuration values for this Base Station. Default
Neighboring Access Points	Update Cancel
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	

22.4.1 Baz İstasyonu Yapılandırma Ayarları

Baz istasyonları Psion Teklogix özel protokollerini kullanan telsiz bağlantıları üzerinden iletişim sağlar. Baz istasyonları Ethernet üzerinden TCP/IP ağlarını kullanarak ağ denetleyicilerine bağlanabilir. 9160 G2, telsiz bağlantısı aracılığıyla mobil bilgisayarlarla iletişim kuran bir baz istasyonu olarak Ayarlanabilir Sorgulama/Çatışma RF protokolünü kullanır (protokollerle ilgili ayrıntılar için bkz. "*Telsiz Protokolleri*", sayfa 222).

9160 G2, telsiz bağlantısının çalışmasını ve zamanlamasını kontrol eder. Her baz istasyonu farklı bir telsiz kanalı kullanır ve mobil bilgisayarlar, istasyonlar arasında gezinmek için hücresel geçişi kullanır.

İleriki sayfalarda yer alan seçenek ve parametreler, 9160 G2'yi Ethernet ağı üzerinden 32 adede kadar bağımlı 9160 G2 baz istasyonuna bağlı bir ana baz istasyonu olarak yapılandırmanıza olanak sağlar. Ana 9160 G2, 9500 İletişim Sunucusuna ya da Psion Teklogix Yazılım Geliştirme Kiti'ne sahip altı adede kadar ana bilgisayara bağlıdır. *Connectivity* (Bağlantı) sekmesinin altındaki *Base Station* (Baz İstasyonu) seçeneği, sisteme yeni bir bağımlı baz istasyonu eklemenize ya da mevcut bir bağımlı baz istasyonundaki parametreleri değiştirmenize olanak sağlar.

Update (Güncelle) düğmesine bastığınızda ayarlarınız kaydedilir, **Default** (Varsayılan) düğmesine bastığınızda o baz istasyonunun varsayılan yapılandırma ayarları yeniden yüklenir.

Number of Configured Slave Base Stations (Yapılandırılan Bağımlı Baz İstasyonlarının Sayısı)

32 adede kadar bağımlı 9160 G2 baz istasyonu yapılandırabilirsiniz.

Base Station Number (Baz İstasyonu Sayısı)

Bu parametre atanan baz istasyonu sayısını gösterir. Açılır listeden **Base Station Number**'ı (Baz İstasyonu Numarası) seçmek, o ana bilgisayara ait değiştirilebilecek ya da silinebilecek parametreleri gösterir. Atanmamış bir numara seçerek ve parametreleri yapılandırarak yeni bağımlı baz istasyonları eklenebilir.

Status (Durum)

Bu parametre, bu bağımlı baz istasyonunu **etkinleştirir** ya da **devre dışı bırakır**.

Description (Açıklama)

Bu parametreye girilen ad, bağımlı baz istasyonunun IP Adresini tanımlamak için alternatif bir yol olarak kullanılır.

IP Address (IP Adresi)

Bu parametre, bağımlı baz istasyonu için ilgili IP adresini sağlar. Her bir bağımlı baz istasyonunun ağda tanımlanabilmesi için *IP Adresinin benzersiz bir değer* olması gereklidir.

Kabul edilen değerler **0.0.0.0** ile **239.255.255.255** arasında değişiklik gösterir.

IP bağlantı noktasının varsayılan değeri **16.100**'dür.

Message Size (Mesaj Boyutu)

Mesaj Boyutu, bir mobil bilgisayara gönderilebilecek en büyük mesajı belirler. Bu parametre için izin verilen aralık **32-380** karakterdir. (Uzun mesajlar birkaç paket halinde gönderilir.)

Sorgulama protokolü baz istasyonları için üst sınır **116**'dır.

Auto-Startup (Otomatik Başlama)

Bu parametre **etkinken**, **ana 9160 G2** başlatıldığında bağımlı baz istasyonları sorgulama işlemine başlar. *Otomatik Başlama devre dışıyken* baz istasyonları, **ana bilgisayardan start polling** (sorgulamayı başlat) komutunu almadan sorgulama işlemine başlamaz.

22.4.2 RRM Grupları Yapılandırma Ayarları

9160 G2, Uzak Telsiz Modülü (RRM, bkz. "Bağlantı Seçenekleri: RRM Modu", sayfa 231) olarak çalışırken aynı zamanda diğer RRM'leri kontrol edebilir. 9160 G2'nin RRM'leri kontrol edebilmesi için RRM gruplarının yapılandırılması gerekir. Bir RRM grubu tanımlandığında 1-4 adet RRM, gruba üye olabilir.

Bir gruptaki tüm RRM'ler aynı telsiz kanalında çalışır. 9160 G2, bir gruptaki tüm RRM'lerin aktarımlarını koordine eder (bu sebeple, kontrolü yapan 9160 G2 bazen "Zaman Çıklayıcı Yönetici" olarak adlandırılır).

Şekil 22.7 RRM Grupları Yapılandırma Ayarlarına Genel Bakış

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

View RRM Groups configuration settings

RRM Groups:

Number of Configured RRM Groups: 0

RRM Group Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed RRM Group

Auto-Startup: ☒ Enabled ☐ Disabled

Shared Channel: ☐ Enabled ☒ Disabled

Polling Protocol Parameters:

Number of Poll Windows: 3 (Range 2..4)

Size of Poll Windows: 8 (Range 5..32)

Maximum Message Segment Size: 100 (Range 32..116)

Number of Retries: 3 (Range 1..7)

Collision Size: 6 (Range 3..10)

Free Window Factor: 0 (Range 0..7)

Message Mode Limit: 4 (Range 0..7)

Call Sign Period: 0 (Range 0..60)

Call Sign String: Teklogix (Max 10 letters or digits)

Radio Parameters:

Sync Delay: 22 (Range 3..45)

Remote Tx On: 13 (Range 3..60)

Active Channel: 1 (Range 1..20)

Group Parameters:

Combination 1: (Sequence of RRM indices)

Combination 2: (Sequence of RRM indices)

Remote Radio Modules:

Enabled	Description	IP Address	Port
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132

Update

22.4.2.1 RRM Grupları

RRM Groups:	
Number of Configured RRM Groups:	0
RRM Group Number:	1 ▼
Status:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Description:	Unnamed RRM Group
Auto-Startup:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Shared Channel:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Kullanıcı, bu ekranda yeni bir RRM grubunun seçeneklerini ayarlayabilir. Her bir RRM, bir RRM grubunun üyesi olmalıdır; 9160 G2'de yapılandırılan birden fazla RRM grubu olabilir. Bir RRM grubu 1-4 adet RRM içerebilir.

Bu ekran, "Bağlantı Seçenekleri: Baz İstasyonu Modu", sayfa 225'teki ekrana çok benzer; tek fark, o telsiz menülerinde yapılandırılan parametreler 9160 G2'de yer alan RA1001A telsizi için geçerliken burada yapılandırılan parametrelerin diğer uzak 9160 G2'ler (RRM'ler) için geçerli olmasıdır.

Number of Configured RRM Groups (Yapılandırılan RRM Grubu Sayısı)

Bu 9160 G2'de yapılandırılan RRM grubu sayısını gösterir.

RRM Group Number (RRM Grubu Sayısı)

Bu parametre, atanan RRM grubu sayısını gösterir. Açılır listeden **RRM Group Number**'ı (RRM Grubu Numarası) seçmek, o gruba ait değiştirilebilecek ya da silinebilecek parametreleri gösterir. Atanmamış bir numara seçerek ve parametreleri yapılandırarak yeni RRM grupları eklenebilir.

Status (Durum)

Bu parametre, bu RRM grubunu **etkinleştirir** ya da **devre dışı bırakır**.

Description (Açıklama)

Bu metin kutusu, kullanıcının yeni RRM grubu için yeni bir ad girmesine izin verir. Değer, herhangi bir metin dizesidir. Varsayılan **Unnamed RRM Group**'tur (Adsız RRM Grubu).

Auto-Startup (Otomatik Başlama)

Bu parametre **etkin**ken 9160 G2 başlatıldığında ve otomatik olarak sorgulama işlemine başladığında bu RRM grubundaki RRM'lerle iletişim kurar. Otomatik **Başlama devre dışı**ken 9160 G2 başlatıldığında bu gruptaki RRM'lerle iletişim kurar ancak ana bilgisayardan sorgulamayı başlatma komutunu almadan sorgulama işlemine başlamaz. 9160 G2 başlatıldığında RRM grubundaki en az bir RRM çalışıyorsa sorgulama işlemi başlar.

Shared Channel (Paylaşılan Kanal)

Bu parametre **etkinleştirildiğinde** 9160 G2, sorgulama işlemine başlamadan önce bu RRM grubu tarafından kullanılan telsiz kanalındaki diğer trafiği kontrol eder.

Bu parametre **devre dışı bırakıldığında** 9160 G2, bu RRM grubu için telsiz kanalını ayrıcalıklı olarak kullanabildiğini varsayar ve telsiz trafiğini kontrol etmeden sorgulamayı gerçekleştirir.

Bu parametre, Hollanda'da kurulan sistemler için gereklidir.

22.4.2.2 Sorgulama Protokolü Parametreleri



Uyarı: *Bu parametreler, sisteminizde önceden yapılandırılmıştır ve telsiz bağlantısını nasıl etkiledikleri iyice anlaşılmadan değiştirilmemelidir.*

Polling Protocol Parameters:	
Number of Poll Windows:	<input type="text" value="3"/> (Range 2..4)
Size of Poll Windows:	<input type="text" value="8"/> (Range 5..32)
Maximum Message Segment Size:	<input type="text" value="100"/> (Range 32..116)
Number of Retries:	<input type="text" value="3"/> (Range 1..7)
Collision Size:	<input type="text" value="6"/> (Range 3..10)
Free Window Factor:	<input type="text" value="0"/> (Range 0..7)
Message Mode Limit:	<input type="text" value="4"/> (Range 0..7)
Callsign Period:	<input type="text" value="0"/> (Range 0..60)
Callsign String:	<input type="text" value="Teklogix"/> (Max 10 letters or digits)

Number of Poll Windows (Sorgulama Pencerelerinin Sayısı)

Bu metin kutusu, RRM'in sorgu gönderdikten sonra mobil bilgisayar yanıtlarını duymak için beklediği sorgu pencerelerinin sayısının kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **2-4** arasındır. Varsayılan değer **3**'tür.

Size of Poll Windows (Sorgulama Pencerelerinin Boyutu)

Bu metin kutusu, bu RRM grubundaki RRM'lerin mobil bilgisayar yanıtlarını duymak için bekledikleri sorgu pencerelerinin boyutunun kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **5-32** arasındır. Varsayılan değer **8**'dir.

Maximum Message Segment Size (Maksimum Mesaj Bölümü Boyutu)

Bu metin kutusu, Psion Teklogix telsiz ağı üzerinden gönderilecek en büyük mesaj bölümü boyutunun kullanıcı tarafından belirlenmesini (bayt cinsinden) sağlar. Büyük mesajlar parçalara bölünür. İzin verilen değer, **32-116** arasındır. Varsayılan değer **100**'dür.

Number of Retries (Yeniden Deneme Sayısı)

Bu metin kutusu, RRM mobil bilgisayardan herhangi bir bilgilendirme almadığında ve mobil bilgisayarın çevrimdışı olduğunu bildirmeden önce RRM'in bir mesajı kaç kez yeniden iletileceğinin kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **1- 7** arasındır. Varsayılan değer **3**'tür.

Collision Size (Çarpışma Boyutu)

Bu metin kutusu, RRM tarafından alınan gürültünün, Psion Teklogix ekipmanından gelen aktarımlarla parazit oluşturduğu şeklinde yorumlanması için sahip olması gereken en az karakter sayısının kullanıcı tarafından belirlenmesini sağlar. Bu eşik aşıldığında RRM, çarpışma çözümlemesine başlar. İzin verilen değer, **3- 10** arasındır. Varsayılan değer **6**'dır.

Free Window Factor (Boş Pencere Faktörü)

Bu metin kutusu, herhangi bir mobil bilgisayarın aktarım yapabildiği RRM sorgusu süresince RRM'nin boş bir pencere içirme ihtimalinin kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **0- 7** arasındır. Varsayılan değer **0**'dir.

Message Mode Limit (Mesaj Modu Sınırı)

Bu metin kutusu, sorgu aktarımına bir mesaj modu sorgusu dahil etme olasılığının kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **0- 7** arasındır. Varsayılan değer **4**'tür.

Callsign Period (Çağrı İşareti Süreci)

Bu metin kutusu, çağrı işareti iletimleri arasındaki zamanın kullanıcı tarafından belirlenmesini sağlar. Bu parametre dakika cinsinden belirlenir. 0 (sıfır) değeri, hiçbir çağrı işaretinin iletilmediğini gösterir. İzin verilen değer, **0- 60** arasındır. Varsayılan değer **0**'dir.

Callsign String (Çağrı İşareti Dizesi)

Bu metin kutusu, RRM'in çağrı işareti olarak iletilecek metnin kullanıcı tarafından belirlenmesini sağlar. Metin, Mors kodunda iletilir. Varsayılan değer **Teklogix**'tir.

22.4.2.3 Telsiz Parametreleri

Radio Parameters:		
Sync Delay:	<input type="text" value="22"/>	(Range 3..45)
Remote Tx On:	<input type="text" value="13"/>	(Range 3..60)
Active Channel:	<input type="text" value="1"/>	(Range 1..20)

Bazı telsiz parametreleri, belirli bir zaman çoklamalı RRM'ler grubu için aynı olduğundan 9160 G2'de bir kereye mahsus olarak kullanıcı tarafından yapılandırılabilir. 9160 G2, daha sonra bu parametreleri gruptaki RRM'lere iletir. Bu parametreler şunları içerir: senkronizasyon bekleme süresi (*Sync Delay*), zamanında uzaktan aktarma (*Remote Txon* [*Uzak Txon*]) ve kullanılacak kanal numarası (*Active Channel* [*Etkin Kanal*]).

Grupta yer alan her RRM'deki RA1001A dar bant telsiz ayrı olarak yapılandırılrsa da 9160 G2, aynı şekilde yapılandırıldığını varsayar. 9160 G2, bunu sağlamak için her RRM tarafından döndürülen belirli parametrelere bakar. Bu parametreler, telsiz baud hızı ve zamanında aktarmayı içerir.

Bu parametreler, aynı gruptaki diğer RRM'ler tarafından döndürülen değerlerle karşılaştırılır. Bu değerler eşleşmezse hata mesajları görüntülenir ancak en kötü durumda kullanılacak değer seçilir.



Uyarı: *Bu parametreler, sisteminizde önceden yapılandırılmıştır ve telsiz bağlantısını nasıl etkiledikleri iyice anlaşılmadan değiştirilmemelidir.*

Sync Delay (Senkronizasyon Bekleme Süresi)

Bu metin kutusu, RRM aktarımı ve ilk yanıt penceresi arasında girilecek bekleme süresi karakterleri sayısının kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **3- 45** arasındır. Varsayılan değer **22**'dir.

Remote Txon (Uzak Txon)

Bu metin kutusu, mobil bilgisayar mesaj verisi göndermeden önce mobil bilgisayar telsizleri tarafından gönderilen doldurma karakterleri sayısının kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **3- 60** arasındır. Varsayılan değer **13**'tür.

Active Channel (Etkin Kanal)

Bu metin kutusu, RRM grubundaki tüm RRM'lerin kullanacağı telsiz kanalının kullanıcı tarafından belirlenmesini sağlar. İzin verilen değer, **1- 20** arasındır. Varsayılan değer **1**'dir.

22.4.2.4 Grup Parametreleri

Group Parameters:	
Combination 1:	<input type="text"/> (Sequence of RRM indices)
Combination 2:	<input type="text"/> (Sequence of RRM indices)

Combination (Kombinasyon)

Bu metin kutuları, *kombinasyon* adı verilen RRM alt gruplarının kullanıcı tarafından belirlenmesini sağlar. Bu RRM grubundaki iki ya da daha fazla RRM'in kapsama alanı çakışmıyorsa çakışmayan RRM'ler aynı anda sorgulama yapabilir. Bu durum, sistem yanıt süresini geliştirir ve ağdaki sinyal miktarını azaltır. Kombinasyonlara atanmayan RRM'ler, kombinasyon sorgusundan sonra ayrı ayrı sorgulama yapar.

Örneğin, RRM grubunun 3 RRM'i varsa ve RRM 1 ve 3 çakışmıyorsa bu RRM'ler tek bir alt gruba yerleştirilebilir (*Combination 1 [Kombinasyon 1]*) ve ardından aynı anda sorgulama yapar. RRM 2, başka bir alt gruba yerleştirilir (*Combination 2 [Kombinasyon 2]*). Sorgulama işlemi iki alt gruba sırayla gerçekleşir.

Bir kombinasyon yapılandırmak için RRM sayısını o kombinasyonun metin kutusuna yazın. Sayılar, *Remote Radio Modules* (Uzak Telsiz Modülleri) menüsündeki (bkz. sayfa 241) RRM listesinde yer alan RRM sayılarına karşılık gelir. Örneğin, *Combination 1* (Kombinasyon 1) metin kutusunda yazan "13" sayısı RRM 1 ve 3'ü aynı alt gruba yerleştirir.



Not: RRM kombinasyonlarını yapılandırırken yapılandırılmış RRM'lerin sıralı olduğundan ve hiçbir sayının eksik olmadığından emin olun. Bu durum, RRM'ler silindiğinde ve eklendiğinde oluşabilir. Kombinasyonlar RRM'leri listedeki numaralarına göre değil, görüntülendikleri sıraya göre kullanır.

22.4.2.5 Uzak Telsiz Modülleri

Remote Radio Modules:				
	Enabled	Description	IP Address : Port	
1	<input checked="" type="checkbox"/>	Built-in	10.128.75.174	16132
2	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
3	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132
4	<input type="checkbox"/>	Unnamed RRM	0.0.0.0	16132

Bu menü, bu RRM Grubu ile her Açıklama, IP adresi ve Bağlantı Numarasını RRM çalışma moduna ayarlanan 9160 G2'nin *Connectivity Options* (Bağlantı Seçenekleri) alt menüsünde ayarlanan şekilde içeren RRM'leri görüntüler. (bkz. "Bağlantı Seçenekleri: RRM Modu", sayfa 231). Her RRM bu menüden etkinleştirilebilir veya devre dışı bırakılabilir.

22.4.3 Telsiz Bağlantısı Özellikleri Yapılandırma Ayarları

Connectivity (Bağlantı) seçenekleri listesinden *Radio Link Features* (Telsiz Bağlantısı Özellikleri) kısmına girildiğinde sorgulama ve hücresel parametrelerin yapılandırma ayarları sayfası açılır.

Şekil 22.8 Telsiz Bağlantısı Özellikleri Yapılandırma Ayarlarına Genel Bakış

Basic Settings	View Radio Link Features configuration settings
User Management	
Cluster	Radio Link Features:
Access Points	Operate in Cellular Mode: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Sessions	Poll ID: <input type="text" value="35"/> Range (0..255)
Channel Management	Polling Protocol Terminal Timeout: <input type="text" value="60"/> Range (1..240)
Wireless Neighborhood	Percent Polling Protocol Terminal Timeout: <input type="text" value="75"/> Range (50..90)
Security	Direct TCP Connections for TekTerm: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Status	Direct TCP Check Duplicate Terminal Number: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Interfaces	Expiration period (in days) for Automatic Radio Address and Terminal Number: <input type="text" value="2"/> Range (2..365)
Events	
Transmit/Receive	Automatic Radio Address
Client Associations	First Address: <input type="text" value="1024"/> Last Address: <input type="text" value="2048"/> Ranges (1..3840)
Neighboring Access Points	Automatic Terminal Number
Manage	Group Ranges (1..1024)
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	

22.4.3.1 Telsiz Bağlantısı Özellikleri

Radio Link Features:
Operate in Cellular Mode: ☒ Enabled ☐ Disabled
Poll ID: Range (0..255)
Polling Protocol Terminal Timeout: Range (1..240)
Percent Polling Protocol Terminal Timeout: Range (50..90)
Direct TCP Connections for TekTerm: ☐ Enabled ☒ Disabled
Direct TCP Check Duplicate Terminal Number: ☒ Enabled ☐ Disabled
Expiration period (in days) for Automatic Radio Address and Terminal Number: Range (2..365)

Operate in Cellular Mode (Hücresel Modda Çalış)

Hücresel bir baz istasyonu olarak çalışmak için bu parametrenin **etkinleştirilmesi** gerekir.



Not: 9500 İletişim Sunucusunun da hücresel moda ayarlanması gerekir.

Poll ID (Sorgu Kimliği)

Dar bant telsizler için Ayarlanabilir Sorgulama/Çatışma protokolünde her baz istasyonuna ayrı bir adres atamak için *Poll ID* (Sorgu Kimliği) kullanılır. Mobil bilgisayarlar bir baz istasyonundan diğerine geçerken bu adres, birden fazla baz istasyonlu bir sistemde her bir 9160 G2'yi tanımlayarak baz istasyonundan mobil bilgisayarlara iletilir.

Polling Protocol Terminal Timeout (Sorgulama Protokolü Terminal Zaman Aşımı)

Bu parametre, bir mobil bilgisayarın 9160 G2 tarafından çevrimdışı olduğu bildirilene kadar kaç dakika eylemsiz kalabileceğini belirler. Bu durum gerçekleşmeden önce, *Yüzde Sorgulama Protokolü Terminal Zaman Aşımı* parametresi mobil bilgisayarın çevrimdışı olduğunu bildirir (aşağıya bakın).

Mobil bilgisayar, sistemden çıkarıldıktan sonra 9160 G2 ile iletişim kurmak için yeniden başlatılmalıdır. Bu parametre, telsiz bağlantısı üzerindeki iletişim kurmayan mobil bilgisayarların desteklenmesiyle oluşan ek yükü azaltır. İzin verilen değer, **1 - 240** arasındır.

Percent Polling Protocol Terminal Timeout (Yüzde Sorgulama Protokolü Terminal Zaman Aşımı)

Bu parametre, bir mobil bilgisayarın 9160 G2 tarafından çevrimdışı olduğu bildirilene kadar eylemsiz kalmasına izin verilen süreyi belirler. Bu süre, *Sorgulama Protokolü Terminal Zaman Aşımı* parametresinin bir yüzdesiyle ifade edilir (yukarı bakın). Örneğin, *Yüzde Sorgulama Protokolü Terminal Zaman Aşımı* 60 ise ve bu parametre %75 olarak ayarlanmışsa zaman aşımı 60 dk. x %75 = 45 dakikadır.

Çevrimdışı bir mobil bilgisayar halen sistemin bir parçası kabul edilir. Çevrimdışı mobil bilgisayarlara gelen mesajlar 9160 G2'de kuyruğa eklenir. Mobil bilgisayar çevrimiçi bir mesaj iletene kadar çevrimdışı kalır. Bu parametrenin değerleri **50 - 90** arasındır.

Direct TCP Connections for TekTerm (TekTerm İçin Doğrudan TCP Bağlantıları)

Bu parametre etkinleştirildiğinde Psion Teklogix mobil bilgisayarlarda bulunan *TekTerm* programı, 9160 G2'nin TCP/IP aracılığıyla bir ana bilgisayarın baz istasyonu olarak çalıştığı durumlarda doğrudan 9160 G2'ye bağlanabilir.

Direct TCP Check Duplicate Terminal Number (Doğrudan TCP Kontrolü Yinelenen Terminal Numarası)

Bu parametre etkinleştirildiğinde 9160 G2, halihazırda başka bir mobil bilgisayarın kullandığı bir terminal numarasını kullanarak bağlanmaya çalışan Doğrudan TCP mobil bilgisayarlara reddeder. Devre dışı bırakıldığında, en son bağlanmaya çalışan mobil bilgisayar, aynı terminal numarasını kullanan diğer mobil bilgisayarların önüne geçer.

22.4.3.2 Otomatik Telsiz Adresleri

Automatic Radio Address				
First Address:	<input type="text" value="1024"/>	Last Address:	<input type="text" value="2048"/>	Ranges (1..3840)

Telsiz bağlantısını kullanan her bir Psion Teklogix mobil bilgisayarının benzersiz bir telsiz adresi numarası vardır. Bu numara, bu parametre etkinleştirildikten sonra 9160 G2 tarafından otomatik olarak atanabilir.

Bu parametreyi **etkinleştirmek** için ilk ve son telsiz adresi numaraları **1 - 3840** arası olmalıdır. Bu aralık için varsayılan değerler **1024 ... 2084**'tür. Bu parametreyi **devre dışı bırakmak** için değerleri **0** olarak ayarlayın.



Notlar: Bu parametreyi etkinleştirirken:

1. *TekTerm için Doğrudan TCP Bağlantıları devre dışı bırakılmalıdır (bkz. sayfa 244).*
2. *Telsiz adresinin otomatik olarak atanması için mobil bilgisayardaki Otomatik Kimlik parametresi etkinleştirilmelidir.*
3. *Otomatik Telsiz Adresi ve Otomatik Terminal Numarasını kullanan oturumlarla 802.IQ modunda çalışan herhangi bir 9150 ya da 9160 G2 baz istasyonunda Auto Startup (Otomatik Başlat) özelliğini etkinleştirmeyin (bkz. sayfa 303).*

Bitiş Süresi

Bu parametre, belirli bir telsiz adresinin ya da terminal numarasının 9160 G2 tarafından "süresi geçmiş" olarak ilan edilmeden önce kaç gün eylemsiz kalması gerektiğini belirtir. Süresi geçen bir adres ya da terminal numarası, başka bir telsize ya da oturuma yeniden atanabilir.



Not: Bu özellikle ilgili olarak SNTP'yi etkinleştirmeniz ve net bitiş süreleri için bir SNTP sunucusuna sahip olmanız önerilir.

22.4.3.3 Otomatik Terminal Numarası

Mobil bilgisayarda oluşturulan her uygulama oturumu için bir terminal numarası atanır. Bu numara, bu oturuma gelen ve buradan gönderilen tüm aktarımların ayrı ayrı tanımlanmasına yardımcı olur.

Automatic Terminal Number			
Group Ranges (1..1024)			Comments
1	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
2	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
3	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
4	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>
5	<input type="text" value="0"/>	... <input type="text" value="0"/>	<input type="text"/>

Terminal numaraları, uygulama oturumlarına otomatik olarak atanabilir. Ayrıca denetleyici, TESS ve ANSI oturumlarıyla kullanmak için bir grup numarası sağlar. Beş adede kadar terminal oturumu grubu tanımlanabilir ve her bir gruba otomatik atamayla farklı bir terminal numarası aralığı verilebilir. Bu aralıklar, gruplar arasında çakışamaz.

Gruplar, yalnızca TESS ve ANSI oturumları için geçerlidir. Mobil bilgisayarda, TESS ya da ANSI terminal uygulamaları hangi gruba ait olduklarını belirtir ve o grubun Otomatik Terminal Numarası atama aralığını kullanır.

Diğer tüm oturum türleri Otomatik Terminal Numarası aralığı olarak 1 - 3840'ı kabul eder ve "grup" parametresini kullanmaz. Otomatik Terminal Numarası atamayı kullanan ANSI ve TESS olmayan emülasyonların (örneğin Uzak Soketler), terminal aralıklarını 1'den başlayacak şekilde ayarlamalıdır ve bu aralık, tüm mobil bilgisayarları içerecek kadar geniş olmalıdır.

Radio Link Features (Telsiz Bağlantısı Özellikleri) ekranı, her Otomatik Terminal Numarası için pek çok parametre sunar: daha düşük ve daha yüksek terminal numaralarıyla belirlenen bir aralık ve bir yorum. Yorum, grubu anlatmak için kullanılabilecek bir ASCII metni dizesidir.



Notlar: Otomatik Terminal Numarasını etkinleştirirken:

1. *TekTerm için Doğrudan TCP Bağlantıları devre dışı bırakılmalıdır (bkz. sayfa 244).*
2. *Terminal oturum numarasının otomatik olarak atanması için mobil bilgisayardaki Otomatik Oturum parametresi etkinleştirilmelidir.*

22.4.4 Ana Bilgisayarlar Menüsü

9160 G2, baz istasyonu olarak kullanılırken 9500 İletişim Sunucusu gibi bir "sunucu" ile ya da Psion Teklogix Yazılım Geliştirme Paketi (SDK) kullanan bir ana bilgisayarla iletişim kurmalıdır. Bu nedenle, 9160 G2 ile iletişim kuran her ana ağ denetleyici, SDK sunucusu ya da ana baz istasyonu bir ana bilgisayar olarak yapılandırılmalıdır. *Connectivity* (Bağlantı) seçeneklerinin *Hosts* (Ana Bilgisayarlar) sayfası, açılır menüden seçilen ana bilgisayarla ilgili açıklamaları gösterir (bkz. Şekil 22.9, sayfa 247).

Bu seçenekteki menü sayfası, sistemdeki ana bilgisayar adlarını gösterir. Altı adede kadar ana bilgisayar desteklenebilir. Bir ana bilgisayar yapılandırıldığında, o ana bilgisayarın **Ana Bilgisayar Numarasını** seçmek değiştirilebilecek ya da silinebilecek parametreleri listeler.

Şekil 22.9 Baz İstasyonunun Ana Bilgisayar Yapılandırma Ayarlarına Genel Bakış

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

9010 Configuration:

No Online/Offline: ☐ Enabled ☒ Disabled

Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. [Default](#)

[Update](#) [Cancel](#)

Number Of Configured Hosts (Yapılandırılan Ana Bilgisayar Sayısı)

Connectivity (Bağlantı) seçeneklerindeki *Hosts* (Ana Bilgisayarlar) sayfası, sistemde yapılandırılan ana bilgisayarların sayısını gösterir. Altı adede kadar ana bilgisayar desteklenebilir.

Host Number (Ana Bilgisayar Numarası)

Bu parametre, atanan ana bilgisayar numarasını belirtir. Açılır listeden **Host Number** (Ana Bilgisayar Numarası) seçeneğini belirlemek, o ana bilgisayara ait değiştirilebilecek ya da silinebilecek parametreleri gösterir. Atanmamış bir numara seçerek ve parametreleri yapılandırarak yeni ana bilgisayarlar eklenebilir.

Birden fazla ana bilgisayarın olduğu ortamlarda, ana bilgisayarlar arası geçiş yapılırken ana bilgisayar numarası RF mobil bilgisayarda da görüntülenir.

Status (Durum)

Bu ana bilgisayarla iletişim kurmak için mobil bilgisayarların durumu **Enabled** (Etkinleştirildi) olarak ayarlanmalıdır.

Açıklama

Bu metin kutusu, ana bilgisayar tarafından kullanılan protokolü adlandırmanızı sağlar. Protokoller, mobil bilgisayarların Ethernet ve radyolink bağlantıları gibi fiziksel ortamlar üzerinden ana bilgisayarlarla iletişim kurmak için kullandığı yöntemlerdir.

9160 G2, baz istasyonu görevi gördüğünde, ağ bağlantısı kullanarak **9010/ TCP/IP** ana bilgisayarıyla iletişim kurar. 9010 protokolü, mobil bilgisayarlarla iletişim kurmak için TESS (Teklogix Ekran Alt Sistemi) ya da ANSI veri akışlarını kullanan Psion Teklogix tarafından geliştirilen özel, asenkron bir protokoldür. Ayrıntılı bilgi için *9500 İletişim Sunucusu, SDK, TESS* ya da *ANSI* ile ilgili *Psion Teklogix Kullanım Kılavuzlarından* uygun olana bakın.

First Terminal/Last Terminal (İlk Terminal/Son Terminal)

Bu parametrelere girilen değerler, ana bilgisayarla iletişim kuracak mobil bilgisayarın menzilineki ilk ve son terminali belirtir. Terminal numaraları, bu belirli ana bilgisayarla eşleşir. Terminal numaraları **1** ila **3840** arası olabilir.

To Restore Default Configuration (Varsayılan Yapılandırmayı Geri Yüklemek İçin)

Bu ana bilgisayarın varsayılan yapılandırma ayarlarını yeniden yüklemek için Host (Ana Bilgisayar) menü sayfasının alt kısmında yer alan **Default** (Varsayılan) düğmesine tıklayabilirsiniz.

Ayarları Güncelleme

Ana bilgisayarı yapılandırma işleminin herhangi bir aşamasında sayfanın alt kısmındaki *Update* (Güncelle) düğmesini kullanarak ayarları güncelleyebilir ya da *Cancel* (İptal Et) düğmesini kullanarak işlemi iptal edebilirsiniz.

22.4.4.1 9010 Yapılandırma

9010 Configuration:
No Online/Offline: ☐ Enabled ☒ Disabled
Monitor Poll: ☐ Enabled ☒ Disabled

To Restore Default Configuration...
Click "Default" to re-load the default configuration values for this Host. Default

No Online/Offline (Çevrimiçi/Çevrimdışı Yok)

Bu parametre için **Enabled** (etkin) seçildiğinde 9160 G2 baz istasyonu, mobil bilgisayarın durumu çevrimiçi ya da çevrimdışı olarak değiştiğinde ana bilgisayarı bu değişiklikle ilgili **bilgilendirmez**. Bu parametre için **Disabled** (devre dışı) seçildiğinde 9160 G2, ana bilgisayarı mobil bilgisayarın durum değişiklikleriyle ilgili **bilgilendirir**. Bu parametre için varsayılan seçenek **Disabled** (devre dışı) seçeneğidir.

Monitor Poll (Sorguları İzle)

Ana bilgisayarlar genellikle yaklaşık 40 saniyede bir 9160 G2'ye mesaj ya da boş sorgu gönderir. Bu parametre için **enabled** (etkin) seçildiğinde 9160 G2 baz istasyonu, bu ana bilgisayardan gelen mesajları ve sorguları izler; 40 saniye içinde herhangi bir mesaj ya da sorgu almazsa bağlantıyı kapatır. Bu parametre için varsayılan seçenek **disabled** (devre dışı) seçeneğidir.

Mini DENETLEYİCİ YAPILANDIRMASI

23

23.1 Genel Bakış	253
23.2 Mini Denetleyici Yapılandırma Menüsü	254
23.3 Hosts (Ana Bilgisayarlar) Menüsü	254
23.4 Ana Bilgisayar Menüsü Seçenekleri	258
23.4.1 3274 Emülasyonu	258
23.4.1.1 Emulation Options (Emülasyon Seçenekleri)	258
23.4.1.2 TESS Options (TESS Seçenekleri)	259
23.4.1.3 Telnet Protokol Seçenekleri	269
23.4.1.4 İşlev Tuşu Eşlemeleri	273
23.4.2 5250 Emülasyonu	274
23.4.2.1 Emulation Options (Emülasyon Seçenekleri)	274
23.4.2.2 TESS Options (TESS Seçenekleri)	275
23.4.2.3 Telnet Protokol Seçenekleri	285
23.4.2.4 İşlev Tuşu Eşlemeleri	288
23.4.3 ANSI Emülasyonu	289
23.4.3.1 Emulation Options (Emülasyon Seçenekleri)	289
23.4.3.2 Telnet Protokol Seçenekleri	293
23.4.3.3 Otomatik Telnet/Otomatik Oturum Açma	295
23.4.3.4 İşlev Tuşu Eşlemeleri	299

23.1 Genel Bakış

Bir Psion Teklogix sistemindeki ağ denetleyicisi pek çok önemli görevi yerine getirir. Bu görevlerden biri *emülasyondur*. Emülasyon, ana bilgisayar protokolü ile Psion Teklogix mobil bilgisayarları tarafından kullanılan protokol arasında veri aktarımı olarak tanımlanabilir.

Kendi ekranını sağlamak için ana bilgisayardan mobil bilgisayara gönderilen ve mobil bilgisayardaki işlemlerden sonra ana bilgisayara geri dönen veriye veri akışı denir. Ana bilgisayarlar mobil bilgisayarlarına çeşitli türlerde veri akışı sağlayabilir.

Psion Teklogix mobil bilgisayarlar yalnızca iki tür veri akışını doğrudan alabilir: *TESS* ve *ANSI*. TESS (Teklogix Screen Subsystem [Teklogix Ekran Alt Sistemi]) Psion Teklogix mobil bilgisayarlar tarafından kullanılan özel bir veri akışdır. ANSI veri akışları kablolu ANSI mobil bilgisayarlar tarafından kullanılan standart bir veri akışdır. Psion Teklogix mobil bilgisayarların ana bilgisayarın sağladığı diğer veri akışı türleriyle çalışabilmesi için bu veri akışlarının önce TESS ya da ANSI'ye dönüştürülmesi gerekir. Bu dönüştürme işlemi ağ denetleyicisindeki emülasyon yazılımı tarafından yapılır.

9160 G2 Kablosuz Ağ Geçidi, mini bir denetleyici olarak kullanılmasına olanak veren emülasyon özelliklerine sahiptir. 9160 G2 mini denetleyici olarak yapılandırıldığında Psion Teklogix mobil bilgisayarlar, 9500 İletişim Sunucusu yerine 9160 G2 aracılığıyla bir ANSI, 5250 ya da 3274 mobil bilgisayar gibi çalışabilir.



Önemli: *Mini denetleyici olarak çalışan 9160 G2'ler küçük, işlem sayısı az olan siteler için tasarlanmıştır. 50'den fazla mobil bilgisayar destekleyen sistemler için 9500 İletişim Sunucusu gerekir.*

Mini denetleyici olarak çalışan 9160 G2 Kablosuz Ağ Geçidi 32 adede kadar ağ tabanlı baz istasyonu ve 50 adede kadar mobil bilgisayar destekleyebilir. 9160 G2 mini denetleyici kablosuz LAN yapılandırmalarını da yönetebilir.

Mini denetleyici olarak yapılandırılan 9160 G2 şu emülasyonları destekler:

- Ethernet LAN üzerinden TCP/IP kullanarak 5250 emülasyonu.
- Ethernet LAN üzerinden TCP/IP kullanarak 3274 emülasyonu.
- Ethernet LAN üzerinden TCP/IP kullanarak ANSI emülasyonu.



Not: 9160 G2 ana parametrelerinin önce bu kılavuzun önceki bölümlerinde anlatıldığı şekilde ayarlanması gerekir.

Ayrıca 9160 G2, 802.IQv2 protokolü kullanılarak bir mapRF sistemine entegre edilebilir (ayrıntılar için bkz. "802.IQ v2 Özellikleri Menüsü", sayfa 307).



Not: Mini denetleyici özelliği, ancak konsol isteminde kullanılan şifre aracılığıyla kilidi açıldıktan sonra kullanılabilir.

23.2 Mini Denetleyici Yapılandırma Menüsü

9160 G2'yi mini denetleyici olarak çalıştırmak için *Hosts* (Ana Bilgisayarlar) sayfalarındaki parametrelerin uygun şekilde ayarlanması gerekir. *Connectivity* (Bağlantı) seçenekleri listesinde *Hosts* (Ana Bilgisayarlar) bölümüne girdiğinizde *Configuration Settings For A Base Station's Host* (Baz İstasyonu Ana Bilgisayarı İçin Yapılandırma Ayarları) sayfası açılır. Telsiz protokolü parametrelerini yapılandırma hakkında bilgi için bkz. "Telsiz Bağlantısı Özellikleri Yapılandırma Ayarları", sayfa 241.

23.3 Hosts (Ana Bilgisayarlar) Menüsü

Bu seçenekteki menü sayfası, sistemdeki ana bilgisayar adlarını gösterir. Altı adede kadar ana bilgisayar desteklenebilir. 9160 G2 mini denetleyiciyle iletişim kuran her ana bilgisayar için bir "ana bilgisayar" yapılandırılmalıdır. Bir ana bilgisayar yapılandırıldığında, o ana bilgisayarın **Ana Bilgisayar Numarasını** seçmek, değiştirilebilecek ya da silinebilecek parametreleri listeler.

Şekil 23.1 Ana Bilgisayar Yapılandırma Ayarlarına Genel Bakış

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Interfaces

Events

Transmit/Receive

Client Associations

Neighboring Access Points

Manage

Ethernet Settings

802.11 Settings

802.11 Advanced Settings

VWN

WDS

Guest Login

MAC Filtering

Load Balancing

Services

QoS

Time

SNMP

Narrow Band

Radio

Connectivity Options

Connectivity

Base Station

RRM Groups

Radio Link Features

Hosts

802.1Q

Maintenance

Configuration

Upgrade

View the configuration settings for a Base Station's Host

Hosts:

Number of configured Hosts: 0

Host Number: 1

Status: ☐ Enabled ☒ Disabled

Description: Unnamed Host

First Terminal: 1

Last Terminal: 32

Emulation: 5250

5250 Emulation Options:

Write Error Code: Advisory text

Use International EBCDIC: ☐

Allow null character in fixed fields: ☐

TESS Options:

Field Underline Remapping: None

Alarm: ☐

Clear: ☐

Passthru: ☐

Procedures: ☐

Local: ☐

Host Print: ☐

Remote Print: ☐

Pages: 8 (Range 1..79)

Transmit Line: 0 (Range 0..24)

AIAG: 0 (Range 0..255)

Visible Match Character: 0 (Range 0..255)

Hidden Match character: 0 (Range 0..255)

Serial I/O: 0 (Range 0..255)

Print Line: 0 (Range 0..24)

Print Form Length: 0 (Range 0..24)

Barcode: 0 (Range 0..255)

Entry Line: 0 (Range 0..24)

Field Overhead: 5 (Range 0..80)

Command Region: 0, 0, 0, 0

Telnet Protocol Options:

Terminal Type: IBM-5251-11

Host Port: 23 (Range 1..32767)

Maximum Sessions per Terminal: 4 (Range 1..127)

First Local Terminal Port: 10000 (Range 1..32767)

Local IP Address to Bind: 0.0.0.0

First Terminal Listen Port: 0 (Range 0..32767)

Actively Negotiate with Host: ☐

Auto-telnet: DISABLE

Auto-telnet Host:

Auto-telnet without User Action: ☒

Enable Virtual Device Names: ☐

- Configure Device Names: Configure

- Device Name Prefix:

Function Key Mappings:

F1: F1 F14: F14 F27: F17

F2: F2 F15: F15 F28: F18

F3: F3 F16: CLEAR F29: UP

F4: F4 F17: PRINT F30: SESS

F5: F5 F18: HELP F31: ENTER

F6: F6 F19: F19 F32: ENTER

F7: F7 F20: F20 F33: ENTER

F8: F8 F21: F21 F34: ENTER

F9: F9 F22: F22 F35: ENTER

F10: F10 F23: F23 F36: ENTER

F11: F11 F24: F24 F37: ENTER

F12: F12 F25: DOWN F38: SELECTOR

F13: F13 F26: F16 F39: ENTER

To Restore Default Configuration...

Click "Default" to re-load the default configuration values for this Host. Default

Update Cancel

When the 9160 acts as a Base Station, it must communicate with a "host" - a 9500 or 9400 network Controller, or a host computer using Psion Teklogix Software Development Kit (TSDK).

This page allows you to select the host names present on the system. Up to six hosts can be supported. A "host" must be configured for each master network controller, TSDK host, or master Base Station that communicates with the 9160.

Psion Teklogix 9160 G2 Kablosuz Ağ Geçidi Kullanım Kılavuzu 255

Number Of Configured Hosts (Yapılandırılan Ana Bilgisayar Sayısı)

Connectivity (Bağlantı) seçeneklerindeki *Hosts* (Ana Bilgisayarlar) sayfası, sistemde yapılandırılan ana bilgisayarların sayısını gösterir. Altı adede kadar ana bilgisayar desteklenebilir.

Host Number (Ana Bilgisayar Numarası)

Bu parametre, atanan ana bilgisayar numarasını belirtir. Açılır listeden **Host Number** (Ana Bilgisayar Numarası) seçeneğini belirlemek, o ana bilgisayara ait değiştirilebilecek ya da silinebilecek parametreleri gösterir. Atanmamış bir numara seçerek ve parametreleri yapılandırarak yeni ana bilgisayarlar eklenebilir.

Birden fazla ana bilgisayarın olduğu ortamlarda, ana bilgisayarlar arası geçiş yapılırken ana bilgisayar numarası RF mobil bilgisayarda da görüntülenir.

Status (Durum)

Bu ana bilgisayarla iletişim kurmak için mobil bilgisayarların durumu **Enabled** (Etkinleştirildi) olarak ayarlanmalıdır.

Description (Açıklama)

Bu metin kutusu, ana bilgisayar tarafından kullanılan protokolü adlandırmanızı sağlar. Protokoller, mobil bilgisayarların Ethernet ve radyolink bağlantıları gibi fiziksel ortamlar üzerinden ana bilgisayarlarla iletişim kurmak için kullandığı yöntemlerdir.

9160 G2, baz istasyonu görevi gördüğünde, ağ bağlantısı kullanarak **9010/ TCP/IP** ana bilgisayarıyla iletişim kurar. 9010 protokolü, mobil bilgisayarlarla iletişim kurmak için TESS (Teklogix Ekran Alt Sistemi) ya da ANSI veri akışlarını kullanan Psion Teklogix tarafından geliştirilen özel, asenkron bir protokoldür. Ayrıntılı bilgi için *9500 İletişim Sunucusu, SDK, TESS* ya da *ANSI* ile ilgili *Psion Teklogix Kullanım Kılavuzlarından* uygun olana bakın.

First Terminal/Last Terminal (İlk Terminal/Son Terminal)

Bu parametrelere girilen değerler, ana bilgisayarla iletişim kuracak mobil bilgisayarın menzilineki ilk ve son terminali belirtir. Terminal numaraları, bu belirli ana bilgisayarla eşleşir. Terminal numaraları **1** ila **3840** arası olabilir.

Emulation (Emülasyon)

Bu açılır menü, 9160 G2 Kablosuz Ağ Geçidi tarafından desteklenen ana bilgisayar emülasyonlarının listesini sunar. Psion Teklogix mobil bilgisayarlar ve baz istasyonlarıyla çalışan 9160 G2, ANSI mobil bilgisayarların yanı sıra IBM 3278-2, 5251-11 ve 5555-B01 mobil bilgisayarları da emüle edebilir.

Protokoller, mobil bilgisayarların Ethernet ve radyolink bağlantıları gibi çeşitli ortamlar üzerinden ana bilgisayarlarla iletişim kurmak için kullandığı yöntemlerdir. 9160 G2, TCP/IP protokolünü destekler. Desteklenen emülasyonlar şunlardır:

- 9010/ TCP/IP (Ayrıntılar için aşağı bakın).
- 3274 Emülasyonu (Yapılandırma Parametreleri için bkz. 258 - 273).
- 5250 Emülasyonu (Yapılandırma Parametreleri için bkz. 274 - 288).
- ANSI Emülasyonu (Yapılandırma Parametreleri için bkz. 289 - 299).

9160 G2 Kablosuz Ağ Geçidi baz istasyonu görevi gördüğünde 9500 İletişim Sunucusuyla veya Psion Teklogix Yazılım Geliştirme Paketi (SDK) kullanan bir ana bilgisayarla iletişime geçmek için 9010 emülasyonunu (Psion Teklogix tarafından geliştirilen özel, asenkron bir protokol) kullanır. 9160 G2'yi baz istasyonu olarak yapılandırma ve 9010 emülasyonu hakkında bilgi için bkz. Bölüm 22: “9160 G2'nin Baz İstasyonu Olarak Kullanılması”.

9160 G2 Kablosuz Ağ Geçidi, mini denetleyici görevi gördüğünde IBM ana bilgisayarlarıyla iletişim kurmak için 3274 ve 5250 emülasyon protokollerini; ANSI mobil bilgisayarlarla iletişim kurmak için ANSI emülasyon protokolünü kullanır.

To Restore Default Configuration (Varsayılan Yapılandırmayı Geri Yükleme İçin)

Bu ana bilgisayarın varsayılan yapılandırma ayarlarını yeniden yüklemek için Host (Ana Bilgisayar) menü sayfasının alt kısmında yer alan **Default** (Varsayılan) düğmesine tıklayabilirsiniz.

Ayarları Güncelleme

Ana bilgisayarı yapılandırma işleminin herhangi bir aşamasında sayfanın alt kısmındaki *Update* (Güncelle) düğmesini kullanarak ayarları güncelleyebilir ya da *Cancel* (İptal Et) düğmesini kullanarak işlemi iptal edebilirsiniz.

23.4 Ana Bilgisayar Menüü Seçenekleri

Mevcut bir *Ana Bilgisayar Numarasını* seçtiğinizde 9160 G2, o ana bilgisayarın yapılandırma parametrelerini gösterir. 5250, 3274 ve ANSI emülasyonlarının dört alt menüsü vardır: ana bilgisayarın *Emülasyon Seçenekleri*, *TESS Seçenekleri*, *Telnet Protokol Seçenekleri* ve *Fonksiyon Tuşu Eşlemeleri* (sayfanın genel görünümü için bkz. Şekil 23.1, sayfa 255).

23.4.1 3274 Emülasyonu

23.4.1.1 Emulation Options (Emülasyon Seçenekleri)

3274 Emulation Options:
Is Host Fujitsu: ☐
Use International EBCDIC: ☐
Allow null character in fixed fields: ☐

9160 G2 mini denetleyici, IBM 3274 ya da IBM 5250 emülasyonu ile uygulama veri akışını ana bilgisayardan TESS (Teklogix Ekran Alt Sistemi) komutlarına dönüştürür. Bu sayfadaki parametrelerin bazıları ana bilgisayar ekranlarının TESS'ye dönüştürülmesini yönetir.

Is Host Fujitsu (Ana bilgisayar Fujitsu mu?)

Bu parametre **etkinleştirildiğinde** 9160 G2 mini denetleyici, ana bilgisayardan gelen verilerin bir Fujitsu ana bilgisayarına özgü komutlar gibi komutları içermesini bekler. Bu parametrenin etkinleştirilmesi standart IBM biçimlendirme kodlarının (alan başlangıcı, arabellekleri ayarlama vb.) Fujitsu ana bilgisayarlar tarafından kullanılan kodlarla değiştirilmesine neden olur.

Use International EBCDIC (Uluslararası EBCDIC'yi kullan)

Bu parametre **etkinleştirildiğinde** 9160 G2 mini denetleyici, ! ve] karakterlerinin yerini değiştirerek Uluslararası EBCDIC karakter setini kullanır.

Allow null character in fixed fields (Sabit alanlarda boş karaktere izin ver)

Bu parametre **etkinleştirildiğinde** 9160 G2 mini denetleyici, ters video gibi görsel video özelliklerine sahip alanlarda boşluklardaki boş karakterlere izin verir. 3274 ana bilgisayar emülasyonunda bu seçenek varsayılan olarak **devre dışıdır**.

23.4.1.2 TESS Options (TESS Seçenekleri)

TESS Options:	
Alarm:	<input type="checkbox"/>
Clear:	<input type="checkbox"/>
Passthru:	<input type="checkbox"/>
Procedures:	<input type="checkbox"/>
Local:	<input type="checkbox"/>
Host Print:	<input type="checkbox"/>
Remote Print:	<input type="checkbox"/>
Pages:	<input type="text" value="8"/> (Range 1..79)
Transmit Line:	<input type="text" value="0"/> (Range 0..24)
AIAG:	<input type="text" value="0"/> (Range 0..255)
Visible Match Character:	<input type="text" value="0"/> (Range 0..255)
Hidden Match character:	<input type="text" value="0"/> (Range 0..255)
Serial I/O:	<input type="text" value="0"/> (Range 0..255)
Print Line:	<input type="text" value="0"/> (Range 0..24)
Print Form Length:	<input type="text" value="0"/> (Range 0..24)
Barcode:	<input type="text" value="0"/> (Range 0..255)
Entry Line:	<input type="text" value="0"/> (Range 0..24)
Field Overhead:	<input type="text" value="5"/> (Range 0..80)
Command Region:	<input type="text" value="0"/> , <input type="text" value="0"/> , <input type="text" value="0"/> , <input type="text" value="0"/>

Alarm

Bu parametre **etkinleştirildiğinde** uygulama ekranının *Command Region* (Komut Bölgesi) parametresi tarafından belirlenen bir konumunda "ALARM" kelimesi görüntülendiğinde mobil bilgisayardan bip sesi duyulur (bkz. sayfa 268). "ALARM" kelimesi yalnızca görüntülenen bir alan olmalıdır.



Not: Bu parametrenin çalışması için Komut Bölgesi parametresinin etkinleştirilmesi gerekir.

Clear (Temizle)

Bu parametre **etkinleştirildiğinde** 9160 G2 mini denetleyici, boşluklarla dolu bir girdi alanı için boş bir girdi alanı oluşturur.

Bazı ana bilgisayar uygulamalarında, özellikle girdi alanları gibi alanları vurgulama işlemleri görüntülenen karakterlerin video özellikleri tarafından gerçekleştirilir. Örneğin, uygulama ekranı tüm girdi alanlarını ters videoyla tanımlayabilir ve alanı boşlukla doldurabilir. Bu özellik, ters videoyu destekleyen mobil bilgisayarlarda geçerlidir ancak özellik, tamamen boşluklardan oluştuğu için, ters videoyu desteklemeyen mobil bilgisayarlarda alanın görünmez olmasına yol açabilir.

Varsayılan olarak Psion Teklogix mobil bilgisayarlarda görüntülenen tüm boş girdi alanları, mobil bilgisayarın yapılandırmasında seçilen "girdi karakteri" ile vurgulanır.



Not: Bu işlem yalnızca ana bilgisayardan alınan ekranlarda gerçekleşir. Ana bilgisayara gönderilen veriler bu işlemde etkilenmez.

Passthru (Doğrudan Geçiş)

Bu parametre **etkinleştirildiğinde** 9160 G2, verilerin ana bilgisayar tarafından doğrudan RF mobil bilgisayarın seri bağlantı noktasına gönderilmesine olanak sağlar. Bu seçenek genellikle yazdırma işleminde kullanılır.

Ana Bilgisayar Ekranlarını Doğrudan Geçişe Hazırlama

Mobil bilgisayarın seri bağlantı noktasına gönderilecek olan ekranda, ikinci sütundan itibaren ilk satırda büyük harflerle **PASSTHRU** (Doğrudan Geçiş) yazmalıdır. Mobil bilgisayara gönderilecek gerçek veri ilk satırdan sonra herhangi bir yerde başlayabilir.

5250 veya 3274 emülasyonlarında, özellikler ekran arabelleğinde yer alır. 2. sütunla "PASSTHRU" (Doğrudan Geçiş) kelimesinin sonu arasındaki özellikler, sonraki karakterlerin hepsini bir sağa "kaydırır". Bu nedenle, gerekli özellikler ilk satırın ilk sütununda ("PASSTHRU" [Doğrudan Geçiş] kelimesinin önünde) yer almalıdır.

Örnek:

sütun: 1 2 3 4 5 6 7 8 9
satır 1: @ P A S S T H R U @
satır 2: @ P A R T : 1 2 3 4 5

@, bir özelliği işaret eder.

9160 G2, mobil bilgisayarın yazıcısına veri göndermeyi tamamladığında ana bilgisayara **ENTER** (GİRİŞ) anahtarı gönderir. Ana bilgisayar, bu mobil bilgisayara daha fazla ekran göndermeden önce (diğer PASSTHRU ekranları dahil) **ENTER** (GİRİŞ) anahtarını beklemelidir.



Not: Doğrudan geçiş için mobil bilgisayarlarda parametre ayarlama hakkında bilgi için ilgili mobil bilgisayarın Kullanım Kılavuzuna bakın.

Procedures (Prosedürler)

Bu parametre **etkinleştirildiğinde** ana bilgisayar, TESS prosedürlerini mobil bilgisayara 9160 G2 aracılığıyla gönderebilir. TESS prosedürü, TESS *execute procedure* (TESS çalıştırma prosedürü) komutu tarafından çalıştırılabilen bir TESS komutu grubudur.

Local (Yerel)

Bu parametre **etkinleştirildiğinde** 9160 G2, ana bilgisayarın mobil bilgisayarlarda yerel TESS prosedürleri olarak yüklenecek sayfalar sunmasına olanak sağlar.

Yerel prosedürler mobil bilgisayardaki bir menüden seçilir. Mobil bilgisayarlar bu prosedürleri çevrimdışı olduklarında gerçekleştirebilir. Mobil bilgisayarlar daha sonra çevrimiçi olduklarında bu fonksiyonların sonuçlarını ana bilgisayara gönderir.



Not: Yerel parametresinin çalışması için Prosedürler parametresinin de etkinleştirilmesi gerekir.

Host Print (Ana Bilgisayarla Yazdırma)

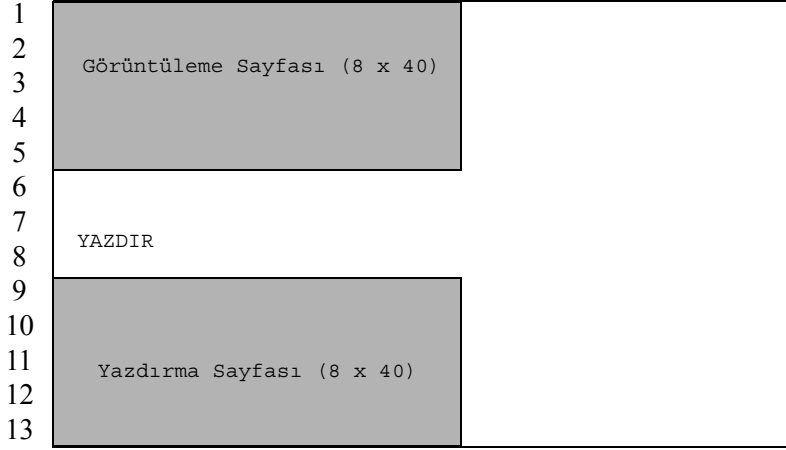
Bu parametre **etkinleştirildiğinde** ana bilgisayar mobil bilgisayar ekranına ekstra veri gönderebilir ve mobil bilgisayara bu veriyi yazdırması için talimat verebilir. Bu özellik, *Local Print* (Yerel Yazdırma) özelliğinin tam tersidir. Yerel Yazdırmada ilk yazdırma talebini mobil bilgisayar gönderir.

Yazıcıya gönderilen metin 24 x 80 uygulama ekranına göre biçimlendirilir. Ana bilgisayar, yazdırma işlemini başlatabilirse metin yazdırılır. 24 x 80 ekranda 13. satırın 2. sütunundan başlayarak büyük harflerle "PRINT" (YAZDIR) yazıldığında 9160 G2, ek metnin yazdırılacak bir sayfa olduğunu anlar. "PRINT" kelimesi *yalnızca görüntülenen* bir metin olarak tanımlanmalıdır.

Yazdırma sayfası mobil bilgisayarın görüntüleme sayfasının altında bulunur (aşağıdaki şekle bakın). Yazdırma sayfasının boyutu her zaman mobil bilgisayarın görüntüleme sayfasının boyutuyla aynıdır (mobil bilgisayar yapılandırılırken sayfa boyutunun 12 satırdan az olacak şekilde ayarlandığı düşünülür).

Host Print (Ana Bilgisayarla Yazdırma) **etkinleştirildiğinde** 9160 G2, uygulama ekranını ana bilgisayardan aldıktan sonra yazdırma sayfasını mobil bilgisayara gönderir.

Şekil 23.2 Yazdırma Sayfasını Gösteren Uygulama Ekranı



Notlar:

1. *Passthru (Doğrudan Geçiş) seçeneğinden farklı olarak Host Print (Ana Bilgisayarla Yazdırma) kullanılırken kaçış komutları yazıcıya gönderilemez.*
2. *Mobil bilgisayarın yazdırma desteği, TESS Features (TESS Özellikleri) menüsündeki Printer (Yazıcı) komutundan etkinleştirilmelidir. Daha fazla bilgi için ilgili mobil bilgisayara ait kullanım kılavuzuna bakın.*

Remote Print (Uzaktan Yazdırma)

Bu parametre **etkinleştirildiğinde** (mobil bilgisayardan “F17” işlev tuşunu ya da daha eski mobil bilgisayarlarda "PRINT" tuşunu göndererek) 9160 G2, mobil bilgisayar her istediğinde bir yazdırma sayfası gönderir. 9160 G2, işlev yanıtını ana bilgisayara geri gönderir.

Bu özellik, *Host Print* (Ana Bilgisayarla Yazdırma) özelliğinin tam tersidir. Ana Bilgisayarla Yazdırmada ilk yazdırma talebini ana bilgisayar gönderir.



Not: Mobil bilgisayarda yazdırma desteğinin etkinleştirilmesi gerekir. Daha fazla bilgi için ilgili mobil bilgisayara ait Kullanıcı Kılavuzuna bakın.

Pages (Sayfalar)

Bu parametre, mobil bilgisayarda saklanan ana bilgisayar ekran (ya da sayfa) sayısını (en fazla 79) belirler.

9160 G2, mobil bilgisayarın görüntülediği her ekran için bir veri sayfası saklama özelliğini kullanarak mobil bilgisayara veri aktarımını azaltır. 9160 G2, mobil bilgisayarda saklanan her sayfanın görüntüsünü alır. 9160 G2, bir uygulama ekranı aldıktan sonra ekranı saklanan sayfalardan biriyle eşlemeye çalışır. Mobil bilgisayarın belleğinde benzer bir sayfa varsa 9160 G2, mobil bilgisayardan sayfanın kopyasını yeniden görüntülemesini ister; yalnızca gerekli değişiklikler denetleyiciden gönderilir. Herhangi bir eşleşme bulunmazsa sayfanın tamamı telsiz bağlantısı aracılığıyla mobil bilgisayara gönderilir.



Not: Mobil bilgisayarda bu parametreye karşılık gelen bir parametre vardır ve kaydedilen sayfaların gerçek sayısı belirtilen iki değerden küçük olanıdır.

Transmit Line (Aktarma Satırı)

Bu özellik **etkinleştirildiğinde** operatörün *transmit-upon-entry* (girdi eklendiğinde aktar) alanına veri girmesiyle, mobil bilgisayarda düzenlenen tüm veriler otomatik olarak aktarılır.

Bu metin kutusunda belirtilen değer *transmit line* (aktarma satırı) olarak belirlenen ekran satırını gösterir. Aktarma satırındaki ya da aktarma satırının üzerindeki son girdi *transmit-upon-entry* (girdi eklendiğinde aktar) alanı olarak tanımlanır. Aktarma satırının altındaki satırlarda herhangi bir girdi alanı varsa hiçbir alan *transmit-upon-entry* (girdi eklendiğinde aktar) alanı olarak seçilmez.

Alana **0** (sıfır) değerinin yazılması özelliği devre dışı bırakır. **24** değeri, her uygulama ekranının *son* girdi alanını *transmit-upon-entry* (girdi eklendiğinde aktar) alanı olarak belirler.

AIAG

Bu parametre, barkod okuyuculardan gelen verileri otomatik olarak bulma ve doldurma özelliği sağlar. Mobil bilgisayara bir barkod verisi girildiğinde mobil bilgisayar, geçerli sayfada barkod verisini kabul edebilecek "AIAG" alanlarını arar. Uygulama programı tarafından "AIAG" alanına önceden yüklenen veri barkod verisinin kabul edilip edilmeyeceğini belirler.

9160 G2 mini denetleyicide, ana bilgisayarda ayarlanan "AIAG Alan Tanımlayıcı" ile eşleşecek **0 - 255** arası ondalık bir ASCII karakteri ayarlanır. Alana **0** değerinin yazılması özelliği devre dışı bırakır.

Önceden yüklenen verinin biçimi aşağıdaki gibidir:

`<mode> <AIAG prefix(data)>`

Komutta kullanılan mod karakteri çeşitli uygulama işlemleri için farklı çalışma modlarının kullanılmasına olanak sağlar. Otomatik bulma ve doldurma işlemi yalnızca barkod okuyuculardan alınan veriler için geçerlidir. Modların ve AIAG ön eklerinin açıklamaları için bkz. Tablo 23.1, sayfa 264. Bu modlar ana bilgisayarda ayarlanır.

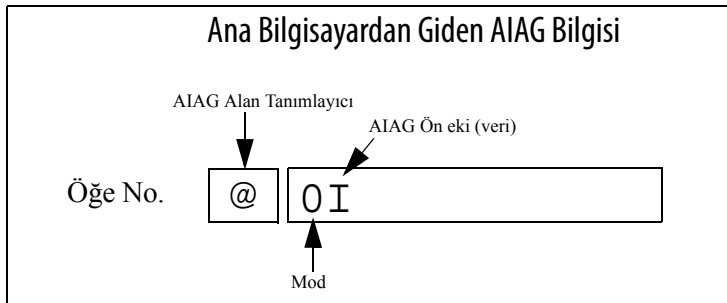
Tablo 23.1 Mod İşlevleri ve AIAG Ön Eki Açıklamaları

Mod	İşlev
0	Ön eki görüntüle, ana bilgisayara gönder.
1	Ön eki görüntüleme, ana bilgisayara gönder.
2	Ön eki görüntüle, ana bilgisayara gönderme.
3	Ön eki görüntüleme, ana bilgisayara gönderme.
+4	4 gruplu tüm AIAG alanları doluyken ana bilgisayara veri aktarımı sağlamak için yukarıdaki değerlere 4 ekleyin. Bu bit grubuna sahip başka alanlar da varsa ve bu alanlar operatör girdisiyle doldurulmuşsa İşlev 0 tuşuna "basılır".
+8	Önceden girilen verilerin üzerine yazmaya izin vermek için yukarıdaki değerlere 8 ekleyin.
+16	Arama ve doldurma işlevlerinde imleç konumu önceliğini belirtmek için yukarıdaki değerlere 16 ekleyin.
AIAG Ön eki (veri)	AIAG alanında eşleşecek metin.

Örnek:

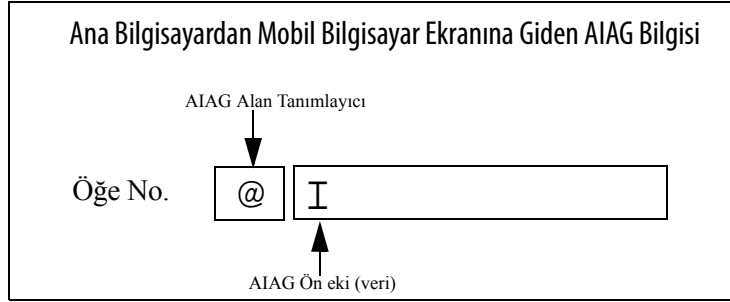
Aşağıdaki örnek ekranda yer alan bilgiler ana bilgisayarda tanımlanmış ve **oradan** gönderilmiştir. Ekran “AIAG Identifier” (AIAG Tanımlayıcı: bu alanın bir AIAG alanı olduğunu belirten etiket) ve modu içerir. Bu örnekte Mode (Mod) 0 ve sondaki "AIAG Prefix" (AIAG Ön Eki) I olarak gösterilmiştir.

Şekil 23.3 Ana Bilgisayardan Gönderilen AIAG Alanı



Bilgi, mobil bilgisayar ekranına ulaştığında "AIAG Tanımlayıcı" kullanılarak taranan bilgi için uygun AIAG alanı belirlenir. Mod 0 ana bilgisayarda ayarlandığından "AIAG Ön Eki" (I) mobil bilgisayar ekranında görüntülenir. Bu ekran tamamlandığında ön ek ana bilgisayara geri gönderilir.

Şekil 23.4 Mobil Bilgisayara Gönderilen AIAG Alanı



Visible Match Character (Görünür Eşleşme Karakteri)

Bir girdi alanından hemen önce özel bir ASCII karakteri girildiğinde uygulama programı "eşleşme alanını" girdi alanından ayırt eder. Örneğin ">" açılı ayracının görünür eşleşme alanları için tanımlandığını varsayalım.

Girdi alanından hemen önce ">" simgesini koymak, bu alanı aşağıda gösterildiği gibi bir eşleşme alanı olarak tanımlar.

Part #> _____

Bu parametrenin aralığı (0 - 255) ASCII karakterlerinin ondalık değerini temsil eder. Alana 0 değerinin yazılması özelliği devre dışı bırakır. 9160 G2'de girilen ASCII ondalık değeri, uygulama programı tarafından ayarlanan değerle aynı olmalıdır.

Visible Match (Görünür Eşleşme) özelliğini kullanmak için ana bilgisayar bir girdi eşleşme alanına önceden veri yükler; bu veri mobil bilgisayar ekranında görünür. Mobil bilgisayara gönderilen önceden yüklü veriler tam karakterlerden, özel eşleşme karakterlerinden ya da ikisinin kombinasyonundan oluşabilir. Psion Teklogix mobil bilgisayarların tanıdığı eşleşme karakterleri için bkz. Tablo 23.2.

Bir girdi önceden yüklenen veriyle eşleşmezse girdi görüntülenir, mobil bilgisayardan bip sesi duyulur ve imleç eşleşme alanındaki ilk konuma gider. Operatör, eşleşme alanına başka bir girdi yazabilir ya da imleci yeni bir alana taşıyabilir. Eşleşme alanına bir girdi yazıldığında (önceden yüklenen veriyle eşleşmeyen bir girdi dahil) bu girdi bir sonraki aktarımda mobil bilgisayarın düzenlenen verilerinin bir parçası olarak ana bilgisayara gönderilir.

Tablo 23.2 Eşleşme Karakterleri

Karakter	Açıklama
#	Sayı eşleştirir.
&	Harf eşleştirir (küçük ya da büyük harf).
^	Büyük harf eşleştirir.
_	Küçük harf eşleştirir.
	Alfanümerik karakter eşleştirir.
"	Harf, sayı ya da boşluk eşleştirir.
?	Noktalama işareti eşleştirir.
'	Herhangi bir karakter eşleştirir.
:	Alandaki tüm karakter konumlarını bir önceki karakterle eşleştirir.
;	Geri kalan karakterleri (alanda kalan karakterlerin olması şart değil) bir önceki karakterle eşleştirir.

Örnek:

Parça numarası içeren bir girdi alanını önceden yüklemek istediğinizi varsayalım. Parça numarası biliniyorsa bu parça numarasını alana önceden yükleyebilirsiniz. Daha fazla esneklik gerekiyorsa parça numaraları her zaman iki alfabetik karakterle başlayıp tire (-) ve dört rakamla devam eder. Alandaki eşleşen satır şu şekilde görünür: **&&-####** .

Hidden Match Character (Gizli Eşleşme Karakteri)

“Visible match” (görünür eşleşme) alanındaki verilerin aksine “hidden match” (gizli eşleşme) alanındaki önceden yüklenmiş veriler mobil bilgisayarda *görüntülenmez*.



Not: Alan eşleme hakkında ayrıntılı bilgi için bkz. “Visible Match Character (Görünür Eşleşme Karakteri)”, sayfa 265.

Bu parametrenin aralığı (**0 - 255**) ASCII karakterlerinin ondalık değerini temsil eder. Alana **0** değerinin yazılması özelliği devre dışı bırakır. 9160 G2'de girilen ASCII ondalık değeri, uygulama programı tarafından ayarlanan değerle aynı olmalıdır.

Serial I/O (Seri G/Ç)

Serial I/O (Seri G/Ç) alanları, seri bağlantı noktalarından giriş ve çıkış kabul eden özel girdi alanları ve sabit alanlardır. Uygulama programı *Serial I/O* (Seri G/Ç) alanının önüne özel bir karakter koyarak bu alanı ayırt eder.

Bu karakter, sabit bir alanın önünde yer aldığı veriler mobil bilgisayarın seri bağlantı noktasına gönderilir. Karakter, girdi alanının önünde yer aldığı alana mobil bilgisayarın seri bağlantı noktasından veri gönderilir.

Bu parametrenin aralığı **(0 - 255)** ASCII karakterlerinin ondalık değerini temsil eder. Alana **0** (sıfır) değerinin yazılması özelliği devre dışı bırakır.

Print Line (Yazdırma Satırı)

Bu parametre uygulama ekranındaki yazdırma sayfasının başlangıç satırı numarasını girmenizi sağlar (ayrıca bkz. *Entry Line [Girdi Satırı]*). **1- 24** arasındaki değerler görüntüleme sayfasının yazdırılmasını sağlar, **0** (sıfır) bu özelliği devre dışı bırakır.

Print Form Length (Yazdırma Biçimi Uzunluğu)

Bu parametre yazıcının biçim uzunluğunu satır cinsinden ayarlar. Değer aralığı **0 - 24**'tür.

Barcode (Barkod)

Barcode-input-only (yalnızca barkod girişi) alanları yalnızca barkod okuyuculardan gelen girişleri kabul eden özel girdi alanlarıdır. Uygulama programı *barcode-input-only* (yalnızca barkod girişi) alanının önüne özel bir karakter koyarak bu alanı ayırt eder.

Bu parametrenin aralığı **(0 - 255)** ASCII karakterlerinin ondalık değerini temsil eder. Alana **0** (sıfır) değerinin yazılması özelliği devre dışı bırakır.

Entry Line (Girdi Satırı)

Bu parametre, ekranın sol üst kısmında herhangi bir girdi alanı yoksa ve bir girdi alanı ilk satırda veya bu satırın altındaysa gösterilen ilk satırın numarasını içerir.

Entry Line (Girdi Satırı) parametresi ana bilgisayar ekranında otomatik ofset sağlar; böylece mobil bilgisayar tarafından görüntülenen alan, normalde sınırların dışında olacak bir girdi alanını içerir. Bazı Psion Teklogix mobil bilgisayarları, ekran boyutları daha küçük olduğundan uygulamanın yalnızca sol üst köşesini görüntüler.

Field Overhead (Alan Ek Yüğü)

Bu parametre iki *sabit* alan arasında izin verilen maksimum karakter sayısını içerir. Bu parametre, 9160 G2'nin bu alanları tek bir alanda birleştirmesini sağlar.

9160 G2 bazen iki bitişik sabit alanı birleştirdikten sonra tek bir alan olarak gönderebilir. Bu sayede telsiz bağlantısı üzerindeki ek yük azalmış olur.

Örneğin, iki alan arasında 4 karakter varsa ve bu parametre "5" ise bu alanlar tek bir alanda birleştirilebilir.

Command Region (Komut Bölgesi)

Bu parametre, 9160 G2'nin kayıtlı komutlar için denetleyeceği ana bilgisayar ekranı bölgesini tanımlar.

Command Region (Komut Bölgesi) metin kutusundaki dört sayı, komut bölgesinin sol üst ve sağ alt köşesindeki satır ve sütun adreslerini temsil eder. Her çiftteki ilk metin kutusu sıra numarasını, ikinci metin kutusu sütun numarasını içerir. Sıra değerlerinin aralığı **0 - 24**; sütun değerlerinin ise **0 - 80**'dir.

Örneğin, ana bilgisayar ekranının son iki satırını komut bölgesi olarak tanımlamak için *23, 1* ve *24, 80* değerlerini girin.

Şu an desteklenen tek komut *ALARM*'dır (Bu komutla ilgili ayrıntılar için bkz. sayfa 259). "ALARM" kelimesi komut bölgesinin herhangi bir yerine yazıldığında 9160 G2, mobil bilgisayara bir TESS *bip* komutu gönderir.

23.4.1.3 Telnet Protokol Seçenekleri

Telnet Protocol Options:
Terminal Type: IBM-3278-2
Host Port: 23 (Range 1..32767)
Maximum Sessions per Terminal: 4 (Range 1..127)
First Local Terminal Port: 10000 (Range 1..32767)
Local IP Address to Bind: 0.0.0.0
First Terminal Listen Port: 0 (Range 0..32767)
Actively Negotiate with Host: ☐
Configure LU Names: ☐ **Configure**
LU Name Prefix:
Send IAC Interrupt Process as a System Request: ☐
Send IAC Break as an Attention Key: ☐
Auto-telnet: DISABLE
Auto-telnet Host:
Auto-telnet without User Action: ☒

Terminal Type (Terminal Türü)

Bu parametre 9160 G2 tarafından bu ana bilgisayar için emüle edilecek mobil bilgisayar türünü seçmenizi sağlar. Şu anda *3274 Emülasyonu* için mevcut olan mobil bilgisayar seçenekleri şunlardır: **IBM 3278-2** ve **IBM 3278-2-E**.

Host Port (Ana Bilgisayar Bağlantı Noktası)

Bu parametre, seçili *3274 Emülasyonu* ana bilgisayar bağlantısı için bir ana bilgisayar bağlantı noktası değeri girmenize olanak sağlar. Varsayılan değer **23**'tür.

Maximum Sessions per Terminal (Terminal Başına Maksimum Oturum Sayısı)

Bu oturum, her bir mobil bilgisayardan çıkmasına izin verilen maksimum telnet oturum sayısını içerir. Varsayılan değer **4**, değer aralığı **1 - 127**'dir.

First Local Terminal Port (İlk Yerel Terminal Bağlantı Noktası)

Bu parametre, ilk mobil bilgisayarın giden telnet oturumlarına bağlanacağı yerel bağlantı noktası numarasını içerir. Varsayılan değer **10.000**'dir.

Local IP Address to Bind (Bağlanılacak Yerel IP Adresi)

Bu parametre ilk mobil bilgisayarın giden telnet oturumlarına bağlanacağı, 9160 G2'de yer alan ağ adaptörü IP adresini içerir.

First Terminal Listen Port (İlk Terminal Dinleme Bağlantı Noktası)

Bu parametre 9160 G2'nin mobil bilgisayarlara yapılacak olan telnet bağlantı isteklerini dinleyeceği ilk bağlantı noktası numarasını belirtir. Bu parametreyi **etkinleştirmek** için minimum değer **1024** olmalıdır. Dinleme bağlantı noktasını **devre dışı bırakmak** için değer **0** olmalıdır.

Varsayılan değer **0**'dır (devre dışı).

Actively Negotiate with Host (Ana Bilgisayarla Etkin Biçimde Görüşme)

Bu parametre etkinleştirildiğinde 9160 G2, telnet bağlantısının kurulması sırasında ana bilgisayarla görüşmeye başlar. Pek çok ana bilgisayar için önerilmez.

Configure LU Names (LU Adlarını Yapılandırma)

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

<input type="checkbox"/> Edit	Terminal Number	LU Name
<input type="checkbox"/> [Edit]	1	ABC
<input type="checkbox"/> [Edit]	5	THING

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

Yapılandırılan her mobil bilgisayar için bir LU Adı gereklidir. Bu sayfa LU Adları atamanızı sağlar (aşağıdaki *LU Name Prefix* [LU Adı Ön Eki] bölümüne de bakın). LU Adı benzersiz olmalıdır ve mobil bilgisayarın Terminal Numarasıyla ilişkili olmalıdır. LU Adları maksimum 10 alfanümerik karakterden oluşabilir. Küçük harfle yazılan karakterler otomatik olarak büyük harfe dönüştürülür.

LU Name Prefix (LU Adı Ön Eki)

Bir mobil bilgisayar için herhangi bir LU Adı belirlenmemişse 9160 G2, tam bir LU Adı oluşturmak için Terminal Numarasını (beş rakam, gerektiğinde başa sıfır koyarak) LU Ön Ekine ekleyecektir.

Send IAC Interrupt Process as a System Request (Sistem İsteği Olarak IAC İşlemi Durdur İsteği Gönderme)

Bu parametre etkinleştirildiğinde 9160 G2, 3274 Sistem İsteği olarak ana bilgisayara IAC Interrupt Process (IAC İşlemi Durdur) isteği gönderir.

Send IAC Break as an Attention Key (Dikkat Tuşu Olarak IAC Break Gönderme)

Bu parametre etkinleştirildiğinde 9160 G2, 3274 Dikkat tuşu olarak ana bilgisayara IAC Break isteği gönderir.

Auto-telnet (Otomatik telnet)

Bu parametre, telnet oturumlarının mobil bilgisayarlardan bu ana bilgisayara olan otomatik bağlantısını devre dışı bırakmanızı ya da etkinleştirmenizi sağlar.

Sunulan seçenekler şunlardır: **Disable** (Devre dışı bırak) ve **Auto-telnet** (Otomatik telnet). Varsayılan değer **Disable** (Devre dışı bırak) seçeneğidir.

Auto-telnet (Otomatik telnet) **devre dışı bırakıldığında** mobil bilgisayarlardan ana bilgisayara doğru kurulan telnet oturum bağlantılarının mobil bilgisayarlardan manuel olarak başlatılması gerekir.

Auto-telnet (Otomatik telnet) **etkinleştirildiğinde** 9160 G2, terminal numaraları bu ana bilgisayarla eşleşen her mobil bilgisayardan bir telnet oturumu başlatır. Her mobil bilgisayardan ana bilgisayara ek telnet oturumu başlatılabilir ancak bu oturumların manuel olarak başlatılması gerekir.

Auto-telnet (Otomatik telnet) **etkinleştirildiğinde** 9160 G2, oturum açıldığında ve kapatıldığında otomatik olarak ana bilgisayara erişir.



Not: Otomatik telnet oturumları yalnızca "çevrimiçi" (açık ve Psion Teklogix RF ağında sorunsuz biçimde çalışan) mobil bilgisayarlar için başlatılır.

Auto-telnet Host (Otomatik Telnet Ana Bilgisayarı)

Bu parametre 9160 G2'nin otomatik telnet oturumu bağlantısı oluşturduğu ana bilgisayarın adını ya da IP adresini içerir.



Not: Bu metin kutusunda yer alan ana bilgisayar adı 9160 G2 tarafından "çözümünebilir" olmalıdır; yani 9160 G2'nin ana bilgisayar adı için bir IP adresi alınabilmesi gerekir. Örneğin, ana bilgisayar adı 9160 G2 ana bilgisayar tablosundaki bir girdiye karşılık gelebilir ya da 9160 G2 bir etki alanı adı sunucusu sorgulayabilir.

Mobil bilgisayarın TCP> isteminde kullanılabilen her ana bilgisayar adı burada da kullanılabilir.

Auto-telnet Without User Action (Kullanıcı Etkinliği Olmadan Otomatik Telnet)

Bu parametre etkinleştirildiğinde kullanıcının [ENTER] tuşuna basmasına gerek kalmadan denetleyici başlatılan her mobil bilgisayar için hemen ana bilgisayarda bir bağlantı açar.

23.4.1.4 İşlev Tuşu Eşlemeleri

Function Key Mappings:

F1:	<input type="text" value="F1"/>	F14:	<input type="text" value="PA2"/>	F27:	<input type="text" value="F13"/>
F2:	<input type="text" value="F2"/>	F15:	<input type="text" value="PA3"/>	F28:	<input type="text" value="F14"/>
F3:	<input type="text" value="F3"/>	F16:	<input type="text" value="CLEAR"/>	F29:	<input type="text" value="F15"/>
F4:	<input type="text" value="F4"/>	F17:	<input type="text" value="F17"/>	F30:	<input type="text" value="SESS"/>
F5:	<input type="text" value="F5"/>	F18:	<input type="text" value="F18"/>	F31:	<input type="text" value="F16"/>
F6:	<input type="text" value="F6"/>	F19:	<input type="text" value="F19"/>	F32:	<input type="text" value="ENTER"/>
F7:	<input type="text" value="F7"/>	F20:	<input type="text" value="F20"/>	F33:	<input type="text" value="ENTER"/>
F8:	<input type="text" value="F8"/>	F21:	<input type="text" value="F21"/>	F34:	<input type="text" value="ENTER"/>
F9:	<input type="text" value="F9"/>	F22:	<input type="text" value="F22"/>	F35:	<input type="text" value="ENTER"/>
F10:	<input type="text" value="F10"/>	F23:	<input type="text" value="F23"/>	F36:	<input type="text" value="ENTER"/>
F11:	<input type="text" value="F11"/>	F24:	<input type="text" value="F24"/>	F37:	<input type="text" value="ENTER"/>
F12:	<input type="text" value="F12"/>	F25:	<input type="text" value="SYSREQ"/>	F38:	<input type="text" value="ENTER"/>
F13:	<input type="text" value="PA1"/>	F26:	<input type="text" value="ATTN"/>	F39:	<input type="text" value="ENTER"/>

n İşlev Tuşu

Function Key (İşlev Tuşu) parametresi, mobil bilgisayarınızda bir işlev tuşuna bastığınızda ana bilgisayara gönderilecek kodu seçmenize olanak sağlar. Her işlev tuşu aynı kod aralığından seçilebilir ancak her işlev tuşunun farklı bir varsayılan kodu vardır. Varsayılan değerler bu sayfada gösterilmiştir.

23.4.2 5250 Emülasyonu

23.4.2.1 Emulation Options (Emülasyon Seçenekleri)

5250 Emulation Options:
Write Error Code: Advisory text ▼
Use International EBCDIC: ☐
Allow null character in fixed fields: ☐

IBM 5250 ya da IBM 3274 emülasyonda, 9160 G2 mini denetleyici uygulama veri akışını ana bilgisayardan TESS (Teklogix Ekran Alt Sistemi) komutlarına dönüştürür. Bu sayfadaki parametrelerin bazıları ana bilgisayar ekranlarının TESS'ye dönüştürülmesini yönetir.

Write Error Code (Hata Kodu Yaz)

Bu alanda *advisory text* (tavsiye metni) seçildiğinde 9160 G2, hata kodlarını tavsiye metni olarak mobil bilgisayar ekranına gönderir. Hata kodları ekranın alt kısmında görünür. *Screen text* (ekran metni) seçildiğinde 9160 G2, hata kodlarını normal ekran metni olarak gönderir.

Use International EBCDIC (Uluslararası EBCDIC'yi kullan)

Bu parametre **etkinleştirildiğinde** 9160 G2, ! ve] karakterlerinin EBCDIC karakter tablosunda yerini değiştirir.

Allow null character in fixed fields (Sabit alanlarda boş karaktere izin ver)

Bu parametre **etkinleştirildiğinde** 9160 G2 mini denetleyici, ters video gibi görsel video özelliklerine sahip alanlarda boşluklardaki boş karakterlere izin verir. 5250 ana bilgisayar emülasyonunda bu seçenek varsayılan olarak **etkindir**.

23.4.2.2 TESS Options (TESS Seçenekleri)

TESS Options:	
Field Underline Remapping:	None ▼
Alarm:	<input type="checkbox"/>
Clear:	<input type="checkbox"/>
Passthru:	<input type="checkbox"/>
Procedures:	<input type="checkbox"/>
Local:	<input type="checkbox"/>
Host Print:	<input type="checkbox"/>
Remote Print:	<input type="checkbox"/>
Pages:	8 (Range 1..79)
Transmit Line:	0 (Range 0..24)
AIAG:	0 (Range 0..255)
Visible Match Character:	0 (Range 0..255)
Hidden Match character:	0 (Range 0..255)
Serial I/O:	0 (Range 0..255)
Print Line:	0 (Range 0..24)
Print Form Length:	0 (Range 0..24)
Barcode:	0 (Range 0..255)
Entry Line:	0 (Range 0..24)
Field Overhead:	5 (Range 0..80)
Command Region:	0 , 0 , 0 , 0

Field Underline Remapping (Alan Vurgusunu Yeniden Ayarlama)

Girdi alanlarını vurgulamak için, görüntülenen karakterlerin video özelliklerini değiştirme seçeneğiniz vardır. Bu seçenekler şunlardır: *None* (Yok), *Blink* (Yanıp Sönen), *Bold* (Kalın) ve *Reverse* (Ters).

Alarm

Bu parametre **etkinleştirildiğinde** uygulama ekranının *Command Region* (Komut Bölgesi) parametresi tarafından belirlenen bir konumunda "ALARM" kelimesi (büyük harfle) görüntülendiğinde mobil bilgisayardan bip sesi duyulur (bkz. sayfa 284). "ALARM" kelimesi yalnızca görüntülenen bir alan olmalıdır.



Not: Bu parametrenin çalışması için Komut Bölgesi parametresinin etkinleştirilmesi gerekir.

Clear (Temizle)

Bu parametre **etkinleştirildiğinde** 9160 G2 mini denetleyici, boşluklarla dolu bir girdi alanı için *boş* bir girdi alanı oluşturur.

Bazı ana bilgisayar uygulamalarında, özellikle girdi alanları gibi alanları vurgulama işlemleri görüntülenen karakterlerin video özellikleri tarafından gerçekleştirilir. Örneğin, uygulama ekranı tüm girdi alanlarını ters videoyla tanımlayabilir ve alanı boşlukla doldurabilir. Bu özellik, ters videoyu destekleyen mobil bilgisayarlarda geçerlidir ancak özellik, tamamen boşluklardan oluştuğu için, ters videoyu desteklemeyen mobil bilgisayarlarda alanın görünmez olmasına yol açabilir.

Varsayılan olarak Psion Teklogix mobil bilgisayarlarda görüntülenen tüm boş girdi alanları, mobil bilgisayarın yapılandırmasında seçilen "girdi karakteri" ile vurgulanır. *Clear* (Temizle) özelliği boşluklarla dolu bir girdi alanı yerine boş bir girdi alanı oluşturur.



Not: Bu işlem yalnızca ana bilgisayardan alınan ekranlarda gerçekleşir. Ana bilgisayara gönderilen veriler bu işlemde etkilenmez.

Passthru (Doğrudan Geçiş)

Bu parametre **etkinleştirildiğinde** 9160 G2, verilerin ana bilgisayar tarafından doğrudan RF mobil bilgisayarın seri bağlantı noktasına gönderilmesine olanak sağlar. Bu seçenek genellikle yazdırma işleminde kullanılır.

Ana Bilgisayar Ekranlarını Doğrudan Geçişe Hazırlama

Mobil bilgisayar seri bağlantı noktasına gönderilecek olan ekranda, ikinci sütundan itibaren ilk satırda büyük harflerle "**PASSTHRU**" (Doğrudan Geçiş) yazmalıdır. Mobil bilgisayara gönderilecek gerçek veri ilk satırdan sonra herhangi bir yerde başlayabilir.

5250 veya 3274 emülasyonlarında, özellikler ekran arabelleğinde yer alır. 2. sütunla "PASSTHRU" (Doğrudan Geçiş) kelimesinin sonu arasındaki özellikler, sonraki karakterlerin hepsini bir sağa kaydırır. Bu nedenle, gerekli özellikler ilk satırın ilk sütununda ("PASSTHRU" [Doğrudan Geçiş] kelimesinin önünde) yer almalıdır.

Örnek:

sütun: 1 2 3 4 5 6 7 8 9
satır 1: @ P A S S T H R U @
satır 2: @ P A R T : 1 2 3 4 5

Şu simge bir özelliği işaret eder: @.

9160 G2, mobil bilgisayarın yazıcısına veri göndermeyi tamamladığında ana bilgisayara "ENTER" (GİRİŞ) anahtarı gönderir. Ana bilgisayar, bu mobil bilgisayara daha fazla ekran göndermeden önce (diğer "PASSTHRU" ekranları dahil) "ENTER" (GİRİŞ) anahtarını beklemelidir.



Not: Doğrudan geçiş için mobil bilgisayarlarda parametre ayarlama hakkında bilgi için ilgili mobil bilgisayarın Kullanım Kılavuzuna bakın.

Procedures (Prosedürler)

Bu parametre **etkinleştirildiğinde** ana bilgisayar, TESS prosedürlerini mobil bilgisayara 9160 G2 aracılığıyla gönderebilir. TESS prosedürü, TESS *execute procedure* (TESS çalıştırma prosedürü) komutu tarafından çalıştırılabilen bir TESS komutu grubudur.

Local (Yerel)

Bu parametre **etkinleştirildiğinde** 9160 G2, ana bilgisayarın mobil bilgisayarlarda yerel TESS prosedürleri olarak yüklenecek sayfalar sunmasına olanak sağlar.

Yerel prosedürler mobil bilgisayardaki bir menüden seçilir. Mobil bilgisayarlar bu prosedürleri çevrimdışı olduklarında gerçekleştirebilir. Mobil bilgisayarlar daha sonra çevrimiçi olduklarında bu fonksiyonların sonuçlarını ana bilgisayara gönderir.



Not: Yerel parametresinin çalışması için Prosedürler parametresinin de etkinleştirilmesi gerekir.

Host Print (Ana Bilgisayarla Yazdırma)

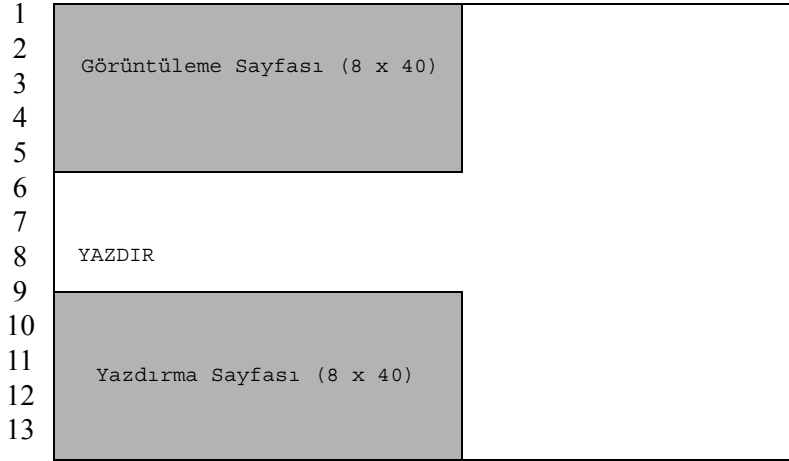
Bu parametre **etkinleştirildiğinde** ana bilgisayar mobil bilgisayar ekranına ekstra veri gönderebilir ve mobil bilgisayara bu veriyi yazdırması için talimat verebilir. Bu özellik, *Local Print* (Yerel Yazdırma) özelliğinin tam tersidir. Yerel Yazdırmada ilk yazdırma talebini mobil bilgisayar gönderir.

Yazıcıya gönderilen metin 24 x 80 uygulama ekranına göre biçimlendirilir. Ana bilgisayar, yazdırma işlemini başlatabilirse metin yazdırılır. 24 x 80 ekranda 13. satırın 2. sütunundan başlayarak büyük harflerle "PRINT" (YAZDIR) yazıldığında 9160 G2, ek metnin yazdırılacak bir sayfa olduğunu anlar. "PRINT" kelimesi *yalnızca görüntülenen* bir metin olarak tanımlanmalıdır.

Yazdırma sayfası mobil bilgisayarın görüntüleme sayfasının altında bulunur (Bkz. Şekil 23.5, sayfa 278). Yazdırma sayfasının boyutu her zaman mobil bilgisayarın görüntüleme sayfasının boyutuyla aynıdır (mobil bilgisayar yapılandırılırken sayfa boyutunun 12 satırdan az olacak şekilde ayarlandığı düşünülür).

Host Print (Ana Bilgisayarla Yazdırma) **etkinleştirildiğinde** 9160 G2, uygulama ekranını ana bilgisayardan aldıktan sonra yazdırma sayfasını mobil bilgisayara gönderir.

Şekil 23.5 Yazdırma Sayfasını Gösteren Uygulama Ekranı



Notlar:

1. *Passthru* (Doğrudan Geçiş) seçeneğinden farklı olarak *Host Print* (Ana Bilgisayarla Yazdırma) kullanılırken kaçış komutları yazıcıya gönderilemez.
2. Mobil bilgisayarın yazdırma desteği, *TESS Features* (TESS Özellikleri) menüsündeki *Printer* (Yazıcı) komutundan etkinleştirilmelidir. Daha fazla bilgi için ilgili mobil bilgisayara ait kullanım kılavuzuna bakın.

Remote Print (Uzaktan Yazdırma)

Bu parametre **etkinleştirildiğinde** (mobil bilgisayardan “F17” işlev tuşunu ya da daha eski mobil bilgisayarlarda "PRINT" tuşunu göndererek) 9160 G2, mobil bilgisayar her istediğinde bir yazdırma sayfası gönderir. 9160 G2, işlev yanıtını ana bilgisayara geri gönderir.

Bu özellik, *Host Print* (Ana Bilgisayarla Yazdırma) özelliğinin tam tersidir. Ana Bilgisayarla Yazdırmada ilk yazdırma talebini ana bilgisayar gönderir.



Not: Mobil bilgisayar seviyesinde yazdırma desteğinin etkinleştirilmesi gerekir. Daha fazla bilgi için ilgili mobil bilgisayara ait Kullanıcı Kılavuzuna bakın.

Pages (Sayfalar)

Bu parametre, mobil bilgisayarda saklanan ana bilgisayar ekran (ya da sayfa) sayısını (en fazla 79) belirler.

9160 G2, mobil bilgisayarın görüntülediği her ekran için bir veri sayfası saklama özelliğini kullanarak mobil bilgisayara veri aktarımını azaltır. 9160 G2, mobil bilgisayarda saklanan her sayfanın görüntüsünü alır. 9160 G2, bir uygulama ekranı aldıktan sonra ekranı saklanan sayfalardan biriyle eşlemeye çalışır.

Mobil bilgisayarın belleğinde benzer bir sayfa varsa 9160 G2, mobil bilgisayardan sayfanın kopyasını yeniden görüntülemesini ister; yalnızca gerekli değişiklikler denetleyiciden gönderilir. Herhangi bir eşleşme bulunmazsa sayfanın tamamı telsiz bağlantısı aracılığıyla mobil bilgisayara gönderilir.



Not: Mobil bilgisayarda bu parametreye karşılık gelen bir parametre vardır ve kaydedilen sayfaların gerçek sayısı belirtilen iki değerden küçük olanıdır.

Transmit Line (Aktarma Satırı)

Bu özellik **etkinleştirildiğinde** operatörün *transmit-upon-entry* (girdi eklendiğinde aktar) alanına veri girmesiyle, mobil bilgisayarda düzenlenen tüm veriler otomatik olarak aktarılacaktır.

Bu metin kutusunda belirtilen değer *transmit line* (aktarma satırı) olarak belirlenen ekran satırını gösterir. Aktarma satırındaki ya da aktarma satırının üzerindeki son girdi *transmit-upon-entry* (girdi eklendiğinde aktar) alanı olarak tanımlanır. Aktarma satırının altındaki satırlarda herhangi bir girdi alanı varsa hiçbir alan *transmit-upon-entry* (girdi eklendiğinde aktar) alanı olarak seçilmez.

Alana 0 (sıfır) değerinin yazılması özelliği devre dışı bırakır. 24 değeri, her uygulama ekranının son girdi alanının *transmit-upon-entry* (girdi eklendiğinde aktar) alanı olarak tanımlanmasına neden olur.

AIAG

Bu parametre, barkod okuyuculardan gelen verileri otomatik olarak bulma ve doldurma özelliği sağlar. Mobil bilgisayara bir barkod verisi girildiğinde mobil bilgisayar, geçerli sayfada barkod verisini kabul edebilecek “AIAG” alanlarını arar. Uygulama programı tarafından “AIAG” alanına önceden yüklenen veri barkod verisinin kabul edilip edilmeyeceğini belirler. 9160 G2 mini denetleyicide, ana bilgisayarda ayarlanan "AIAG Alan Tanımlayıcı" ile eşleşecek 0 - 127 arası ondalık bir ASCII karakteri ayarlanır. Alana 0 değerinin yazılması özelliği devre dışı bırakır.

Önceden yüklenen verinin biçimi aşağıdaki gibidir:

<mode> <AIAG prefix(data)>

Komutta kullanılan mod karakteri çeşitli uygulama işlemleri için farklı çalışma modlarının kullanılmasına olanak sağlar. Otomatik bulma ve doldurma işlemi yalnızca barkod okuyuculardan alınan veriler için geçerlidir. Modların ve AIAG ön eklerinin açıklamaları aşağıdaki tabloda listelenmiştir. Bu modlar ana bilgisayarda ayarlanır.

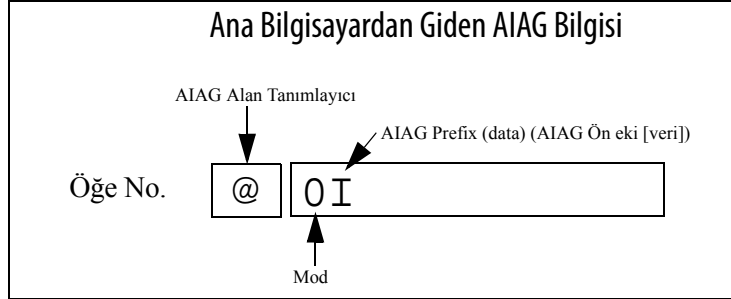
Tablo 23.3 Mod İşlevleri ve AIAG Ön Eki Açıklamaları

Mod	İşlev
0	Ön eki görüntüle, ana bilgisayara gönder.
1	Ön eki görüntüleme, ana bilgisayara gönder.
2	Ön eki görüntüle, ana bilgisayara gönderme.
3	Ön eki görüntüleme, ana bilgisayara gönderme.
+4	4 gruplu tüm AIAG alanları doluyken ana bilgisayara veri aktarımı sağlamak için yukarıdaki değerlere 4 ekleyin. Bu bit grubuna sahip başka alanlar da varsa ve bu alanlar operatör girdisiyle doldurulmuşsa İşlev 0 tuşuna "basılır".
+8	Önceden girilen verilerin üzerine yazmaya izin vermek için yukarıdaki değerlere 8 ekleyin.
+16	Arama ve doldurma işlevlerinde imleç konumu önceliğini belirtmek için yukarıdaki değerlere 16 ekleyin.
AIAG Prefix (data) (AIAG Ön eki [veri])	AIAG alanında eşleşecek metin.

Örnek:

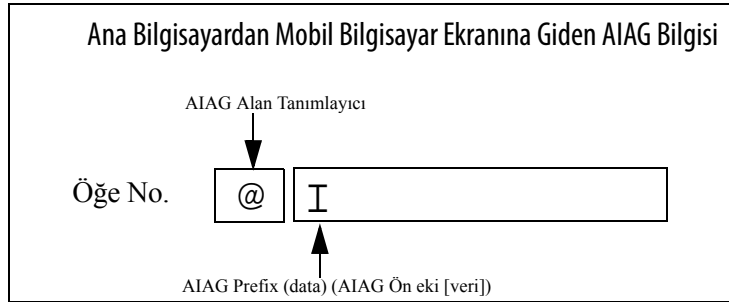
Aşağıdaki örnek ekranda yer alan bilgiler ana bilgisayarda tanımlanmış ve **oradan** gönderilmiştir. Ekran "AIAG Identifier" (AIAG Tanımlayıcı: bu alanın bir AIAG alanı olduğunu belirten etiket) ve modu içerir. Bu örnekte Mode (Mod) 0 ve sondaki "AIAG Prefix" (AIAG Ön Eki) I olarak gösterilmiştir.

Şekil 23.6 Ana Bilgisayardan Gönderilen AIAG Alanı



Bilgi, mobil bilgisayar ekranına ulaştığında "AIAG Tanımlayıcı" kullanılarak taranan bilgi için uygun AIAG alanı belirlenir. Mod 0 ana bilgisayarda ayarlandığından "AIAG Prefix" (AIAG Ön eki) (I) mobil bilgisayar ekranında görüntülenir. Bu ekran tamamlandığında ön ek ana bilgisayara geri gönderilir.

Şekil 23.7 Mobil Bilgisayara Gönderilen AIAG Alanı



Visible Match Character (Görünür Eşleşme Karakteri)

Bir girdi alanından hemen önce özel bir ASCII karakteri girildiğinde uygulama programı "eşleşme alanını" girdi alanından ayırt eder. Örneğin ">" açılı ayarının görünür eşleşme alanları için tanımlandığını varsayalım. Girdi alanından hemen önce ">" simgesini koymak, bu alanı aşağıda gösterildiği gibi bir eşleşme alanı olarak tanımlar.

Part #> _____

Bu parametrenin aralığı (0 - 255) ASCII karakterlerinin ondalık değerini temsil eder. Alana 0 değerinin yazılması özelliği devre dışı bırakır. 9160 G2'de girilen ASCII ondalık değeri, uygulama programı tarafından ayarlanan değerle aynı olmalıdır.

Visible Match (Görünür Eşleşme) özelliğini kullanmak için ana bilgisayar bir girdi eşleşme alanına önceden veri yükler; bu veri mobil bilgisayar ekranında görünür. Mobil bilgisayara gönderilen önceden yüklü veriler tam karakterlerden, özel eşleşme karakterlerinden ya da ikisinin kombinasyonundan oluşabilir. Psion Teklogix mobil bilgisayarların tanıdığı eşleşme karakterleri için aşağıdaki tabloya bakın.

Bir girdi önceden yüklenen veriyle eşleşmezse girdi görüntülenir, mobil bilgisayardan bip sesi duyulur ve imleç eşleşme alanındaki ilk konuma gider. Operatör, eşleşme alanına başka bir girdi yazabilir ya da imleci yeni bir alana taşıyabilir. Eşleşme alanına bir girdi yazıldığında (önceden yüklenen veriyle eşleşmeyen bir girdi dahil) bu girdi bir sonraki aktarımda mobil bilgisayarın düzenlenen verilerinin bir parçası olarak ana bilgisayara gönderilir.

Tablo 23.4 Eşleşme Karakterleri

Karakter	Açıklama
#	Sayı eşleştirir.
&	Harf eşleştirir (küçük ya da büyük harf).
^	Büyük harf eşleştirir.
_	Küçük harf eşleştirir.
	Alfanümerik karakter eşleştirir.
"	Harf, sayı ya da boşluk eşleştirir.
?	Noktalama işareti eşleştirir.
'	Herhangi bir karakter eşleştirir.
:	Alandaki tüm karakter konumlarını bir önceki karakterle eşleştirir.
;	Geri kalan karakterleri (alanda kalan karakterlerin olması şart değil) bir önceki karakterle eşleştirir.

Örnek:

Parça numarası içeren bir girdi alanını önceden yüklemek istediğinizi varsayalım. Parça numarası biliniyorsa bu parça numarasını alana önceden yükleyebilirsiniz. Daha fazla esneklik gerekiyorsa parça numaraları her zaman iki alfabetik karakterle başlayıp tire (-) ve dört rakamla devam eder. Alandaki eşleşen satır şu şekilde görünür: &&-#### .

Hidden Match Character (Gizli Eşleşme Karakteri)

“Visible match” (görünür eşleşme) alanındaki verilerin aksine “hidden match” (gizli eşleşme) alanındaki önceden yüklenmiş veriler mobil bilgisayarda görüntülenmez.



Not: Alan eşleme hakkında ayrıntılı bilgi için bkz. “Visible Match Character (Görünür Eşleşme Karakteri)”, sayfa 281.

Bu parametrenin aralığı (0 - 255) ASCII karakterlerinin ondalık değerini temsil eder. Alana 0 değerinin yazılması özelliği devre dışı bırakır. 9160 G2’de girilen ASCII ondalık değeri, uygulama programı tarafından ayarlanan değerle aynı olmalıdır.

Serial I/O (Seri G/Ç)

Serial I/O (Seri G/Ç) alanları, seri bağlantı noktalarından giriş ve çıkış kabul eden özel girdi alanları ve sabit alanlardır. Uygulama programı *Serial I/O* (Seri G/Ç) alanının önüne özel bir karakter koyarak bu alanı ayırt eder.

Bu karakter, sabit bir alanın önünde yer aldığı veriler mobil bilgisayarın seri bağlantı noktasına gönderilir. Karakter girdi alanının önünde yer aldığı alana mobil bilgisayarın seri bağlantı noktasından veri gönderilir.

Bu parametrenin aralığı (0 - 255) ASCII karakterlerinin ondalık değerini temsil eder. Alana 0 (sıfır) değerinin yazılması özelliği devre dışı bırakır.

Print Line (Yazdırma Satırı)

Bu parametre uygulama ekranındaki yazdırma sayfasının başlangıç satırı numarasını girmenizi sağlar (ayrıca bkz. *Entry Line [Girdi Satırı]*). 1- 24 arasındaki değerler görüntüleme sayfasının yazdırılmasını sağlar, 0 (sıfır) bu özelliği devre dışı bırakır.

Print Form Length (Yazdırma Biçimi Uzunluğu)

Bu parametre yazıcının biçim uzunluğunu satır cinsinden ayarlar. Değer aralığı 0 - 24’tür.

Barcode (Barkod)

Barcode-input-only (yalnızca barkod girişi) alanları yalnızca barkod okuyuculardan gelen girişleri kabul eden özel girdi alanlarıdır. Uygulama programı *barcode-input-only* (yalnızca barkod girişi) alanının önüne özel bir karakter koyarak bu alanı ayırt eder.

Bu parametrenin aralığı (**0 - 255**) ASCII karakterlerinin ondalık değerini temsil eder. Alana **0** (sıfır) değerinin yazılması özelliği devre dışı bırakır.

Entry Line (Girdi Satırı)

Bu parametre, ekranın sol üst kısmında herhangi bir girdi alanı yoksa ve bir girdi alanı ilk satırda veya bu satırın altındaysa gösterilen ilk satırın numarasını içerir.

Entry Line (Girdi Satırı) parametresi ana bilgisayar ekranında otomatik ofset sağlar; böylece mobil bilgisayar tarafından görüntülenen alan, normalde sınırların dışında olacak bir girdi alanını içerir. Bazı Psion Teklogix mobil bilgisayarları, ekran boyutları daha küçük olduğundan uygulamanın yalnızca sol üst köşesini görüntüler.

Field Overhead (Alan Ek Yüğü)

Bu parametre iki *sabit* alan arasında izin verilen maksimum karakter sayısını içerir. Bu parametre, 9160 G2'nin bu alanları tek bir alanda birleştirmesini sağlar.

9160 G2 bazen iki bitişik sabit alanı birleştirdikten sonra tek bir alan olarak gönderebilir. Bu sayede telsiz bağlantısı üzerindeki ek yük azalmış olur.

Örneğin, iki alan arasında 4 karakter varsa ve bu parametre "5" ise bu alanlar tek bir alanda birleştirilebilir.

Command Region (Komut Bölgesi)

Bu parametre, 9160 G2'nin kayıtlı komutlar için denetleyeceği ana bilgisayar ekranı bölgesini tanımlar.

Command Region (Komut Bölgesi) metin kutusundaki dört sayı, komut bölgesinin sol üst ve sağ alt köşesindeki satır ve sütun adreslerini temsil eder. Her çiftteki ilk metin kutusu sıra numarasını, ikinci metin kutusu sütun numarasını içerir. Sıra değerlerinin aralığı **0 - 24**; sütun değerlerinin ise **0 - 80**'dir.

Örneğin, ana bilgisayar ekranının son iki satırını komut bölgesi olarak tanımlamak için 23, 1 ve 24, 80 değerlerini girin.

Şu an desteklenen tek komut *ALARM*'dır (Bu komutla ilgili ayrıntılar için bkz. sayfa 275). "ALARM" kelimesi komut bölgesinin herhangi bir yerine yazıldığında 9160 G2, mobil bilgisayara bir TESS *bip* komutu gönderir.

23.4.2.3 Telnet Protokol Seçenekleri

Telnet Protocol Options:
Terminal Type: IBM-5251-11
Host Port: 23 (Range 1..32767)
Maximum Sessions per Terminal: 4 (Range 1..127)
First Local Terminal Port: 10000 (Range 1..32767)
Local IP Address to Bind: 0.0.0.0
First Terminal Listen Port: 0 (Range 0..32767)
Actively Negotiate with Host: ☐
Auto-telnet: DISABLE
Auto-telnet Host:
Auto-telnet without User Action: ☒
Enable Virtual Device Names: ☐
- Configure Device Names:
- Device Name Prefix:

Terminal Type (Terminal Türü)

Bu parametre 9160 G2 tarafından bu ana bilgisayar için emüle edilecek mobil bilgisayar türünü seçmenizi sağlar. Şu anda *5250 Emülasyonu* için mevcut olan mobil bilgisayar seçenekleri şunlardır: **IBM 5251-11**, **IBM 5555-B01** ve **IBM 3179-2**.

Ana Bilgisayar Bağlantı Noktası

Bu parametre seçili *5250 Emülasyonu* ana bilgisayar bağlantısı için bir ana bilgisayar bağlantı noktası değeri girmenize olanak sağlar. Varsayılan değer **23**'tür.

Maximum Sessions per Terminal (Terminal Başına Maksimum Oturum Sayısı)

Bu oturum, her bir mobil bilgisayardan çıkmasına izin verilen maksimum telnet oturum sayısını içerir. Varsayılan değer **4**, değer aralığı **1 - 127**'dir.

First Local Terminal Port (İlk Yerel Terminal Bağlantı Noktası)

Bu parametre, ilk mobil bilgisayarın giden telnet oturumlarına bağlanacağı yerel bağlantı noktası numarasını içerir. Varsayılan değer **10.000**'dir.

Local IP Address to Bind (Bağlanılacak Yerel IP Adresi)

Bu parametre ilk mobil bilgisayarın giden telnet oturumlarına bağlanacağı ağ adaptörü IP adresini içerir.

First Terminal Listen Port (İlk Terminal Dinleme Bağlantı Noktası)

Bu parametre 9160 G2'nin mobil bilgisayarlara yapılacak olan telnet bağlantı isteklerini dinleyeceği ilk bağlantı noktası numarasını belirtir. Bu parametreyi **etkinleştirmek** için minimum değer **1024** olmalıdır. Dinleme bağlantı noktasını **devre dışı bırakmak** için değer **0** olmalıdır.

Varsayılan değer **0**'dır (devre dışı).

Actively Negotiate with Host (Ana Bilgisayarla Etkin Biçimde Görüşme)

Bu parametre etkinleştirildiğinde 9160 G2, telnet bağlantısının kurulması sırasında ana bilgisayarla görüşmeye başlar. Pek çok ana bilgisayar için önerilmez.

Auto-telnet (Otomatik telnet)

Bu parametre, telnet oturumlarının mobil bilgisayarlardan bu ana bilgisayara olan otomatik bağlantısını devre dışı bırakmanızı ya da etkinleştirmenizi sağlar.

Sunulan seçenekler şunlardır: **Disable** (Devre dışı bırak) ve **Auto-telnet** (Otomatik telnet). Varsayılan değer **Disable** (Devre dışı bırak) seçeneğidir.

Auto-telnet (Otomatik telnet) **devre dışı bırakıldığında** mobil bilgisayarlardan ana bilgisayara doğru kurulan telnet oturum bağlantılarının mobil bilgisayarlardan manuel olarak başlatılması gerekir.

Auto-telnet (Otomatik telnet) **etkinleştirildiğinde** 9160 G2, terminal numaraları bu ana bilgisayarla eşleşen her mobil bilgisayardan bir telnet oturumu başlatır. Her mobil bilgisayardan ana bilgisayara ek telnet oturumu başlatılabilir ancak bu oturumların manuel olarak başlatılması gerekir.

Auto-telnet (Otomatik telnet) **etkinleştirildiğinde** 9160 G2, oturum açıldığında ve kapatıldığında otomatik olarak ana bilgisayara erişir.



Not: Otomatik telnet oturumları yalnızca "çevrimiçi" (açık ve Psion Teklogix RF ağında sorunsuz biçimde çalışan) mobil bilgisayarlar için başlatılır.

Auto-telnet Host (Otomatik Telnet Ana Bilgisayarı)

Bu parametre 9160 G2'nin otomatik telnet oturumu bağlantısı oluşturduğu ana bilgisayarın adını ya da IP adresini içerir.



Not: Bu metin kutusunda yer alan ana bilgisayar adı 9160 G2 tarafından "çözümlenebilir" olmalıdır; yani 9160 G2'nin ana bilgisayar adı için bir IP adresi alabilmesi gerekir. Örneğin, ana bilgisayar adı 9160 G2 ana bilgisayar tablosundaki bir girdiye karşılık gelebilir ya da 9160 G2 bir etki alanı adı sunucusu sorgulayabilir. Mobil bilgisayarın TCP > isteminde kullanılabilen her ana bilgisayar adı burada da kullanılabilir.

Auto-telnet Without User Action (Kullanıcı Etkinliği Olmadan Otomatik Telnet)

Bu parametre etkinleştirildiğinde kullanıcının [ENTER] tuşuna basmasına gerek kalmadan denetleyici başlatılan her mobil bilgisayar için hemen ana bilgisayarda bir bağlantı açar.

Enable Virtual Device Names (Sanal Cihaz Adlarını Etkinleştir)

Bu parametre etkinleştirildiğinde 9160 G2, telnet bağlantısı için sanal cihaz adı almak üzere ana bilgisayarla görüşür.

Configure Device Names (Cihaz Adlarını Yapılandır)

Telnet Terminal Naming

To remove an LU Name, click the "Remove" button. Ensure that you have selected at least one terminal. See the Help panel for more information.

<input type="checkbox"/> Edit	Terminal Number	LU Name
<input type="checkbox"/> [Edit]	1	ABC
<input type="checkbox"/> [Edit]	5	THING

Selected Terminals:

Add a Terminal...

To associate an LU Name with a Terminal, fill in the fields below and click "Add Name".

Terminal Number:

LU Name:

Yapılandırılan her mobil bilgisayar için bir LU Adı gereklidir. Bu sayfa LU Adları atamanızı sağlar (aşağıdaki *Device Name Prefix* [Cihaz Adı Ön Eki] bölümüne de bakın). LU Adı benzersiz olmalıdır ve mobil bilgisayarın Terminal Numarasıyla ilişkili olmalıdır. LU Adları maksimum 10 alfanümerik karakterden oluşabilir. Küçük harfle yazılan karakterler otomatik olarak büyük harfe dönüştürülür.

Device Name Prefix (Cihaz Adı Ön Eki)

Bir mobil bilgisayar için herhangi bir LU Adı belirlenmemişse 9160 G2, tam bir LU Adı oluşturmak için Terminal Numarasını (beş rakam, gerektiğinde başa sıfır koyarak) LU Ön Ekine ekleyecektir.

23.4.2.4 İşlev Tuşu Eşlemeleri

Function Key Mappings:		
F1: <input type="text" value="F1"/>	F14: <input type="text" value="F14"/>	F27: <input type="text" value="F17"/>
F2: <input type="text" value="F2"/>	F15: <input type="text" value="F15"/>	F28: <input type="text" value="F18"/>
F3: <input type="text" value="F3"/>	F16: <input type="text" value="CLEAR"/>	F29: <input type="text" value="UP"/>
F4: <input type="text" value="F4"/>	F17: <input type="text" value="PRINT"/>	F30: <input type="text" value="SESS"/>
F5: <input type="text" value="F5"/>	F18: <input type="text" value="HELP"/>	F31: <input type="text" value="ENTER"/>
F6: <input type="text" value="F6"/>	F19: <input type="text" value="F19"/>	F32: <input type="text" value="ENTER"/>
F7: <input type="text" value="F7"/>	F20: <input type="text" value="F20"/>	F33: <input type="text" value="ENTER"/>
F8: <input type="text" value="F8"/>	F21: <input type="text" value="F21"/>	F34: <input type="text" value="ENTER"/>
F9: <input type="text" value="F9"/>	F22: <input type="text" value="F22"/>	F35: <input type="text" value="ENTER"/>
F10: <input type="text" value="F10"/>	F23: <input type="text" value="F23"/>	F36: <input type="text" value="ENTER"/>
F11: <input type="text" value="F11"/>	F24: <input type="text" value="F24"/>	F37: <input type="text" value="ENTER"/>
F12: <input type="text" value="F12"/>	F25: <input type="text" value="DOWN"/>	F38: <input type="text" value="SELECTOR"/>
F13: <input type="text" value="F13"/>	F26: <input type="text" value="F16"/>	F39: <input type="text" value="ENTER"/>

n İşlev Tuşu

Function Key (İşlev Tuşu) parametresi, mobil bilgisayarınızda bir işlev tuşuna bastığınızda ana bilgisayara gönderilecek kodu seçmenize olanak sağlar. Her işlev tuşu aynı kod aralığından seçilebilir ancak her işlev tuşunun farklı bir varsayılan kodu vardır. Varsayılan değerler bu sayfada gösterilmiştir.

23.4.3 ANSI Emülasyonu

23.4.3.1 Emulation Options (Emülasyon Seçenekleri)

ANSI Emulation Options:	
Maximum Screen Size:	24 rows 80 columns
Host Timeout:	15 (Range 0..255)
Escape Timeout:	12 (Range 0..255)
Threshold:	200 (Range 0..999)
Echo:	<input checked="" type="checkbox"/>
Function Key Remapping:	<input type="checkbox"/>
Arrow Key Remapping:	<input type="checkbox"/>
Page Saving:	<input checked="" type="checkbox"/>
Page Saving consider Double Byte Characters:	<input type="checkbox"/>
RLE:	<input type="checkbox"/>
Convert 7 to 8 bits:	<input type="checkbox"/>
Lower Character Set (GL):	ASCII ▼
Upper Character Set (GR):	ASCII ▼
Terminal Initialization Data:	
Host Initialization Data:	

Maximum Screen Size (Maksimum Ekran Boyutu)

Maximum Screen Size (Maksimum Ekran Boyutu) mobil bilgisayarlar için gerekli maksimum ekran boyutunu satır ve sütunlar aracılığıyla ayarlamana sağlar. Bu özellik sayfa kaydetme seçeneği kullanılırken belleği en iyi şekilde kullanmanızı sağlar (bkz. “Page Saving (Sayfa Kaydetme)”, sayfa 291).

Değer aralığı minimum 24 x 80, maksimum 60 x 132'dir. Varsayılan ayar 24 x 80'dir.

Host Timeout (Ana Bilgisayar Zaman Aşımı)

Host Timeout (Ana Bilgisayar Zaman Aşımı), ana bilgisayardan alınan veri yığınları arasındaki süredir (*saniye* ya da *salise* cinsinden). Varsayılan değer **15**, değer aralığı **0 - 255**'tir.

Bu zaman aşımı sona erdikten sonra 9160 G2 ana bilgisayardan herhangi bir karakter almazsa ana bilgisayarın veri gönderme işlemini tamamladığını varsayar ve kullanıcı girişini bekler (başka bir deyişle veri ekranının tamamlandığını varsayar).



Önemli: *Host Timeout (Ana Bilgisayar Zaman Aşımı) parametresindeki değeri değiştirmek için Page Saving (Sayfa Kaydetme) parametresinin (sayfa 291) etkinleştirilmesi gerekir.*

Escape Timeout (Kaçış Zaman Aşımı)

Escape Timeout (Kaçış Zaman Aşımı), 9160 G2'nin ana bilgisayardan alınan bir "ESC"yi beklettiği ve alınan bir sonraki baytın bir kaçış sekansının parçası olduğunu düşündüğü süredir (*saniye* ya da *salise* cinsinden). Varsayılan değer **12**, değer aralığı **0 - 255**'tir.

Bu zaman aşımı sona erdiğinde ana bilgisayarın yeni bir kaçış sekansı başlatmak için başka bir "ESC" karakteri göndermesi gerekecektir.



Not: Özellikle ESC'nin bir veri paketinin sonunda yer aldığı durumlarda bu çok önemlidir.

Threshold (Eşik)

Threshold (Eşik), 9160 G2'nin ekranı yeni bir "kaydedilen sayfa" olarak saklamadan önce ana bilgisayardan alınması gereken mobil bilgisayara ait güncelleme verilerinin bayt cinsinden minimum miktarıdır. Varsayılan değer **200**, değer aralığı **0 - 999**'dur.



Önemli: *Threshold (Eşik) parametresindeki değeri değiştirmek için Page Saving (Sayfa Kaydetme) parametresinin (sayfa 291) etkinleştirilmesi gerekir.*

Echo (Yansıtma)

Bu parametre **etkinleştirildiğinde** 9160 G2 “*Smart*” *Echo* (Akıllı Yansıtma) modunu kullanır. Bu mod, telsiz aktarımlarının sayısını azaltarak mobil bilgisayara gönderilen veri miktarını düşürür.

Normalde, bir karakter modu uygulaması kullanıldığında her tuş vuruşu ana bilgisayara tek bir aktarımda gönderilir ve karakter ana bilgisayar tarafından başka bir aktarımda yansıtılır. “*Smart*” *Echo* (Akıllı Yansıtma) **etkinleştirildiğinde** ana bilgisayarın yansıttığı veri mobil bilgisayardan gelen veriyle aynıysa 9160 G2, ana bilgisayarın yansıttıklarını mobil bilgisayara göndermez. Böylece telsiz aktarımlarının sayısı azaltılmış olur.

Bu mod ayrıca klavyede bir tuşa basılmasıyla ana bilgisayar tarafından yansıtılan karakterin görüntülenmesi arasındaki bekleme süresini de azaltır ya da tamamen ortadan kaldırır. Yansıtma için bekleyen maksimum karakter sayısı **25**'tir. Daha fazla karakterin olması durumunda bu karakterler ana bilgisayara gönderilecek ancak görüntülenmeyecektir.



Notlar:

1. *Bu parametre ayrıca bir ANSI parametre sorgusunun mobil bilgisayara gönderilip gönderilmeyeceğini de belirler.*
2. *“Smart” Echo (Akıllı Yansıtma) özelliğinin de mobil bilgisayarda etkinleştirilmesi gerekir (ilgili mobil bilgisayarın kullanım kılavuzuna bakın).*

Function Key Remapping (İşlev Tuşlarını Yeniden Ayarlama)

Bu parametre **etkinleştirildiğinde** 9160 G2, işlev tuşlarını bu ana bilgisayar için Function Key Remapping (İşlev Tuşlarını Yeniden Ayarlama) sayfasında anlatıldığı gibi yeniden ayarlar (sayfa 299).

Arrow Key Remapping (Ok Tuşlarını Yeniden Ayarlama)

Bu parametre **etkinleştirildiğinde** 9160 G2, ok tuşlarını bu ana bilgisayar için Function Key Remapping (İşlev Tuşlarını Yeniden Ayarlama) sayfasında anlatıldığı gibi yeniden ayarlar (sayfa 299).

Page Saving (Sayfa Kaydetme)

Bu parametre **etkinleştirildiğinde** 9160 G2, sayfa kaydetmeyi kullanarak mobil bilgisayarlara iletilen veri miktarını azaltır.

9160 G2, mobil bilgisayarda saklanan her sayfanın görüntüsünü alır. 9160 G2, bir uygulama ekranı aldıktan sonra ekranı saklanan sayfalardan biriyle eşlemeye çalışır. Sayfa hali hazırda mobil bilgisayarda bulunuyorsa 9160 G2, mobil bilgisayara sayfanın sakladığı kopyasını yeniden görüntülemesi talimatını verir; bu sayfa için telsiz bağlantısıyla veri gönderilmesine gerek kalmaz. 9160 G2 sayfayı herhangi bir sayfayla eşleyemezse sayfanın tamamı mobil bilgisayara gönderilir. Varsayılan değer **enabled** (etkin) seçeneğidir.



Notlar: *Sayfa kaydetme etkinleştirildiğinde kaydedilen sayfa sayısı mobil bilgisayarda belirlenen sayıdır. Ayrıntılar için ilgili mobil bilgisayara ait kullanıcı kılavuzuna bakın.*

Çince ve Korece gibi çift baytlık karakter kümeleri kullanıyorsanız aşağıdaki Page Saving Consider Double Byte Character (Çift Baytlık Karakterlerle Sayfa Kaydetme) parametresine bakın.

Page Saving Consider Double Byte Character (Çift Baytlık Karakterlerle Sayfa Kaydetme)

Çince veya Korece gibi çift baytlık karakter kümeleri kullanılırken *Page Saving* (Sayfa Kaydetme) (yukarı bakın) çift baytlık bir karakterin bir kısmının üzerine yazılmasına izin verir. Bu durum tek baytlık yazdırılamaz bir ekran verisine ya da iki farklı karakterin birleşiminden oluşan yeni, istenmeyen bir karakterin oraya çıkmasına yol açabilir. Ayrıca mobil bilgisayar kötü veriyi kesmek için ekrandaki veriyi değiştirebilir.

Page Saving Consider Double Byte Character (Çift Baytlık Karakterlerle Sayfa Kaydetme) **etkinleştirildiğinde** *Page Saving* (Sayfa Kaydetme), değiştirilmiş karakterlerin ve yarıda kesilen verilerin mobil bilgisayarda görüntülenmesini önlemek için tek kalan çift baytlık karakter yarısının yerine boşluk koyar. Varsayılan değer **disabled** (devre dışı) seçeneğidir.



Not: Bu parametre yalnızca çift baytlık karakter kümeleri kullanılırken kullanılmalıdır.

RLE

Bu parametre **etkinleştirildiğinde** 9160 G2, telsiz bağlantısı aracılığıyla gönderdiği veriye seçirdim kodlaması (RLE) uygular. *RLE* ana bilgisayardan mobil bilgisayara giden tekrarlanan karakterleri sıkıştırır. Veri akışında tekrarlanan karakterler bulunduğunda ilk karakter gönderildikten sonra mobil bilgisayara bu karakteri kaç kere tekrarlayacağını söyleyen kısa bir kaçış sekansı (3-4 karakter) gönderilir. Böylece RLE verileri sıkıştırır ve toplam telsiz bağlantısı trafiğini azaltır.

Convert 7 to 8 Bits (7 Biti 8 Bite Dönüştür)

Bu parametre **etkinleştirildiğinde** 9160 G2, 7 bit kontrol sekanslarını mobil bilgisayara giden ANSI veri akışlarındaki 8 bitlik karşılıklarına dönüştürür. Bu işlem, veriyi sıkıştırarak iki karakterli kaçış sekanslarını tek karakterli karşılıklarıyla değiştirir.

Lower Character Set (GL) (Küçük Harf Kümesi)

Bu parametre, mobil bilgisayarlarda seçilen karakter kümesiyle aynı karakter kümesine ayarlanmalıdır. Bu parametre yalnızca sayfa kaydetme etkin olduğunda kullanılır.

Upper Character Set (GR) (Büyük Harf Kümesi)

Bu parametre, mobil bilgisayarlarda seçilen karakter kümesiyle aynı karakter kümesine ayarlanmalıdır. Bu parametre yalnızca sayfa kaydetme etkin olduğunda kullanılır.

Terminal Initialization Data / Host Initialization Data (Terminal Başlatma Verisi / Ana Bilgisayar Başlatma Verisi)

Bu alanlar, mobil bilgisayar her sıfırlandığında denetleyiciden mobil bilgisayara ya da ana bilgisayara gönderilecek verileri girmek için kullanılır. Örneğin, bu alanlar ana bilgisayarın yenilenmesi ya da oturum açıldığında ana bilgisayar tarafından mobil bilgisayarda ayarlanan karakter kümelerinin sıfırlanması isteği gönderilirken kullanılır.

Yazdırılamayan veriler \xnn şeklinde onaltılık sistemde ya da \nnn şeklinde sekizlik sistemde girilebilir. Örneğin, kaçış karakteri şu şekilde girilebilir: \x1b ya da \033.

Bu parametreler en fazla 256 karakter uzunluğunda olabilir. Bu alanlar boşsa hiç veri gönderilmemiş demektir.

23.4.3.2 Telnet Protokol Seçenekleri

Telnet Protocol Options:	
Terminal Type:	VT100
Host Port:	23 (Range 1..32767)
Maximum Sessions per Terminal:	4 (Range 1..127)
Close Host sessions on Terminal reset:	<input type="checkbox"/>
First Local Terminal Port:	10000 (Range 1..32767)
Local IP Address to Bind:	0.0.0.0
First Terminal Listen Port:	0 (Range 0..32767)
TCP Session Request Key:	1 (Range 0..255)
Session Cycle Key:	2 (Range 0..255)
Last Active Session Key:	5 (Range 0..255)

Terminal Type (Terminal Türü)

Bu parametre, 9160 G2 tarafından emüle edilecek mobil bilgisayar türünü belirler. Metin kutusuna girilecek karakterler, ana bilgisayar tarafından kabul edilen **maksimum 32** karakterden oluşan herhangi bir ASCII dizesi olabilir. Varsayılan değer **VT100**'dür.

Ana Bilgisayar Bağlantı Noktası

Bu parametre, seçili ANSI ana bilgisayar bağlantısının ana bilgisayar bağlantı noktası değerini belirler. Varsayılan değer **23**'tür.

Maximum Sessions per Terminal (Terminal Başına Maksimum Oturum Sayısı)

Bu oturum, her bir mobil bilgisayardan çıkmasına izin verilen maksimum telnet oturum sayısını içerir. Varsayılan değer **4**, değer aralığı **1 - 127**'dir.

Close Host Sessions on Terminal Reset (Terminal Sıfırlanırken Ana Bilgisayar Oturumlarını Kapat)

Bu parametre **etkinleştirildiğinde** ve terminal sıfırlama mesajı alındığında o terminal numarasındaki ana bilgisayar oturumu kapatılır. Varsayılan değer **disabled** (devre dışı) seçeneğidir.

First Local Terminal Port (İlk Yerel Terminal Bağlantı Noktası)

Bu parametre, 9160 G2'nin ilk mobil bilgisayar için bir telnet bağlantısı kurmayı deneyeceği bağlantı noktası numarasını belirler. Varsayılan değer **10.000**'dir. Ek telnet oturumları daha büyük bağlantı noktası numaralarına atanır.

Local IP Address to Bind (Bağlanılacak Yerel IP Adresi)

Bu parametre, bu ana bilgisayara bağlanan 9160 G2 arabiriminin IP adresini belirler. Her terminal oturumuna benzersiz bir yuva oluşturmak için yerel bağlantı noktası numaralarıyla birlikte kullanılır.

First Terminal Listen Port (İlk Terminal Dinleme Bağlantı Noktası)

Bu parametre 9160 G2'nin mobil bilgisayarlara yapılacak olan telnet bağlantı isteklerini dinleyeceği ilk bağlantı noktası numarasını belirtir. Bu parametreyi **etkinleştirmek** için minimum değer **1024** olmalıdır. Dinleme bağlantı noktasını **devre dışı bırakmak** için değer **0** olmalıdır.

Varsayılan değer **0**'dır (devre dışı).

TCP Session Request Key (TCP Oturumu İstek Tuşu)

Bu parametre mobil bilgisayarın yeni bir ANSI terminal oturumu isteği göndermesini sağlayacak karakterin ondalık ASCII karakter kodunu içerir. Varsayılan değer **1**, değer aralığı **0 - 255**'tir.

Session Cycle Key (Oturum Döngüsü Tuşu)

Bu parametre mobil bilgisayarın bir sonraki ANSI terminal oturumunu görüntülemesini sağlayacak karakterin ondalık ASCII karakter kodunu içerir. Varsayılan değer **2**, değer aralığı **0 - 255**'tir.

Last Active Session Key (Son Etkin Oturum Tuşu)

Bu parametre mobil bilgisayarın son ANSI terminal oturumunu görüntülemesini sağlayacak karakterin ondalık ASCII karakter kodunu içerir. Varsayılan değer 5, değer aralığı 0 - 255'tir.

23.4.3.3 Otomatik Telnet/Otomatik Oturum Açma

Auto-Telnet / Auto-Login:	
Auto-telnet/login Enable:	<input type="text" value="DISABLE"/>
Auto-telnet Host:	<input type="text"/>
Auto-telnet Terminal Prompt:	<input type="text" value="Press ENTER to login."/>
Auto-login User ID:	<input type="text"/>
Auto-login Password:	<input type="password"/>
Auto-login User ID prompt:	<input type="text" value="gin:"/>
Auto-login Password prompt:	<input type="text" value="word:"/>
Auto-login failed login:	<input type="text" value="incorrect"/>
Auto-telnet without User Action:	<input type="checkbox"/>
Auto-telnet without User Action Timing Delay:	<input type="text" value="25"/> (Range 0..255)
Maximum of Auto-telnet Retries:	<input type="text" value="0"/> (Range 0..255)
Allow TCP Sessions:	<input checked="" type="checkbox"/>

Auto-telnet/login Enable (Otomatik Telneti/Oturum Açmayı Etkinleştir)

Bu parametre, telnet oturumlarının mobil bilgisayarlardan bu ana bilgisayara olan otomatik bağlantısını devre dışı bırakmanızı ya da etkinleştirmenizi sağlar. Sunulan seçenekler şunlardır: **DISABLE** (DEVRE DIŞI BIRAK); **AUTO-TELNET** (OTOMATİK TELNET) ve **AUTO-TELNET/LOGIN** (OTOMATİK TELNET/OTURUM AÇMA). Varsayılan değer **DISABLE** (Devre dışı bırak) seçeneğidir.

Auto-telnet (Otomatik telnet) **devre dışı bırakıldığında** mobil bilgisayarlardan ana bilgisayara doğru kurulan telnet oturum bağlantılarının mobil bilgisayarlardan manuel olarak başlatılması gerekir.

Auto-telnet (Otomatik telnet) **etkinleştirildiğinde** 9160 G2, terminal numaraları bu ana bilgisayarla eşleşen her mobil bilgisayardan bir telnet oturumu başlatır. Her mobil bilgisayardan ana bilgisayara ek telnet oturumu başlatılabilir ancak bu oturumların manuel olarak başlatılması gerekir.



Not: Otomatik telnet oturumları yalnızca "çevrimiçi" (açık ve Psion Teklogix RF ağında sorunsuz biçimde çalışan) mobil bilgisayarlar için başlatılır.

Auto-telnet (Otomatik telnet) ve *Auto-login* (Otomatik oturum açma) **etkinleştirildiğinde** 9160 G2, terminal numaraları bu ana bilgisayarla eşleşen her mobil bilgisayardan bir telnet oturumu başlatır. Ardından bu sayfada verilen Kullanıcı Kimliği ve Şifreyi kullanarak her oturumu ana bilgisayara kaydeder.



Not: Bu ana bilgisayara otomatik olarak kaydedilen tüm Otomatik telnet oturumlarının Kullanıcı Kimliği ve Şifresi aynıdır.

Auto-telnet Host (Otomatik Telnet Ana Bilgisayarı)

Bu parametre 9160 G2'nin otomatik telnet oturumu bağlantısı oluşturduğu ana bilgisayarın adını ya da IP adresini içerir.



Not: Bu metin kutusunda yer alan ana bilgisayar adı 9160 G2 tarafından "çözümlelenebilir" olmalıdır; yani 9160 G2'nin ana bilgisayar adı için bir IP adresi alabilmesi gerekir. Örneğin, ana bilgisayar adı 9160 G2 ana bilgisayar tablosundaki bir girdiye karşılık gelebilir ya da 9160 G2 bir etki alanı adı sunucusu sorgulayabilir.

Mobil bilgisayarın TCP> isteminde kullanılabilen her ana bilgisayar adı burada da kullanılabilir.

Auto-telnet Terminal Prompt (Otomatik Telnet Terminal İstemi)

Bu parametre oturum açma isteği gönderen kullanıcıya sunulan metni içerir. Karakterler herhangi bir ASCII dizesi ya da sekizlik veya onaltılık sistemde sunulan sayısal kaçış sekansından oluşabilir.

Sekizlik bir kaçış sekansı şu şekillerde olabilir: \0d, \Odd ya da \Oddd (her bir d harfi 0-7 arası herhangi bir rakam olabilir). "ddd" ondalık 256'dan büyükse temsil edilen karakterin kod değeri, ondalık ddd/256'dan kalan değerdir.

Onaltılık bir kaçış sekansı şu şekillerde olabilir: \xh ya da xhh (her bir "h" harfi 0-9 arası herhangi bir rakam veya a-f ya da A-F arası herhangi bir alfa değeri olabilir).



Not: \0, kod değeri 0 olan bir karakterdir.

İzin verilen değer, bir satırda **maksimum 60** karakterdir. Varsayılan olarak metin yoktur, oturum açmak için <ENTER> tuşuna basmak yeterlidir.

Auto-login User ID (Otomatik Oturum Açma Kullanıcı Kimliği)

Bu parametre otomatik oturum açma oturumları için 9160 G2 tarafından ana bilgisayara sunulan kullanıcı kimliğini içerir. Karakterler, ana bilgisayar tarafından kabul edilen **maksimum 32** karakterden oluşan herhangi bir ASCII dizesi olabilir.

Auto-login Password (Otomatik Oturum Açma Şifresi)

Bu parametre otomatik oturum açma oturumları için 9160 G2 tarafından ana bilgisayara sunulan şifreyi içerir. Karakterler, ana bilgisayar tarafından kabul edilen **maksimum 32** karakterden oluşan herhangi bir ASCII dizesi olabilir.

Auto-login User ID (Otomatik Oturum Açma Kullanıcı Kimliği İstemi)

9160 G2, bu metin kutusundaki metinle kendisine ana bilgisayar tarafından sunulan metni karşılaştırır. Bu metinler eşleştğinde 9160 G2 ana bilgisayarın bir kullanıcı adı isteği gönderdiğini varsayar ve ana bilgisayara *Auto-Login User ID* (Otomatik Oturum Açma Kullanıcı Kimliği) parametresinde belirtilen kullanıcı kimliğini gönderir. Karakterler **maksimum 32** karakterden oluşan herhangi bir ASCII dizesi olabilir. Varsayılan metin **gin:**'dir



Not: Eşleşen dize mümkün olduğu kadar kısa ancak kullanıcı kimliği istemini benzersiz şekilde tanımlayacak kadar uzun olmalıdır. Bazı ana bilgisayarlar ekranda boşluk bırakmak için boşluk karakterinden başka karakterler de kullandığından boşluk karakteriyle ayrılmış birden fazla bölümü olan kelimeler kullanmayın.

Auto-login Password Prompt (Otomatik Oturum Açma Şifre İstemi)

9160 G2, bu metin kutusundaki metinle kendisine ana bilgisayar tarafından sunulan metni karşılaştırır. Bu metinler eşleştğinde 9160 G2 ana bilgisayarın bir şifre isteği gönderdiğini varsayar ve ana bilgisayara *Auto-Login Password* (Otomatik Oturum Açma Şifresi) parametresinde belirtilen şifreyi gönderir. Karakterler **maksimum 32** karakterden oluşan herhangi bir ASCII dizesi olabilir. Varsayılan metin **word:**'dür



Not: Eşleşen dize mümkün olduğu kadar kısa ancak şifre istemini benzersiz şekilde tanımlayacak kadar uzun olmalıdır. Bazı ana bilgisayarlar ekranda boşluk bırakmak için boşluk karakterinden başka karakterler de kullandığından boşluk karakteriyle ayrılmış birden fazla bölümü olan kelimeler kullanmayın.

Auto-login Failed Login (Otomatik Oturum Açma Başarısız)

9160 G2, bu metin kutusundaki metinle kendisine ana bilgisayar tarafından sunulan metni karşılaştırır. Bu metinler eşleştğinde 9160 G2, ana bilgisayarın mobil bilgisayara oturum açma denemesinin başarısız olduğu bilgisini içeren bir dize yolladığını varsayar. Ardından 9160 G2, kullanıcının manuel olarak giriş yapmasını istemek için mobil bilgisayar ekranında *Auto-telnet Terminal Prompt* (Otomatik Telnet Terminal İstemi) parametresini görüntüler. Karakterler **maksimum 32** karakterden oluşan herhangi bir ASCII dizesi olabilir. Varsayılan metin **incorrect**'tir.



Not: Eşleşen dize mümkün olduğu kadar kısa ancak başarısız oturum açma istemini benzersiz şekilde tanımlayacak kadar uzun olmalıdır. Bazı ana bilgisayarlar ekranda boşluk bırakmak için boşluk karakterinden başka karakterler de kullandığından boşluk karakteriyle ayrılmış birden fazla bölümü olan kelimeler kullanmayın.

Auto-telnet Without User Action (Kullanıcı Etkinliği Olmadan Otomatik Telnet)

Bu parametre etkinleştirildiğinde kullanıcının [ENTER] tuşuna basmasına gerek kalmadan denetleyici başlatılan her mobil bilgisayar için hemen ana bilgisayarda bir bağlantı açar. Bu parametre seçildiğinde *Auto Telnet Terminal Prompt*'un (Otomatik Telnet Terminal İstemi) değiştirilerek kullanıcının bağlantı yapılabildiği kadar beklemesinin sağlanması tavsiye edilir.

Auto-telnet Without User Action Timing Delay (Kullanıcı Etkinliği Zamanlama Bekleme Süresi Olmadan Otomatik Telnet)

Bu parametre etkinleştirildiğinde, *Auto-telnet Without User Action (Kullanıcı Etkinliği Olmadan Otomatik Telnet)* seçeneği bağlantı denemeleri arasında belirli bir süre (milisaniye cinsinden) bekleyebilir.

Maximum Of Auto-telnet Retries (Maksimum Otomatik Telnet Yeniden Deneme Sayısı)

Vazgeçmeden önce otomatik olarak yapılan bağlantı denemesi sayısı.

Allow TCP Sessions (TCP Oturumlarına İzin Ver)

Bu parametre **etkinleştirildiğinde** 9160 G2, mobil bilgisayar kullanıcısının istem sırasında (otomatik oturum açma ya da TCP) istemleri veya oturumları değiştirmesine izin verir.

Allow TCP Sessions (TCP Oturumlarına İzin Ver) **devre dışı bırakıldığında** tüm yeni oturumlar otomatik oturum açma oturumu olarak açılır.

İstem türünü değiştirmek için (başka istem türleri mevcutsa) istem seviyesinde oturum isteği gönderme (mobil bilgisayarlarda normalde <CTRL> a) kullanılabilir.

İstem seviyesinde oturum değiştirmek de mümkündür (mobil bilgisayarlarda <CTRL> b [sonraki oturum] ya da <CTRL> e [son oturum]). İstem seviyesinde oturum değiştirirken mobil bilgisayar durumu (oturum açılmamış), geçilen oturumun durumuyla eşleşecek şekilde ayarlanır.

Varsayılan değer **enabled** (etkin) seçeneğidir.

23.4.3.4 İşlev Tuşu Eşlemeleri

Function Key Mappings:		
F1: 1b,4f,50,00,00,00,00,00	F11: 1b,5b,32,33,7e,00,00,00	F21: 1b,5b,31,7e,00,00,00,00
F2: 1b,4f,51,00,00,00,00,00	F12: 1b,5b,32,34,7e,00,00,00	F22: 1b,5b,32,7e,00,00,00,00
F3: 1b,4f,52,00,00,00,00,00	F13: 1b,5b,32,35,7e,00,00,00	F23: 1b,5b,33,7e,00,00,00,00
F4: 1b,4f,53,00,00,00,00,00	F14: 1b,5b,32,36,7e,00,00,00	F24: 1b,5b,34,7e,00,00,00,00
F5: 1b,5b,31,36,7e,00,00,00	F15: 1b,5b,32,38,7e,00,00,00	F25: 1b,5b,35,7e,00,00,00,00
F6: 1b,5b,31,37,7e,00,00,00	F16: 1b,5b,32,39,7e,00,00,00	F26: 1b,5b,36,7e,00,00,00,00
F7: 1b,5b,31,38,7e,00,00,00	F17: 1b,5b,33,31,7e,00,00,00	F27: 1b,5b,34,31,7e,00,00,00
F8: 1b,5b,31,39,7e,00,00,00	F18: 1b,5b,33,32,7e,00,00,00	F28: 1b,5b,34,32,7e,00,00,00
F9: 1b,5b,32,30,7e,00,00,00	F19: 1b,5b,33,33,7e,00,00,00	F29: 1b,5b,34,33,7e,00,00,00
F10: 1b,5b,32,31,7e,00,00,00	F20: 1b,5b,33,34,7e,00,00,00	F30: 1b,5b,34,34,7e,00,00,00
Up: 1b,5b,41,00,00,00,00,00	Down: 1b,5b,42,00,00,00,00,00	Right: 1b,5b,43,00,00,00,00,00
Left: 1b,5b,44,00,00,00,00,00		

n İşlev Tuşu

Function Key (İşlev Tuşu) parametresi, mobil bilgisayarınızda bir işlev tuşuna bastığınızda ana bilgisayara gönderilecek kodu seçmenize olanak sağlar. Her işlev tuşu aynı kod aralığından seçilebilir ancak her işlev tuşunun farklı bir varsayılan kodu vardır. Varsayılan değerler yukarıdaki ekranda gösterilmiştir.

24.1 802.IQ Özellikleri303
24.1.1 802.IQ v1/v2 Genel Özellikleri303
24.1.2 802.IQ v1 Özellikleri306
24.1.3 802.IQ v2 Özellikleri Menüsü307
24.2 802.IQ Ayarlarını Güncelleme307

24.1 802.IQ Özellikleri

802.IQ, mobil bilgisayarların aynı anda hem TCP/IP hem de 802.IQ protokollerini destekleyen bir ağdaki kablosuz LAN'da çalışmasına olanak sağlayan bir Psion Teklogix özel gelişmiş 802.11 protokolüdür. 802.IQ protokolünün 802.IQ v1 ve 802.IQ v2. olmak üzere iki sürümü vardır. 9160 G2 Kablosuz Ağ Geçidi aynı anda protokolün iki sürümünü de destekler (mobil bilgisayarlar yalnızca birini kullanmalıdır).

802.IQ v1 protokolü, 802.11 kablosuz ağda TCP/IP yönlendirmeye göre daha iyi performans sağlayan bir kablosuz LAN yönlendirme sistemidir. Mobil bilgisayarlar TCP/IP ya da 802.IQ v1 protokolünü kullanarak 9160 G2 erişim noktasıyla iletişim kurabilir. Bu özellik, iki şekilde çalışabilen bir sistemi mümkün kılar. 802.IQv1 ile ilgili daha fazla bilgi ve yapılandırma menüleri için bkz. sayfa 306.

802.IQ v2 protokolü, paketleri UDP katmanı üzerinden aktaran 802.IQ v1 protokolünün geliştirilmiş bir sürümüdür. 802.IQ v1'in tüm işlevlerine sahip olmanın yanı sıra, RF üzerinden yazılım yükseltme, denetleyiciler ve mobil bilgisayarlar arasında üçüncü taraf erişim noktaları ekleme ve istenildiğinde mapRF sistemine entegre olma gibi ek özellikler sunar. 802.IQ v2 mini denetleyici yapılandırma hakkında bilgi için bkz. sayfa 307.

24.1.1 802.IQ v1/v2 Genel Özellikleri



Önemli: *802.IQ, yalnızca kablolu 9160 G2'lerde etkinleştirilmelidir.
802.IQ uyarıları WDS bağlantısı aracılığıyla bir ağdan diğerine
gönderilebildiği için (bkz. Bölüm 20: “Kablosuz Dağıtım Sistemi”)
802.IQ'yu 9160 G2'leri birleştiren ağlarda yapılandırmayın.*

Auto-Startup (Otomatik Başlama)

Bu parametre, 9160 G2 yeniden başlatıldığında 802.IQ'yu hemen **etkinleştirir**. 9160 G2, bir ağ denetleyicisinde baz istasyonu olarak çalışıyorsa bu parametre **devre dışı** olmalıdır.

Varsayılan değer **disabled** (devre dışı) seçeneğidir.



Önemli: *Otomatik Başlama yanlış ayarlanırsa mobil bilgisayarlar düzgün biçimde çalışmayabilir.*

Beacon Period (Uyarı Süreci)

802.IQ uyarısı, tüm 802.IQ özellikli mobil bilgisayarlara gönderilen bir yayındır. Uyarı, mobil bilgisayarların baz istasyonları arasında ne zaman gezineceğini belirlemesini sağlar. Mobil bilgisayarın baz istasyonu ya da denetleyicinin yeniden başlatılıp başlatılmadığını ve yeniden başlatıldıysa nasıl kurtarılacağını belirlemesini sağlar. Denetleyici yeniden başlatıldıysa mobil bilgisayar tüm oturumları kapatır ve tamamen yeniden başlatılır. Baz istasyonu yeniden başlatıldıysa ya da mobil bilgisayar farklı bir 9160 G2'ye taşındıysa hafif bir başlatma gerçekleşir (veri kaybı olmaz).

Duyuru Süreci parametresinin kabul edilebilir değeri **1-20** saniye arasındır. Varsayılan değer **2**'dir.

Terminal Offline Timeout (Terminal Çevrimdışı Zaman Aşımı)

Bu parametre, 9160 G2'deki 802.IQ görevinin, hücresel yöneticiye mobil bilgisayarın çevrimdışı olduğunu bildiren çevrimdışı bir mesaj göndermeden önce geçecek zamanı (dakika cinsinden) ayarlar.

Kabul edilebilir değer **1-240** arasındır. Varsayılan değer **5**'tir.

Şekil 24.1 802.IQ Yapılandırma Ayarlarına Genel Bakış

Basic Settings	Modify 802.IQ settings
User Management	
Cluster	802.IQ v1/v2 Common Features:
Access Points	Auto-Startup: <input type="checkbox"/>
Sessions	Beacon Period: <input type="text" value="2"/> (Range 1..20)
Channel Management	Terminal Offline Timeout: <input type="text" value="5"/> (Range 1..240)
Wireless Neighborhood	
Security	802.IQ v1 Features:
Status	Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Interfaces	Initial RTT: <input type="text" value="1000"/> (Range 10..10000)
Events	Protocol Type ID: <input type="text" value="2457"/> (Range 1501..65535)
Transmit/Receive	Forward 802.IQ packets only: <input type="checkbox"/>
Client Associations	802.IQ v1 Beacon Interfaces:
Neighboring Access Points	Wired: <input type="checkbox"/>
	WLAN0: <input type="checkbox"/>
	WLAN1: <input type="checkbox"/>
	WDS0: <input type="checkbox"/>
	WDS1: <input type="checkbox"/>
	WDS2: <input type="checkbox"/>
	WDS3: <input type="checkbox"/>
Manage	802.IQ v2 Features:
Ethernet Settings	Enabled: <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
802.11 Settings	Beacon UDP port: <input type="text" value="8888"/> (Range 5001..65535)
802.11 Advanced Settings	<input type="button" value="Update"/>
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	
Hosts	
802.IQ	

24.1.2 802.IQ v1 Özellikleri

802.IQ v1 *Features* (802.IQ v1 Özellikleri) menülerine *Connectivity* (Bağlantı) seçeneklerinin 802.IQ sekmesinden girilebilir. (bkz. Şekil 24.1, sayfa 305).

Enabled (Etkin)

Bu parametre 802.IQ v1 özelliğini etkinleştirir ya da devre dışı bırakır. Varsayılan değer **disabled** (devre dışı) seçeneğidir.

Initial RTT (İlk RTT)

Initial RTT (İlk Gidiş Dönüş Süresi), bir *erişim noktası* aktarımı ile *terminalin bilgilendirilmesi* arasındaki süreyi milisaniye cinsinden belirlemek için kullanılır. Erişim noktası, her bir mobil bilgisayara birkaç aktarım yapılırken geçen ortalama süreyi hesaplayarak kabul edilebilir gidiş dönüş süresini sürekli olarak uygun şekilde ayarlar. Bilgilendirmenin alınması ortalama gidiş dönüş süresinin hesapladığından daha uzun sürerse erişim noktası aktarımı yeniden gönderir.

Erişim noktaları *ortalama* gidiş dönüş süresini birkaç aktarım olmadan hesaplayamadığından bir başlangıç noktası ya da "İlk Gidiş Dönüş Süresi" gereklidir. Erişim noktası "İlk RTT" parametresine atanan süreyi gidiş dönüş süresi hesaplamalarında başlangıç değeri olarak kullanır. Erişim noktası mobil bilgisayarla veri alışverişine başladığında bu değer, aktarımlarla bilgilendirmeler arasındaki gerçek ortalama gidiş dönüş süresini yansıtacak şekilde ayarlanacaktır.

Kabul edilebilir değer **10-10.000** arasındır. Varsayılan değer **1000**'dir.

Protocol Type ID (Protokol Türü Kimliği)

Bu parametre, aynı protokol türünü kullanan diğer Ethernet türü paketlerle çalışmaları önlemek için 802.IQ protokol türünü belirler.

Kabul edilebilir değer **1536-65.535** arasındır. Varsayılan değer **2457**'dir.



Önemli: *Protokol Türü Kimliği varsayılan değeri çok nadir değiştirilir. Protokol türü değiştirildiğinde tüm mobil cihazların protokolle eşleşmesi için değiştirilmesi gerekir.*

Forward 802.IQ Packets Only (Yalnızca 802.IQ Paketlerini İlet)

Bu parametre, kablosuz ve kablolu sistemler arasında paket birleştirirken 9160 G2'nin 802.IQ v1 olmayan tüm paketleri otomatik olarak filtreleyerek ayırır. Bu parametre varsayılan olarak **devre dışıdır**.

802.IQ v1 Beacon Interfaces (802.IQ v1 Uyarı Arabirimleri)

Uyarıların hangi arabirim üzerinden gönderileceğini seçin.

Kullanılabilen arabirimler şunlardır: *Kablohu*, *WLAN0*, *WLAN1*, *WDS0* *WDS1*, *WDS2*, *WDS3*.

24.1.3 802.IQ v2 Özellikleri Menüsü

802.IQ v2 Features (802.IQ v2 Özellikleri) menülerine *Connectivity* (Bağlantı) seçeneklerinin *802.IQ* sekmesinden girilebilir. (bkz. Şekil 24.1, sayfa 305).

Enabled (Etkin)

Bu parametre 802.IQv2 protokolünü etkinleştirir ya da devre dışı bırakır.

Varsayılan değer **disabled** (devre dışı) seçeneğidir.

Beacon UDP Port (Uyarı UDP Bağlantı Noktası)

Bu parametre uyarı yayınları için UDP bağlantı noktasını belirler. Ağda birden fazla 802.IQv2 denetleyici varsa sistemleri ayırmak için parametre değiştirilmelidir. Parametre ayrıca mobil bilgisayardaki parametreyle eşleşmelidir. Değer aralığı **5001 - 65.535**'tir. Varsayılan değer **8888**'dir.

24.2 802.IQ Ayarlarını Güncelleme

802.IQ ayarlarını güncellemek için:

1. 802.IQ Settings (802.IQ Ayarları) sayfasına gidin.
2. Ayarları gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

AĞ ZAMAN PROTOKOLÜ SUNUCUSU 25

25.1 Zaman Ayarlarına Gitme	311
25.2 Ağ Zaman Protokolü (NTP) Sunucusunu Etkinleştirme veya Devre Dışı Bırakma.	312
25.3 Ayarları Güncelleme	312

Ağ Zaman Protokolü (NTP) ağınızdaki bilgisayarların saatlerini senkronize eden bir Internet standart protokolüdür. NTP sunucuları, istemci sistemlerine *Eşgüdümlü Evrensel Zaman (UTC, Greenwich Saati* olarak da bilinir) aktarır. NTP, zaman dilimi ayarlamaları gibi saat ayarlamaları yapmak için, dönen zaman damgasını kullanarak sunuculara periyodik zaman istekleri gönderir. Zaman damgası, günlük mesajlarındaki her olayın tarih ve saatini belirtmek için kullanılır. NTP hakkında daha genel bilgiler için <http://www.ntp.org> adresine gidin. Aşağıdaki bölümler belirli bir NTP sunucusu kullanmak için 9160 G2 Kablosuz Ağ Geçidi cihazının nasıl yapılandırılacağını açıklamaktadır.

25.1 Zaman Ayarlarına Gitme

NTP sunucusunu etkinleştirmek için *Services > Time* (Hizmetler > Zaman) sekmesine gidin ve ilgili alanları aşağıda anlatıldığı gibi güncelleyin.

Şekil 25.1 Zaman Ayarları

The screenshot shows the configuration interface of the Pion Teklogix 9160 G2 Wireless Gateway. On the left is a sidebar with a list of configuration categories: Basic Settings, User Management, Cluster, Access Points, Sessions, Channel Management, Wireless Neighborhood, Security, Status, Interfaces, Events, Transmit/Receive, Client Associations, Neighboring Access Points, Manage, Ethernet Settings, 802.11 Settings, 802.11 Advanced Settings, VWN, WDS, Guest Login, MAC Filtering, Load Balancing, Services, QoS, and Time. The 'Time' category is highlighted at the bottom, and an arrow points to it. The main content area is titled 'Modify how the access point discovers the time' and contains the following settings:

- Local Time: Mon Jun 18 18:41:53 UTC 2007
- Network Time Protocol (NTP): ☒ Enabled ☐ Disabled
- NTP Server:
- Time Zone:
-

25.2 Ağ Zaman Protokolü (NTP) Sunucusunu Etkinleştirme veya Devre Dışı Bırakma

Bir ağ zaman protokolü (**NTP**) sunucusu kullanmak üzere erişim noktanızı yapılandırmak için önce NTP kullanımını **etkinleştirin**, ardından kullanmak istediğiniz NTP sunucusunu seçin. (Ağdaki NTP sunucusunu kapatmak için NTP'yi erişim noktasında devre dışı bırakın).

Tablo 25.1 NTP Ayarları

Alan	Açıklama
<i>Local Time</i> (Yerel Saat)	Her güncellemede geçerli yerel saat gösterilir.
<i>Network Time Protocol</i> (Ağ Zaman Protokolü) (NTP)	<p>NTP, erişim noktasının ağdaki bir sunucudan zaman alması ve onu koruması için bir yol sunar. NTP sunucusu kullanmak, AP'nizin günlük mesajlarında ve oturum bilgilerinde doğru saat bilgileri sunmasını sağlar.</p> <p>NTP hakkında daha fazla bilgi için bkz. http://www.ntp.org.</p> <p>Bir ağ zaman protokolü (NTP) sunucusunun kullanımını etkinleştirmeyi ya da devre dışı bırakmayı seçebilirsiniz:</p> <ul style="list-style-type: none"> NTP sunucusunu etkinleştirmek için Enabled (Etkin) seçeneğine tıklayın. NTP sunucusunu devre dışı bırakmak için Disabled (Devre dışı) seçeneğine tıklayın.
<i>NTP Server</i> (NTP Sunucusu)	<p>NTP etkinse kullanmak istediğiniz NTP sunucusunu seçin.</p> <p>NTP sunucusunu ana bilgisayar adı ya da IP adresiyle belirtebilirsiniz ancak IP adresleri daha sık değişebildiğinden IP adreslerini kullanmamanızı öneririz.</p>
<i>Time Zone</i> (Zaman Dilimi)	<p>Açılır listede zaman dilimlerinin (örneğin, "EST [-05:00]") yanı sıra kendi belirlediğiniz değeri girmenizi seçeneği de yer alır. <i>Custom</i> (Özel) seçildiğinde seçim kutucuğunun yanında istediğiniz kısaltmayı ve UTC uzantısını gireceğiniz iki metin kutusu belirir. Özel UTC uzantısı, UTC'nin doğusuna doğru saat ve dakika cinsinden belirtilir. Örneğin, -0800, UTC'nin sekiz saat batısında (yani Pasifik Standart Saati), +0930 ise dokuz saat otuz dakika doğusundadır (yani Avustralya Merkezi Standart Saati).</p> <p>Yaz Saati Uygulaması değişiklikleri yer almaz.</p>

25.3 Ayarları Güncelleme

Zaman ayarlarını güncellemek için:

1. *Time* (Zaman) sekmesine gidin.
2. Zaman ayarlarını gerekli biçimde yapılandırın.
3. Değişiklikleri uygulamak için **Update** (Güncelle) düğmesine tıklayın.

YAPILANDIRMAYI YEDEKLEME VE GERİ YÜKLEME

26

26.1 AP'nin Yapılandırma Ayarlarına Gitme	315
26.2 Fabrika Varsayılanları Yapılandırmasına Sıfırlama	316
26.3 Geçerli Yapılandırmayı Yedekleme Dosyasına Kaydetme	316
26.4 Yapılandırmayı Önceden Kaydedilen Bir Dosyadan Geri Yükleme	316
26.5 Erişim Noktasını Yeniden Başlatma	317
26.6 Ürün Yazılımını Yükseltme	317
26.6.1 Güncelleme	319
26.6.2 Ürün Yazılımı Yükseltmesini Doğrulama	319

9160 G2 Kablosuz Ağ Geçidi cihazındaki geçerli ayarların bir kopyasını yedek bir yapılandırma dosyasına kaydedebilirsiniz. Yedekleme dosyası, erişim noktasını önceden kaydedilen bir yapılandırmaya geri yüklemek için ileriki bir zamanda kullanılabilir.

26.1 AP'nin Yapılandırma Ayarlarına Gitme

Bir erişim noktasının yapılandırılmasını yönetmek için *Maintenance > Configuration* (Bakım > Yapılandırma) sekmesine gidin ve arabirimi aşağıda açıklandığı gibi kullanın.

Şekil 26.1 AP Yapılandırmasına Genel Bakış

The screenshot displays the web interface for managing an Access Point (AP). On the left is a vertical sidebar menu with various configuration categories. The main area on the right is titled 'Manage this Access Point's Configuration' and contains three sections: 'To Restore Factory Default Configuration ...', 'To Save the Current Configuration to a Backup File ...', and 'To Restore the Configuration from a Previously Saved File ...'. Each section includes instructions and a button to perform the action. The 'Configuration' option in the sidebar menu is highlighted with a black arrow pointing to it.

Basic Settings	Manage this Access Point's Configuration
User Management	To Restore Factory Default Configuration ...
Cluster	Click "Reset" to load the factory defaults in place of the current configuration for this AP. Reset
Access Points	To Save the Current Configuration to a Backup File ...
Sessions	Click the link below to download a file containing the current configuration for this AP.
Channel Management	<input type="checkbox"/> Encrypt the configuration file [download configuration]
Wireless Neighborhood	To Restore the Configuration from a Previously Saved File ...
Security	Enter the path and file name of the configuration backup file you want to use, or click "Browse" to open a dialog where you can locate and select the file. Then click "Restore" to load this file in place of the current configuration. Browse... Restore
Status	To Reboot the Access Point ...
Interfaces	Click the "Reboot" button. Reboot
Events	
Transmit/Receive	
Client Associations	
Neighboring Access Points	
Manage	
Ethernet Settings	
802.11 Settings	
802.11 Advanced Settings	
VWN	
WDS	
Guest Login	
MAC Filtering	
Load Balancing	
Services	
QoS	
Time	
SNMP	
Narrow Band	
Radio	
Connectivity Options	
Connectivity	
Base Station	
RRM Groups	
Radio Link Features	
Hosts	
802.1Q	
Maintenance	
Configuration	

26.2 Fabrika Varsayılanları Yapılandırmasına Sıfırlama

9160 G2 Kablosuz Ağ Geçidi cihazıyla ilgili sorunlar yaşıyorsanız ve tüm sorun giderme önlemlerini denediyseniz *Reset Configuration* (Yapılandırmayı Sıfırla) işlevini kullanın. Bu işlevin kullanılması cihazın fabrika varsayılanlarını geri yükler ve yeni şifre ve kablosuz ayarları dahil tüm ayarları sıfırlar.

1. **Maintenance > Configuration** (Bakım > Yapılandırma) sekmesine tıklayın.
2. **Reset** (Sıfırla) düğmesine tıklayın.

Fabrika ayarları geri yüklenir.



Not: Yapılandırmayı bu sayfadan sıfırladığınızda bunu yalnızca geçerli erişim noktası için yaptığınızı, kümedeki diğer erişim noktalarının bundan etkilenmeyeceğini unutmayın. Fabrika varsayılan ayarları hakkında bilgi için bkz. “9160 G2 Kablosuz Ağ Geçidi’nin Varsayılan Ayarları”, sayfa 27.

26.3 Geçerli Yapılandırmayı Yedekleme Dosyasına Kaydetme

Bir erişim noktasındaki geçerli ayarların bir kopyasını yedek yapılandırma dosyasına (.cbk formatında) kaydetmek için:

1. **Download configuration** (yapılandırmayı indir) bağlantısına tıklayın.
File Download or Open (Dosya İndir ya da Aç) iletişim kutusu görüntülenir.

2. Bu ilk iletişim kutusunda *Save* (Kaydet) seçeneğini belirleyin.

Bir dosya tarayıcı açılır.

3. Dosyayı kaydetmek istediğiniz dizine gitmek için dosya tarayıcısını kullanın ve dosyayı kaydetmek için **OK** (Tamam) seçeneğine tıklayın.

Varsayılan dosya adını kullanabilir (config.cbk) ya da yedekleme dosyasını yeniden adlandırabilirsiniz ancak dosyayı .cbk uzantısıyla kaydettiğinizden emin olun.

26.4 Yapılandırmayı Önceden Kaydedilen Bir Dosyadan Geri Yükleme

Bir erişim noktasındaki yapılandırmayı önceden kaydedilen ayarlara geri yüklemek için:

1. *Restore* (Geri Yükle) metin kutusuna yolun tamamını ve dosya adını yazarak ya da **Browse**'a (Gözet) tıklayıp dosyayı seçerek kullanmak istediğiniz yedekleme yapılandırma dosyasını seçebilirsiniz.

(Yalnızca Yedekleme işleviyle oluşturulan ve .cbk yedek yapılandırma dosyası olarak kaydedilen dosyalar [config.cbk gibi] Geri Yükleme işlemi için kullanılabilir.)



Önemli: *Yapılandırma dosyası yalnızca yapılandırma dosyasının alındığı 9160 modelinin aynısında geri yüklenebilir.*

Örneğin, 9160 G2 model bir "9160 Kablosuz Ağ Geçidi", 9160 G2 model "9160 Kablosuz Ağ Geçidi (Çift Telsiz)" cihazında kaydedilen bir yapılandırma dosyasını geri yüklemeyiz.

2. **Restore** (Geri Yükle) düğmesine tıklayın.

Erişim noktası yeniden başlatılır.



Not: ***Restore**'a (Geri Yükle) tıkladığınızda erişim noktası yeniden başlatılır. "Yeniden başlatma" onay iletişim kutusu ve ardından "yeniden başlatılıyor" durum mesajı görüntülenir. Lütfen yeniden başlatma işleminin tamamlanmasını bekleyin (1-2 dakika). Bir dakika bekledikten sonra, bir sonraki adımda açıklandığı gibi Yönetim Web sayfalarına erişmeye çalışın. AP yeniden başlatılana kadar sayfalara erişemezsiniz.*

Erişim noktası yeniden başlatıldıktan sonra sekmelerin birine yeniden tıklayarak (Kullanıcı Arabirimi halen görüntüleniyorsa) ya da erişim noktasının IP adresini tarayıcınıza yazarak Yönetim Web sayfalarına erişin. Artık yapılandırma ayarlarının Yedekleme dosyasından aldığınız orijinal ayarlara geri yüklendiğini görürsünüz.

26.5 Erişim Noktasını Yeniden Başlatma

9160 G2 Kablosuz Ağ Geçidi cihazını bakım amaçlı ya da bir sorun giderme yöntemi olarak şu şekilde yeniden başlatabilirsiniz:

1. *Maintenance > Configuration* (Bakım > Yapılandırma) sekmesine tıklayın.
2. **Restore** (Geri Yükle) düğmesine tıklayın.

Erişim noktası yeniden başlatılır.

26.6 Ürün Yazılımını Yükseltme

9160 G2 Kablosuz Ağ Geçidi cihazının yeni ürün yazılımı sürümleri çıktıkça yeni özelliklerden ve geliştirmelerden faydalanmak için cihazınızdaki ürün yazılımını yükseltebilirsiniz.



Önemli: *Ürün yazılımını, yükseltmekte olduğunuz erişim noktasıyla ilişkili olan kablosuz bir istemciden yükseltmeyin. Bu işlem yükseltmenin başarısız olmasına yol açar. Ayrıca tüm kablosuz istemcilerin ilişkisi kesilmeli ve yeni ilişkilere izin verilmemelidir.*

Bu durumla karşılaşırsanız erişim noktasına erişmek için kablolu bir istemci kullanarak sorunu şu şekilde çözebilirsiniz:

- ***Bilgisayardan erişim noktasına kablolu bir Ethernet bağlantısı oluşturun.***
- ***Yönetim Kullanıcı Arabirimini açın.***

Yükseltme işlemini kablolu istemciyle tekrarlayın.



Not: Bu işlemi her bir erişim noktası için yapmalısınız; ürün yazılımını tüm küme için otomatik olarak yükseltemezsiniz.

Başarılı bir ürün yazılımı yükseltme işleminin erişim noktası yapılandırmasını fabrika varsayılanlarına geri yüklediğini unutmayın. (Bkz. “9160 G2 Kablosuz Ağ Geçidi'nin Varsayılan Ayarları”, sayfa 27.)

Belirli bir erişim noktasındaki ürün yazılımını yükseltmek için:

1. Bu erişim noktasının Yönetim Web sayfalarındaki *Maintenance > Upgrade* (Bakım > Yükseltme) sekmesine gidin.

Upgrade firmware

Model	9160 Wireless Gateway NB (Dual Radio)
Platform	PTX9160G2
Firmware Version	E187k

New Firmware Image

Please note: Uploading the new firmware may take up to 20 seconds. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the upload is complete, a page will be displayed indicating whether the new firmware was uploaded successfully. If successful, the upgrade will proceed automatically.

Geçerli ürün yazılımı sürümüyle ilgili bilgi ekranda görüntülenir ve yeni bir ürün yazılımı imaj dosyasına yükseltme seçeneği yer alır.

2. Yeni Ürün Yazılımı İmaj dosyasının yolunu biliyorsanız *New Firmware Image* (Yeni Ürün Yazılımı İmaj Dosyası) metin kutusuna yazın. Bilmiyorsanız **Browse** (Gözet) düğmesine basın ve ürün yazılımı imaj dosyasını bulun.



Not: Sunulan ürün yazılımı yükseltme dosyası şu formatta olmalıdır:
<FileName>.upgrade.tar

Yükseltme işlemi için <FileName>.bin ya da diğer dosya formatlarını denemeyin. Bu dosyalarla yükseltme yapamazsınız.

26.6.1 Güncelleme

1. Yeni ürün yazılımı imajını uygulamak için **Update** (Güncelle) düğmesine tıklayın. Ürün yazılımı yükseltmesi için Update (Güncelle) düğmesine basıldıktan sonra yükseltme sürecini gösteren bir onay penceresi açılır.
2. Yükseltmeyi onaylamak için **OK** (Tamam) düğmesine basın ve işlemi başlatın.



Önemli: *Ürün yazılımını yükseltme işlemi Update (Güncelle) düğmesine ve ardından açılan onay penceresindeki OK (Tamam) düğmesine tıkladıktan sonra başlar. Yükseltme işlemi birkaç dakika sürebilir. Yükseltme işlemi devam ederken erişim noktası kullanılamaz. Yükseltme işlemi devam ederken erişim noktasını kapatmayın. Yükseltme tamamlandığında erişim noktası yeniden başlatılır ve fabrika varsayılan ayarları kullanılarak normal şekilde çalışmaya devam eder.*

26.6.2 Ürün Yazılımı Yükseltmesini Doğrulama

Ürün yazılımı yükseltmesinin başarıyla tamamlandığını doğrulamak için *Upgrade* (Yükseltme) sekmesinde (ve *Basic Settings* [Temel Ayarlar] sekmesinde) görüntülenen ürün yazılımı sürümünü kontrol edin. Yükseltme başarılı olduysa güncellenen sürüm adı ya da numarası belirtilir.

27.1 Fiziksel Özelliklerle İlgili Açıklamalar	323
27.2 Çevresel Gereksinimler	323
27.3 AC Güç Gereksinimleri	323
27.4 Ethernet Üzerinden Güç Gereksinimleri	323
27.5 İşlemci ve Bellek	324
27.6 Ağ Arabirimleri	324
27.7 Telsizler	324



Not: Performans teknik özellikleri nominaldir ve önceden bildirimde bulunulmaksızın değiştirilebilir.

27.1 Fiziksel Özelliklerle İlgili Açıklamalar

Muhafaza:	Siyah, FR2000 bay blend malzemesi
Boyutlar:	$\leq 30 \times 20 \times 12,5$ cm (11,8 x 7,9 x 4,9 inç)
Ağırlık:	$\leq 2,25$ kg (5,0 lbs.) (telsizler, antenler ve seçenekler hariç)

27.2 Çevresel Gereksinimler

Çalıştırma Sıcaklığı:	0°C - 45°C (32°F - 113°F)
Çalıştırma Bağıl Nemi:	%10 - %90
Saklama Sıcaklığı:	0°C - 70°C (32°F - 158°F)
Toz ve Yağmur:	IP42 ya da üzeri
Titreşim:	EH0002 (Yalnızca nakliye sırasında titreşim)
Güvenilirlik:	MTBF 25.000 Saat (MIL-HDBK-217F)

27.3 AC Güç Gereksinimleri

Standart bir IEC320 konektörü aracılığıyla AC evrensel giriş. Bağlandığında Ethernet Üzerinden Güç (802.3af algılama) devre dışı kalır.

Giriş voltajı:	100 - 240 V AC nominal
Akım:	5,0 A maksimum



Uyarı: *Dışarı kurulmuş bir antene bağlanan tüm 9160 G2'lerde zemin vidası (hızlı montaj yuvasında bulunur) ile uygun bir zemin bağlantı noktası arasına uzunluğu 3 metreyi aşmayan bir zemin kablosu bağlanmalıdır.*

27.4 Ethernet Üzerinden Güç Gereksinimleri

IEEE 802.3af ile uyumluluk (AC gücü bağlandığında devre dışı kalır).

Giriş voltajı:	37 - 57 V DC
Yerleşik	

Güç Kaynakları:	2,5 W (Ethernetten gelen tam 12,5 watt'ta $\eta=0,8$ olduğu varsayılır)
İki 802.11b telsiz:	4 W
Ana İşlem Kartı:	6 W

27.5 İşlemci ve Bellek

Intel IXP420 işlemci, 266 MHz
8 MB Flash ROM
32 MB SDRAM

27.6 Ağ Arabirimleri

Yerleşik Ethernet: 10BaseT/100BaseT (10/100 Mb/sn) kart,
otomatik anlaşıma, yarı ve tam iki yönlü.
Veri hızı otomatik algılanır.

27.7 Telsizler

Entegre anten olmadan Mini-PCI kart 802.11A/G telsiz

Entegre anten olmadan Mini-PCI kart 802.11G telsiz

Aktarım Gücü	FCC ülkeleri için 100 mW; ETSI için 50 mW
Frekans Aralığı	2,4 - 2,5 GHz (802.11b/g); 5,15 - 5,825 GHz (802.11a)
Veri Hızı	802.11b: 1; 2; 5,5; 11 Mb/sn 802.11a/g: 6; 9; 12; 18; 24; 36; 48; 54 Mb/sn
Kanal Sayısı	FCC: 11 (802.11b/g) ve 12 (802.11a) ETSI: 13 (802.11b/g) ve 19 (802.11a) Çin: 13 (802.11b/g) ve 4 (802.11a)



Not: Tüm 802.11a kanalları çakışmayan kanallardır. 2,4 GHz bantında çakışmayan kanallar bulunur.

RA1001A - Dar Bant Telsiz

Psion Teklogix Özel Dar Bant Modülasyonu (2/4 seviye FSK)

Tip III bilgisayar Kartı Form Faktörü

Aktarım Gücü	1 W ya da 0,5 W
Frekans Aralığı	403-422 MHz, 419-435 MHz, 435-451 MHz, 450-470 MHz, 464-480 MHz, 480-496 MHz, 496-512 MHz
Rx Hassasiyeti	19,2 kb/sn'de (4 seviye FSK) -110 dBm'den az
Veri hızları	4800 b/sn; 9600 b/sn; 19,2 kb/sn

BAĞLANTI NOKTASI İŞLEV ŞEMALARI VE KABLO ŞEKİLLERİ

A.1 Konsol Bağlantı Noktası

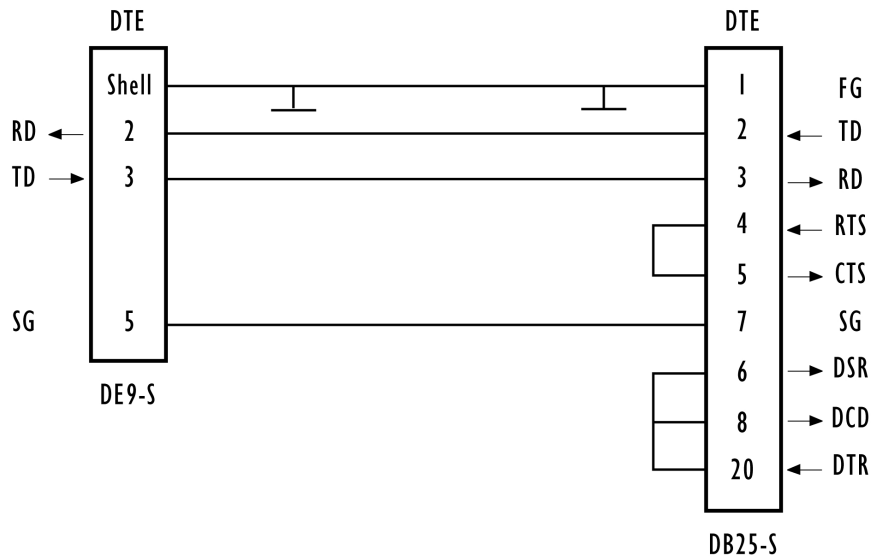
Pin No.	Ad	İşlev	Yön
3	TD	Veri Aktarma	Dışarı
2	RD	Veri Alma	İçeri
5	SG	Sinyal Topraklama	–
4*	DTR	Veri Terminali Hazır	Dışarı
7*	RTS	Gönderme İsteği	Dışarı

* her zaman yukarı çekilir

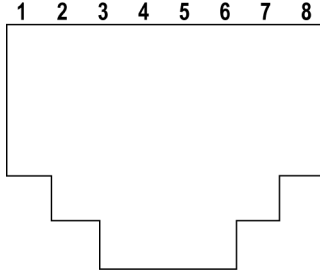
A.2 Seri Kablo Açıklamaları

Kablo No.	İşlev	Bağlantı	Standart Uzunluk
19387	9160 G2'den Konsola	Doğrudan	6 ft

Konsol Bağlantı Noktası Kablo No. 19387



A.3 RJ-45 Konektör İşlev Şemaları (10BaseT/100BaseT Ethernet)



AC kullanan 9160 G2		Ethernet Üzerinden Güç kullanan 9160 G2*	
1	TD+	1	TD+
2	TD-	2	TD-
3	RD+	3	RD+
4	Kullanılmaz	4	
5	Kullanılmaz	5	
6	RD-	6	RD-
7	Kullanılmaz	7	
8	Kullanılmaz	8	
		* 9160 G2, Ethernet üzerinden güç sağlayan sistemlerdeki veri satırı çiftlerinde (1,2) ve (3,6) 48 V DC güç öngерilimini de kabul eder.	



Not: Genellikle Çift Bükümlü kabloyu (10BaseT ya da 100BaseT) hub'a bağlamak için doğrudan bağlantı gerekir.

KABLOSUZ İSTEMCİLERDE/RADIUS SUNUCUSUNDA GÜVENLİK AYARLARI

B.1 Ağ Altyapısı; Dahili ya da Harici Kimlik Doğrulama Sunucusu Arasında Seçim Yapma	8
B.1.1 Dahili Kimlik Doğrulama Sunucusunu (EAP-PEAP) Kullanma.	8
B.1.2 EAP-TLS Sertifikalı ya da EAP-PEAP'li Harici RADIUS Sunucusu Kullanma.	8
B.2 Kablosuz İstemci Yazılımının Güncel Olduğundan Emin Olma	9
B.3 Microsoft Windows Kablosuz İstemci Güvenlik Ayarlarına Erişme	9
B.4 İstemciyi Güvenli Olmayan (Güvenlik Ayarının "None" (Yok) Olduğu) Bir Ağa Erişmesi İçin Yapılandırma	11
B.5 İstemcide Statik WEP Güvenliği Yapılandırma	12
B.6 İstemcide IEEE 802.1x Güvenliği Yapılandırma	15
B.6.1 EAP/PEAP Kullanan IEEE 802.1x İstemci.	15
B.6.2 EAP/TLS Sertifikası Kullanan IEEE 802.1x İstemci.	18
B.7 İstemcide WPA/WPA2 Kurumsal (RADIUS) Güvenliği Yapılandırma.	22
B.7.1 EAP/PEAP Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci	22
B.7.2 EAP-TLS Sertifikası Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci	26
B.8 İstemcide WPA/WPA2 Kişisel (PSK) Güvenliği Yapılandırma	30
B.9 9160 G2'yi Tanıması İçin Harici Bir RADIUS Sunucusu Yapılandırma	33
B.10 İstemci İçin TLS-EAP Sertifikası Edinme	37
B.11 VLAN etiketleri için RADIUS Sunucusu Yapılandırma	43
B.11.1 RADIUS Sunucusu Yapılandırma	43

Kullanıcılar genellikle pek çok farklı ağa (erişim noktasına) erişmek için kablosuz istemcilerinde güvenlik ayarları yapılandırır. "Mevcut Ağlar" listesi, istemcinin konumuna ve o konumda hangi AP'lerin çevrimiçi ve algılanabilir olduğuna bağlıdır.¹ AP, istemci tarafından algılandığında ve AP için güvenlik ayarları yapılandırıldığında AP, istemcinin ağ listesinde kalır ancak duruma bağlı olarak ulaşılabilir ya da ulaşılabilir olarak görünür. Bağlanmak istediğiniz her ağ (AP) için istemcideki güvenlik ayarlarını o ağ tarafından kullanılan güvenlik moduyla eşleştirecek şekilde yapılandırın.

Kablosuz bağlantı için Microsoft® Windows® istemci yazılımını kullanan istemcilerde güvenlik ayarları kurma işlemini anlatıyoruz. Windows istemci yazılımı, Windows masaüstü ve dizüstü bilgisayarlarda geniş biçimde kullanıldığından örnek olarak verilmiştir. İstemcide farklı bir yazılım kullanırsanız (Funk Odyssey® gibi) bu prosedürler çok az farklılık gösterir ancak ihtiyacınız olan yapılandırma bilgisi değişmez.



Not: Güvenlik yapılandırmasında önerilen sıralama şöyledir: (1) erişim noktasında güvenliği ayarlayın, (2) her bir kablosuz istemcide güvenliği ayarlayın.

İlk başta güvenli olmayan bir kablosuz istemciden herhangi bir güvenliğin ayarlanmadığı ("None" [Yok]) bir erişim noktasına bağlanacağınızı varsayıyoruz. Bu ilk bağlantıyla, erişim noktasının Yönetim Web sayfalarına gidip bir güvenlik modu (Security [Güvenlik]) yapılandırabilirsiniz.

*Erişim noktasını bir güvenlik ayarıyla yeniden yapılandırdıktan sonra **Update** (Güncelle) seçeneğine tıkladığınızda kablosuz istemcinin AP ile ilişkisi kesilir ve AP Yönetim Web sayfası bağlantısını yitirir. Bazı durumlarda istemciyi yapılandırmadan önce AP güvenlik ayarlarında ek değişiklikler yapmanız gerekebilir. Bu nedenle yedek bir Ethernet (Kablolu) bağlantınız olmalıdır.*

Aşağıdaki bölümlerde 9160 G2 Kablosuz Ağ Geçidi cihazı tarafından sunulan bir ağın kablosuz istemcilerindeki desteklenen güvenlik modlarının her birinin nasıl yapılandırıldığı anlatılmaktadır.

¹Ağ adının yayınlanmasını engelleyecek şekilde ayarlanan erişim noktaları bu durum için istisnadır. Bu durumda SSID, istemcinin Mevcut Ağlar listesinde yer almaz. İstemcinin bu AP'ye bağlanabilmesi için ağ bağlantı özelliklerinde yapılandırılan ağ adını tam olarak bilmesi gerekir.

B.1 Ağ Altyapısı; Dahili ya da Harici Kimlik Doğrulama Sunucusu Arasında Seçim Yapma

Açık Anahtar Altyapıları (PKI), Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmeti (RADIUS) sunucuları ve Sertifika Yetkilisi (CA) gibi ağ güvenlik yapılandırmaları, Kimlik Doğrulama, Yetkilendirme ve Hesaplama (AAA) özelliklerini nasıl sağladıklarına bağlı olarak bir yapılanmadan diğerine büyük oranda değişiklik gösterebilir. Sonuç olarak, istemcilerin kablosuz ağa erişmek için güvenliği nasıl yapılandıracağını altyapınızın özellikleri belirler. Bu belge, tüm olası senaryoları tahmin etmek ve bunların üzerine eğilmek yerine 9160 G2 Kablosuz Ağ Geçidi cihazının desteklediği her istemci yapılandırması türü için genel açıklamalar sunar.

B.1.1 Dahili Kimlik Doğrulama Sunucusunu (EAP-PEAP) Kullanma

Bir RADIUS sunucunuz ya da PKI altyapınız yoksa ve/veya bu kavramların çoğuna aşina değilseniz 9160 G2 Kablosuz Ağ Geçidi cihazını, AP'de *Dahili Kimlik Doğrulama Sunucusu* kullanan bir güvenlik kurmanızı şiddetle tavsiye ederiz. Bu da, AP'yi ya IEEE 802.1x ya da WPA/WPA2 Kurumsal (RADIUS) güvenlik moduyla kurmak anlamına gelir. (Dahili kimlik doğrulama sunucusu, EAP-PEAP kimlik doğrulama protokolünü kullanır.)

- 9160 G2 Kablosuz Ağ Geçidi cihazı IEEE 802.1x modunu ve Dahili Kimlik Doğrulama Sunucusunu kullanacak şekilde yapılandırıldıysa kablosuz istemcileri “EAP/PEAP Kullanan IEEE 802.1x İstemci”, sayfa B-15'te anlatıldığı gibi yapılandırın.
- 9160 G2 Kablosuz Ağ Geçidi cihazı WPA/WPA2 Kurumsal (RADIUS) modunu ve Dahili Kimlik Doğrulama Sunucusunu kullanacak şekilde yapılandırıldıysa kablosuz istemcileri “EAP/PEAP Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci”, sayfa B-22'de anlatıldığı gibi yapılandırın.

B.1.2 EAP-TLS Sertifikalı ya da EAP-PEAP'li Harici RADIUS Sunucusu Kullanma

Harici bir RADIUS sunucunuz ve PKI/CA kurulumunuz varsa burada verilen temel önerilerin ötesinde güvenlik altyapınıza uygun istemci güvenlik seçeneklerini nasıl yapılandıracağınızı bildiğinizi varsayınız. Burada değinilen ve özellikle RADIUS - PKI ortamındaki istemci güvenlik yapılandırmasıyla ilgili olan konular şunlardır:

- “EAP/TLS Sertifikası Kullanan IEEE 802.1x İstemci”, sayfa B-18.
- “EAP-TLS Sertifikası Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci”, sayfa B-26.
- “9160 G2'yi Tanıması İçin Harici Bir RADIUS Sunucusu Yapılandırma”, sayfa B-33.
- “İstemci İçin TLS-EAP Sertifikası Edinme”, sayfa B-37.

Bu belgede, harici bir RADIUS sunucusu olan EAP-PEAP istemcilerinin nasıl yapılandırıldığıyla ilgili ayrıntılı bilgi sunulmamıştır.

B.2 Kablosuz İstemci Yazılımının Güncel Olduğundan Emin Olma

Başlamadan önce, kablosuz istemcilerde kullanılan hizmet paketlerinin, yamaların, sürücülerin yeni sürümlerinin ve diğer destekleyici teknolojilerin hızla değiştiğini unutmayın. İstemci güvenliği kurulumunda en sık karşılaşılan sorun, istemcide doğru sürücüye ya da sürücü güncellemelerine sahip olmamaktır. Örneğin, istemciye WPA kuruyorsanız nispeten yeni bir teknoloji olan WPA'yı destekleyen bir sürücünün istemcide yüklü olduğundan emin olun.

Şu an piyasada satılan pek çok istemci kartı bile en güncel sürücülerle piyasaya sürülmüyor.

B.3 Microsoft Windows Kablosuz İstemci Güvenlik Ayarlarına Erişme

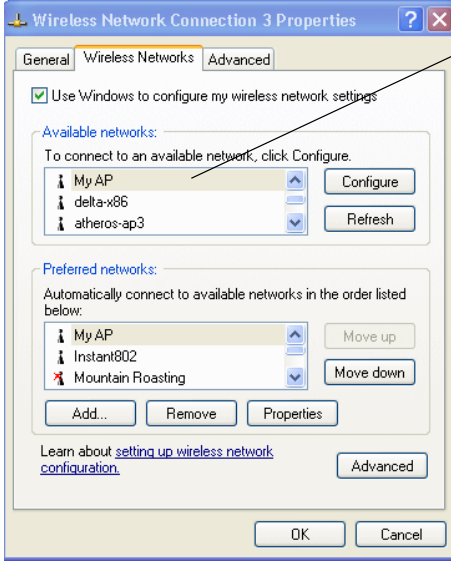
Genel olarak Windows XP'de bir kablosuz istemcinin güvenlik özelliklerine erişmenin iki yolu vardır:

1. Windows görev çubuğundaki *Kablosuz Bağlantı* simgesinden.
 - Görev çubuğunuzdaki Kablosuz bağlantı simgesine sağ tıklayın ve **View available wireless networks** (Kullanılabilir kablosuz ağları görüntüle) seçeneğini belirleyin.
 - Bağlanmak istediğiniz ağın SSID'sini seçin ve *Wireless Network Connection Properties* (Kablosuz Ağ Bağlantı Özellikleri) iletişim kutusunun görüntülenmesi için **Advanced** (Gelişmiş) düğmesine tıklayın.

VEYA

1. Görev çubuğunun sol ucundaki Windows *Start* (Başlat) menüsünden:
 - Ağ Bağlantıları penceresinin görüntülenmesi için görev çubuğundaki Windows *Start* (Başlat) menüsünden **Start, My Network Places**'ı (Başlat, Ağ Bağlantılarım) seçin.
 - *Network Connections* (Ağ Bağlantıları) penceresinin görüntülenmesi için soldaki *Network Tasks* (Ağ Görevleri) menüsünden **View Network Connections** (Ağ Bağlantılarını Görüntüle) seçeneğine tıklayın.
 - Yapılandırmak istediğiniz *Kablosuz Ağ Bağlantısını* seçin ve **View available wireless networks**'ü (Kullanılabilir kablosuz ağları görüntüle) seçin.
 - Bağlanmak istediğiniz ağın SSID'sini seçin ve *Wireless Network Connection Properties* (Kablosuz Ağ Bağlantı Özellikleri) iletişim kutusunun görüntülenmesi için **Advanced** (Gelişmiş) düğmesine tıklayın.

Wireless Networks (Kablosuz Ağlar) sekmesi (otomatik olarak görüntülenmesi gerekir), *Available networks* (Kullanılabilir ağlar) ve *Preferred networks*'ü (Tercih edilen ağlar) listeler.



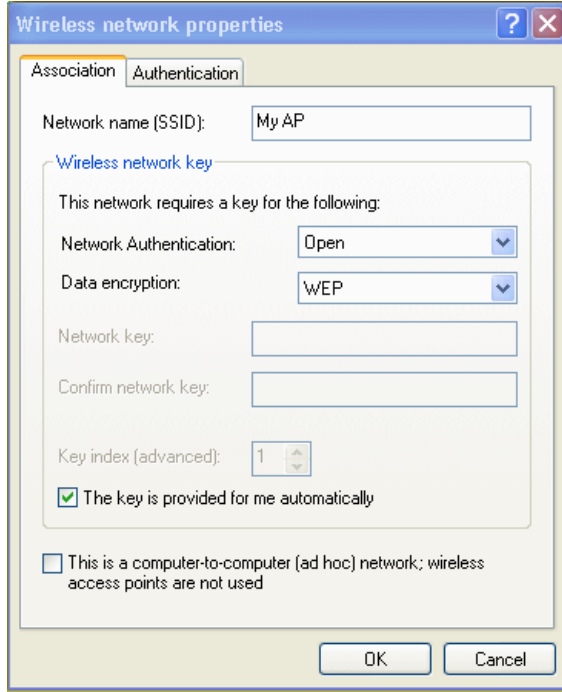
Mevcut ağlar listesi istemci konumuna göre değişiklik gösterir. İstemci tarafından algılanan her ağ (ya da erişim noktası) bu listede yer alır. ("Refresh" [Yenile], listeyi yeni bilgilerle günceller.)

Bağlanmak istediğiniz her ağ için istemcideki güvenlik ayarlarını, o ağda kullanılan güvenlik ayarlarıyla aynı olacak şekilde yapılandırın.

Not: AP, ağ adının yayınlanmasını engelleyecek şekilde yapılandırılmışsa ağ adı bu listede görünmez. Bu durumda, ağa bağlanabilmek için ağ adını tam olarak yazmanız gerekir.

2. *Available networks* (Kullanılabilir Ağlar) sekmesinden, bağlanmak istediğiniz ağın SSID'sini seçin ve **Configure** (Yapılandır) seçeneğine tıklayın.

Bu işlem, seçilen ağ için *Association* (İlişkilendirme) ve *Authentication* (Kimlik Doğrulama) sekmelerini içeren *Wireless Network Connection Properties* (Kablosuz Ağ Bağlantısı Özellikleri) iletişim kutusunun görüntülenmesini sağlar.



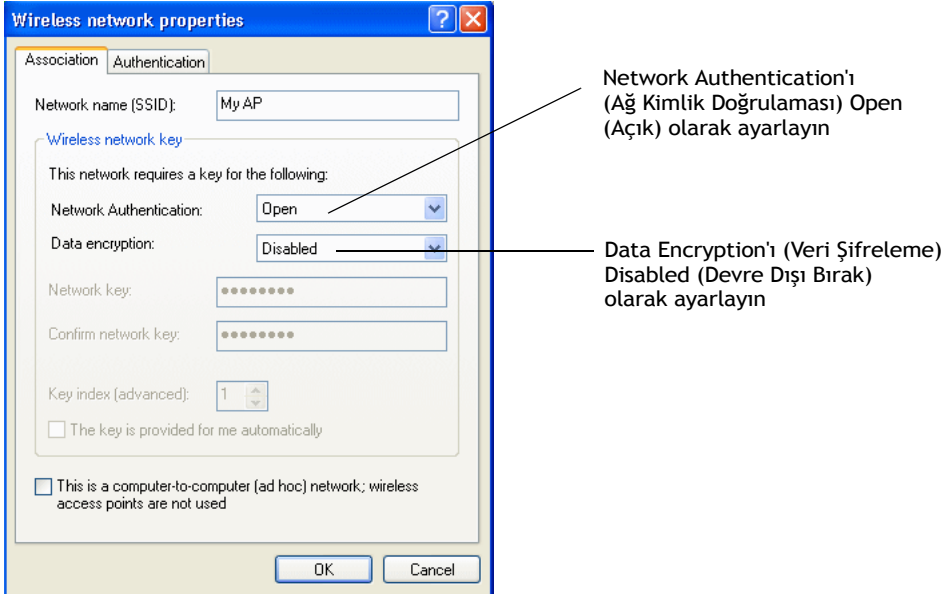
Bu iletişim kutusunu ileriki bölümlerde anlatılan tüm çeşitli istemci güvenliklerini yapılandırmak için kullanın. Görüntülediğiniz *Wireless Network Properties* (Kablosuz Ağ Özellikleri) iletişim kutusunun, yapılandırdığınız kablosuz istemcide ulaşmak istediğiniz ağın Ağ Adına (SSID) ait olduğundan emin olun.

B.4 İstemciyi Güvenli Olmayan (Güvenlik Ayarının "None" (Yok) Olduğu) Bir Ağa Erişmesi İçin Yapılandırma

Bağlanmak istediğiniz erişim noktası ya da kablosuz ağ hiçbir güvenlik olmayacak şekilde "None" (Yok) olarak yapılandırılmışsa istemciyi uygun şekilde yapılandırmanız gerekir. Bağlanmak için hiçbir güvenlik kullanmayan bir istemci, aşağıda açıklandığı gibi **Open** (Açık) Ağ Kimlik Doğrulaması ve **Disabled** (Devre Dışı) Veri Şifreleme ile yapılandırılmıştır.

Güvenli olmayan bir ağa bağlanacak olan bir istemcinizde güvenlik yapılandırması varsa istemci ve erişim noktası güvenlik yapılandırmaları eşleşmeyeceğinden dolayı güvenlik ayarları, istemcinin ağa başarıyla erişmesini önleyebilir.

İstemciyi hiçbir güvenlik kullanmayacak şekilde yapılandırmak için istemci *Network Properties* (Ağ Özellikleri) iletişim kutusunu görüntüleyin ve aşağıdaki ayarları yapılandırın.



Tablo B.1 İlişkilendirme Ayarları

Network Authentication (Ağ Kimlik Doğrulaması)	Open (Açık)
Data Encryption (Veri Şifreleme)	Disabled (Devre Dışı)

B.5 İstemcide Statik WEP Güvenliği Yapılandırma

Statik *Kablolu Eş Değer* (WEP), kablosuz bir ağda dolaşan verileri statik (değişmeyen) bir anahtar kullanarak şifreler. Şifreleme algoritması RC4 adı verilen bir "şifre dizisi"dir. Erişim noktası verileri istemci istasyonuna iletmek için bir anahtar kullanır. Her istemci erişim noktasından aldığı verinin şifresini çözmek için aynı anahtarı kullanmalıdır. Farklı istemciler, erişim noktasına veri aktarırken farklı anahtarlar kullanabilir. (Hepsi aynı anahtarı da kullanabilir ancak bu şekilde bir istasyon başka bir istasyon tarafından gönderilen verinin şifresini çözebileceği için bu yöntem daha az güvenlidir.)

9160 G2 Kablosuz Ağ Geçidi cihazını Statik WEP güvenlik modunda kullanmak için yapılandırdıysanız...

Basic Settings
User Management
Cluster
Access Points
Sessions
Channel Management
Wireless Neighborhood
Security
Status
Interfaces
Events
Transmit/Receive
Client Associations
Neighboring Access Points
Manage

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: Static WEP

Transfer key index: 1

Key Length: ☐ 64 bits ☒ 128 bits ☐ 152 bits

Key Type: ☐ ASCII ☒ Hex

WEP Keys: (Characters required: 26)

1: 012345678901234567890123

2: 012345678901234567890123

3:

4:

Authentication: ☒ Open system ☐ Shared key

Update

...WEP güvenliğini her istemcide aşağıdaki gibi yapılandırın.

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

Open'i (Açık) ya da Shared'ı (Paylaşılan) seçin

Data Encryption (Veri Şifreleme) modu olarak WEP'i seçin

Erişim noktasında aktarma anahtarı dizini konumuna ayarlanan WEP anahtarlarıyla eşleşen bir ağ adı girin (ve onaylamak için tekrar yazın)

İsteğe bağlı olarak istemciden erişim noktasına veri göndermek için farklı bir aktarma anahtarı dizini ayarlayın

Otomatik anahtar atama seçeneğini devre dışı bırakın

Tablo B.2 İlişkilendirme Ayarları

<i>Network Authentication (Ağ Kimlik Doğrulaması)</i>	<p>Bu seçeneği erişim noktasında nasıl yapılandırıđınıza bađlı olarak Open (Açık) ya da Shared (Paylaşılan).</p> <p>Not: Bu erişim noktasındaki Kimlik Doğrulama Algoritması Both (İkisi de) olarak ayarlandıysa Shared (Paylaşılan) ya da Open (Açık) olarak ayarlanan istemciler AP ile ilişkilenebilir. WEP'i Paylaşılan modda kullanmak üzere yapılandırılan istemcilerin AP ile ilişkilenebilmesi için geçerli bir WEP anahtarının olması gerekir. WEP'i Açık sistem olarak kullanmak üzere yapılandırılan istemciler geçerli bir WEP anahtarları olmasa bile AP ile ilişkilenebilirler (ancak verileri görüntülemek ve veri alışverişi yapmak için geçerli bir anahtar gerekecektir). Daha fazla bilgi için erişim noktasındaki Çevrimiçi Yardıma göz atın.</p>
<i>Data Encryption (Veri Şifreleme)</i>	WEP
<i>Network Key (Ağ Anahtarı)</i>	<p>Aktarma Anahtarı Dizini konumunda, erişim noktasının <i>Security settings</i> (Güvenlik ayarları) kısmında girdiđiniz WEP anahtarını yazın.</p> <p>Örneđin, erişim noktasındaki Aktarma Anahtarı Dizini 1'e ayarlandıysa istemci Ağ Anahtarı, erişim noktasında girdiđiniz WEP Anahtarını WEP Anahtarı 1 olarak belirler.</p>
<i>Key Index (Anahtar Dizini)</i>	<p>Erişim noktasının <i>Security</i> (Güvenlik) sayfasında belirlenen WEP anahtarlarından hangisinin istemciden erişim noktasına veri aktarırken kullanılacağını belirlemek için anahtar dizini ayarlayın.</p> <p>Örneđin, bu değeri 1, 2, 3 ya da 4'e ayarlayabilirsiniz (erişim noktasında bu dört WEP anahtarı da yapılandırdıysanız).</p>
<i>The key is provided for me automatically (Anahtar bana otomatik olarak sađlandı)</i>	Bu seçeneđi devre dıřı bırakın (kutunun seçimini kaldırmak için tıklayın).
<i>Enable IEEE 802.1x authentication for this network (IEEE 802.1x kimlik dođrulamayı bu ağ için etkinleřtir)</i>	<p>IEEE 802.1x kimlik dođrulamanın devre dıřı olduđundan emin olun (kutu seçilmemiř olmalıdır).</p> <p>(Şifreleme modu WEP olarak ayarlandıđında kimlik dođrulama otomatik olarak devre dıřı kalır.)</p>

Tablo B.3 Kimlik Doğrulama Ayarları

<i>Enable IEEE 802.1x authentication for this network (IEEE 802.1x kimlik dođrulamayı bu ağ için etkinleřtir)</i>	<p>IEEE 802.1x kimlik dođrulamanın devre dıřı olduđundan emin olun (kutu seçilmemiř olmalıdır).</p> <p>(Şifreleme modu WEP olarak ayarlandıđında kimlik dođrulama otomatik olarak devre dıřı kalır.)</p>
---------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Wireless Network Properties (Kablosuz Ağ Özellikleri) iletişim kutusunda **OK** (Tamam) düğmesine basarak deđişikliklerinizi kaydedin ve iletişim kutusunu kapatın.

Kablosuz Ağ Statik WEP İstemcisiyle Bağlanma

Statik WEP istemcilerinin artık erişim noktalarıyla ilişkilenebilmesi ve kimlik doğrulamasını gerçekleştirebilmesi gerekir. İstemci olarak sizden WEP anahtarı istenmez. Bağlandığınızda istemci güvenlik ayarlarında yapılandırılan WEP anahtarı otomatik olarak kullanılır.

B.6 İstemcide IEEE 802.1x Güvenliği Yapılandırma

IEEE 802.1x, anahtar yönetimi için bağlantı noktası tabanlı kimlik doğrulama ve altyapı tanımlayan standarttır. *Genişletilebilir Kimlik Doğrulama Protokolü* (EAP) mesajları, LAN üzerinden EAP Kuşatma (EAPOL) adlı bir protokol kullanılarak bir IEEE 802.11 kablosuz ağı üzerinden gönderilir. IEEE 802.1x, periyodik olarak yenilenen ve dinamik şekilde oluşturulan anahtarlar sunar. Bir RC4 şifre dizisi, her 802.11 çerçevesinin çerçeve gövdesini ve döngüsel artıklık denetimini (CRC) şifrelemek için kullanılır.

B.6.1 EAP/PEAP Kullanan IEEE 802.1x İstemci

9160 G2 Kablosuz Ağ Geçidi cihazındaki Dahili Kimlik Doğrulama Sunucusu, burada "EAP/PEAP" olarak bahsedilen *Korumalı Genişletilebilir Kimlik Doğrulama Protokolünü* (EAP) kullanır.

- 9160 G2 Kablosuz Ağ Geçidi cihazında Dahili Kimlik Doğrulama Sunucusunu "IEEE 802.1x" güvenlik moduyla kullanıyorsanız kablosuz istemcileri PEAP kullanacak şekilde ayarlamanız gerekir.
- Ayrıca, EAP/PEAP kullanan harici bir RADIUS sunucunuz da olabilir. Böyle bir sunucunuz varsa şunları yapmanız gerekir:
 1. 9160 G2 Kablosuz Ağ Geçidi cihazını RADIUS sunucu istemcileri listesine ekleyin.

VE

2. IEEE 802.1x kablosuz istemcileri PEAP kullanacak şekilde yapılandırın.



Not: Aşağıdaki örnekte, 9160 G2 Kablosuz Ağ Geçidi ile birlikte gelen Dahili Kimlik Doğrulama sunucusunu kullandığınız varsayılır. Harici RADIUS sunucusu kullanan bir AP'nin istemcilerinden birine EAP/PEAP kuruyorsanız istemci yapılandırması süreci özellikle sertifika doğrulama konusunda bu örnekten biraz daha farklı olacaktır.

9160 G2 Kablosuz Ağ Geçidi cihazını IEEE 802.1x güvenlik modunda kullanmak için yapılandırdıysanız...

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: IEEE802.1x

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☐ Enable radius accounting

Update

...IEEE 802.1x güvenliğini PEAP kimlik doğrulamasıyla birlikte her bir istemcide şu şekilde yapılandırın:

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks:

☒ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

Properties

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel

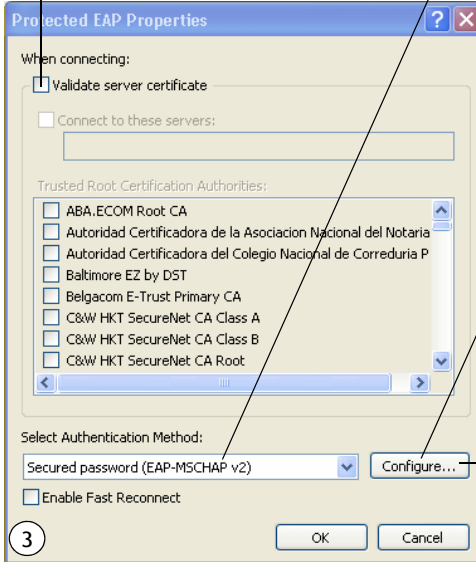
Annotations:

- Open'ı (Açık) seçin
- Data Encryption (Veri Şifreleme) modu olarak WEP'i seçin
- IEEE 8021x kimlik doğrulamayı etkinleştirin (seçmek için tıklayın)
- Protected EAP'yi (PEAP) (Korumalı EAP) seçin
- ... ardından Properties'e (Özellikler) tıklayın
- Otomatik anahtar atamayı etkinleştirin

Validate server certificate'ı
(sunucu sertifikasını doğrula)
devre dışı bırakın

Secured password (EAP-MSCHAP v2)'yi (Güvenli şifre) seçin

... ardından Configure'e (Yapılandır) tıklayın



Windows oturum açma adı ve şifresini
olarak kullanma seçeneğini
devre dışı bırakın



1. *Network Properties* (Ağ Özellikleri) iletişim kutusundaki *Association* (İlişkilendirme) sekmesinde aşağıdaki ayarları yapılandırın.

Tablo B.4 İlişkilendirme Ayarları

<i>Network Authentication</i> (Ağ Kimlik Doğrulaması)	Open (Açık)
<i>Data Encryption</i> (Veri Şifreleme)	WEP Not: Bir RC4 şifre dizisi, her IEEE 802.11 çerçevesinin çerçeve gövdesini ve döngüsel artıklık denetimini (CRC) şifrelemek için kullanılır. Bu algoritma, Statik WEP için kullanılan şifreleme algoritmasıyla aynıdır, bu yüzden bu mod için istemcide yapılandırılan veri şifreleme yöntemi WEP'tir.
<i>This key is provided for me automatically</i> (Bu anahtar bana otomatik olarak sağlandı)	Bu seçeneği etkinleştirin (seçmek için tıklayın).

2. *Authentication* (Kimlik Doğrulama) sekmesinde bu ayarı yapılandırın.

Tablo B.5 Kimlik Doğrulama Ayarları

EAP Type (EAP Türü)	Protected EAP'yi (PEAP) (Korumalı EAP) seçin.
---------------------	-----------------------------------------------

3. *Protected EAP Properties* (Korumalı EAP Özellikleri) iletişim kutusunu görüntülemek için **Properties** (Özellikler) seçeneğine tıklayın ve aşağıdaki ayarları yapılandırın.

Tablo B.6 Korumalı EAP Özellikleri Ayarları

Validate Server Certificate (Sunucu Sertifikasını Doğrula)	Bu seçeneği devre dışı bırakın (kutunun seçimini kaldırmak için tıklayın). Not: Bu örnekte AP üzerindeki Dahili Kimlik Doğrulama sunucusunu kullandığınız varsayılır. Harici RADIUS sunucusu kullanan bir AP'nin istemcilerinden birine EAP/PEAP kuruyorsanız altyapınıza bağlı olarak sertifika doğrulamayı kullanabilir ve bir sertifika seçebilirsiniz.
Select Authentication Method (Kimlik Doğrulama Yöntemi Seçme)	Secured password (EAP-MSCHAP v2)'yi (Güvenli şifre) seçin.

4. *EAP MSCHAP v2 Properties* (EAP MSCHAP v2 Özellikleri) iletişim kutusunu görüntülemek için **Configure** (Yapılandır) seçeneğine tıklayın.

Bu iletişim kutusunda *Automatically use my Windows logon name ...etc* (Windows oturum açma adımı vs. otomatik olarak kullan) seçeneğini **devre dışı bırakın** (seçimini kaldırmak için tıklayın).

Tüm iletişim kutularında **OK** (Tamam) düğmesine tıklayarak (*EAP MSCHAP v2 Properties*'den [EAP MSCHAP v2 Özellikleri] başlayarak) iletişim kutularını kapatın ve değişikliklerinizi kaydedin.

IEEE 802.1x PEAP İstemciyle Kablosuz Ağda Oturum Açma

IEEE 802.1x PEAP istemcilerinin artık erişim noktasıyla ilişkilenebilmesi gerekir. İstemci kullanıcılara ağda kimlik doğrulaması yapmak için kullanıcı adı ve şifre sorulacaktır.

B.6.2 EAP/TLS Sertifikası Kullanan IEEE 802.1x İstemci

Genişletilebilir Kimlik Doğrulama Protokolü (EAP) *Taşıma Katmanı Güvenliği* (TLS) ya da EAP-TLS, akıllı kartların ve sertifikaların kullanımını destekleyen bir kimlik doğrulama protokolüdür. Ağınızda EAP-TLS protokolünü destekleyen harici bir RADIUS sunucunuz varsa bu protokolü hem WPA/WPA2 Kurumsal (RADIUS) hem de IEEE 802.1x modlarıyla kullanabilirsiniz.



Not: İstemcilerin kimlik doğrulaması ve yetkilendirilmesi için IEEE 802.1x modunu EAP-TLS sertifikalarıyla kullanmak istiyorsanız ağınızda yapılandırılmış harici bir RADIUS sunucunuz ve Sertifika Yetkilisi (CA) dahil Açık Anahtar Altyapısı (PKI) sunucunuz olmalıdır. RADIUS sunucusu, PKI ve CA sunucularının yapılandırılmasıyla ilgili açıklamalar bu belgenin kapsamına dahil değildir. Bu ürünlerin yapılandırılmasıyla ilgili bilgi için ürün belgelerine bakın.

Microsoft Windows PKI yazılımıyla ilgili Internette yer alan bazı faydalı başlangıç noktaları şunlardır:

"How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" (Windows 2000 için Açık Anahtar Sertifika Yetkilisini Kurma/Kaldırma):

<http://support.microsoft.com/default.aspx?scid=kb:en-us:231881> ve

"How to Configure a Certificate Server" (Sertifika Sunucusu Kurma):

<http://support.microsoft.com/default.aspx?scid=kb:en-us:318710#3>.

Bu tür bir güvenlik kullanmak için aşağıdakileri yapmanız gerekir:

1. 9160 G2 Kablosuz Ağ Geçidi cihazını RADIUS sunucu istemcileri listesine ekleyin. (Bkz. "9160 G2'yi Tanıması İçin Harici Bir RADIUS Sunucusu Yapılandırma", sayfa B-33.)
2. RADIUS sunucunuzu kullanmak için 9160 G2 Kablosuz Ağ Geçidi cihazınızı yapılandırın ("IEEE 802.1x" güvenlik modu ayarlarının bir parçası olarak RADIUS sunucusu IP adresini sağlayarak).
3. IEEE 802.1x güvenlik modu ve "Akıllı Kart ve diğer Sertifikaları" kullanmak için kablosuz istemcileri bu bölümde anlatıldığı gibi yapılandırın.
4. "İstemci İçin TLS-EAP Sertifikası Edinme", sayfa B-37'te anlatıldığı gibi bu istemci için bir sertifika alın.

9160 G2 Kablosuz Ağ Geçidi cihazını, IEEE 802.1x güvenlik modunu harici bir RADIUS sunucusuyla kullanacak şekilde yapılandırdıysanız...

Basic Settings	<h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: IEEE802.1x</p> <p><input type="checkbox"/> Use internal radius server</p> <p>Radius IP: 10.128.14.14</p> <p>Radius Key: ••••••••</p> <p><input checked="" type="checkbox"/> Enable radius accounting</p> <p>Update</p>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	

...IEEE 802.1x güvenliğini sertifika kimlik doğrulamasıyla birlikte her bir istemcide şu şekilde yapılandırın:

Open'ı (Açık) seçin

Data Encryption (Veri Şifreleme) modu olarak WEP'i seçin

IEEE 802.1x kimlik doğrulamayı etkinleştirin (seçmek için tıklayın)

Smart Card/Certificate'ı (Akıllı Kart/Sertifika) seçin

... ardından Properties'e (Özellikler) tıklayın

Otomatik anahtar atamayı etkinleştirin

1

2

3

Validate server certificate'ı (sunucu sertifikasını doğrula) etkinleştirin (seçmek için tıklayın)

Bu istemciye sertifikanın adını seçin (işaretleyin) (önkoşul olan bir prosedürde RADIUS sunucusundan indirilmiştir)

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: Open

Data encryption: WEP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

☒ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

Properties

☐ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

OK Cancel

Smart Card or other Certificate Properties

When connecting:

☐ Use my smart card

☒ Use a certificate on this computer

☒ Use simple certificate selection (Recommended)

☒ Validate server certificate

☐ Connect to these servers:

Trusted Root Certification Authorities:

☐ Class 2 Public Primary Certification Authority

☐ Class 3 Primary CA

☐ Class 3 Public Primary Certification Authority

☐ Class 3P Primary CA

☐ Class 3TS Primary CA

☒ DC02

☐ Deutsche Telekom Root CA 1

☐ Deutsche Telekom Root CA 2

View Certificate

☐ Use a different user name for the connection

OK Cancel

1. *Network Properties* (Ağ Özellikleri) iletişim kutusundaki *Association* (İlişkilendirme) sekmesinde aşağıdaki ayarları yapılandırın.

Tablo B.7 İlişkilendirme Ayarları

<i>Network Authentication</i> (Ağ Kimlik Doğrulaması)	Open (Açık)
<i>Data Encryption</i> (Veri Şifreleme)	WEP Not: Bir RC4 şifre dizisi, her IEEE 802.11 çerçevesinin çerçeve gövdesini ve döngüsel artıklık denetimini (CRC) şifrelemek için kullanılır. Bu algoritma, Statik WEP için kullanılan şifreleme algoritmasıyla aynıdır, bu yüzden bu mod için istemcide yapılandırılan veri şifreleme yöntemi WEP'tir.
<i>This key is provided for me automatically</i> (Bu anahtar bana otomatik olarak sağlandı)	Bu seçeneği etkinleştirin (seçmek için tıklayın).

2. Bu ayarları *Authentication* (Kimlik Doğrulama) sekmesinde yapılandırın.

Tablo B.8 Kimlik Doğrulama Ayarları

<i>Enable IEEE 802.1x authentication for this network</i> (IEEE 802.1x kimlik doğrulamayı bu ağ için etkinleştir)	Bu seçeneği etkinleştirin (seçmek için tıklayın).
<i>EAP Type</i> (EAP Türü)	Smart Card or other Certificate 'i seçin.

3. *Smart Card or other Certificate Properties* (Akıllı Kart ve Diğer Sertifika Özellikleri) iletişim kutusunu görüntülemek için **Properties** (Özellikler) seçeneğine tıklayın ve **Validate server certificate** (Sunucu sertifikasını doğrula) seçeneğini etkinleştirin.

Tablo B.9 Akıllı Kart ya da Diğer Sertifika Özellikleri Ayarları

<i>Validate Server Certificate</i> (Sunucu Sertifikasını Doğrula)	Bu seçeneği etkinleştirin (kutucuğu seçmek için tıklayın).
<i>Certificates</i> (Sertifikalar)	Görüntülenen sertifika listesinde bu istemcinin sertifikasını seçin.

Tüm iletişim kutularında **OK** (Tamam) düğmesine basarak değişikliklerinizi kaydedin ve iletişim kutularını kapatın.

4. İstemci yapılandırmasını tamamlamak için RADIUS sunucusundan bir sertifika edinmeniz ve bu istemciye yüklemeniz gerekir. Bu işlemin yapılışı hakkında bilgi için bkz. "İstemci İçin TLS-EAP Sertifikası Edinme", sayfa B-37.

Sertifika Kullanan Bir IEEE 802.1x İstemciyle Kablosuz Ağa Bağlanma

IEEE 802.1x istemcilerin artık TLS sertifikalarını kullanarak erişim noktasına bağlanabilmeleri gerekir. Yüklediğiniz sertifika bağlandığınız zaman kullanılmaya başlar, bu nedenle sizden oturum açma bilgileriniz istenmez. Sertifika kimlik doğrulama ve yetkilendirme için otomatik olarak RADIUS sunucusuna gönderilir.

B.7 İstemcide WPA/WPA2 Kurumsal (RADIUS) Güvenliği Yapılandırma

Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmetini (RADIUS) içeren Wi-Fi Korumalı Erişim 2 (WPA2); Gelişmiş Şifreleme Standardı (AES), Sayaç Modu/CBC-MAC Protokolü (CCMP) ve Geçici Anahtar Bütünlüğü Protokolü (TKIP) mekanizmalarını içeren Wi-Fi İttifakı IEEE 802.11h standardının bir uygulamasıdır. Bu mod, kullanıcıların kimliklerinin doğrulanması için bir RADIUS sunucusunun kullanılmasını gerektirir.

Bu güvenlik modu, yalnızca orijinal **WPA**'yi destekleyen kablosuz istemciler için geriye dönük uyumluluk da sunar.

Erişim noktasında WPA/WPA2 Kurumsal (RADIUS) güvenlik modunu yapılandırdıysanız Dahili Kimlik Doğrulama sunucusunu ya da kendi sağladığınız harici bir RADIUS sunucusunu kullanmayı seçebilirsiniz.

9160 G2 Kablosuz Ağ Geçidi Dahili Kimlik Doğrulama Sunucusu, "EAP/PEAP" olarak bilinen *Korumalı Genişletilebilir Kimlik Doğrulama Protokolünü* (EAP) ve Windows tabanlı bir bilgisayar ile erişim noktaları gibi ağ cihazları arasındaki noktadan noktaya (PPP) bağlantıları için kimlik doğrulaması sağlayan *Microsoft Karşılıklı Kimlik Doğrulama İletişim Kuralı Sürüm 2*'yi (MSCHAP V2) destekler.

Bu yüzden, ağınıza (erişim noktasını) güvenlik modu kullanmak üzere yapılandırıp Dahili Kimlik Doğrulamayı kullanacaksanız istemci istasyonlarını WPA/WPA2 Kurumsal (RADIUS) ve EAP/PEAP kullanacak şekilde yapılandırmanız gerekir.

Ağınıza (erişim noktasını) bu güvenlik modunu harici bir RADIUS sunucusuyla kullanmak üzere yapılandırırsanız istemci istasyonlarını WPA/WPA2 Kurumsal (RADIUS) ve RADIUS sunucunuzun kullanmak üzere yapılandırıldığı güvenlik protokolünü kullanacak şekilde yapılandırın.

B.7.1 EAP/PEAP Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci

9160 G2 Kablosuz Ağ Geçidi cihazındaki Dahili Kimlik Doğrulama Sunucusu, "EAP/PEAP" olarak bilinen *Korumalı Genişletilebilir Kimlik Doğrulama Protokolünü* (EAP) kullanır.

- 9160 G2 Kablosuz Ağ Geçidi cihazında Dahili Kimlik Doğrulama Sunucusunu "WPA/WPA2 Kurumsal RADIUS" güvenlik moduyla kullanıyorsanız kablosuz istemcileri PEAP kullanacak şekilde ayarlamanız gerekir.
- Ayrıca, EAP/PEAP kullanan harici bir RADIUS sunucunuz da olabilir. Böyle bir sunucunuz varsa şunları yapmanız gerekir:
 1. 9160 G2 Kablosuz Ağ Geçidi cihazını RADIUS sunucu istemcileri listesine ekleyin.
 2. "WPA/WPA2 Kurumsal (RADIUS)" kablosuz istemcileri PEAP kullanacak şekilde yapılandırın.



Not: Aşağıdaki örnekte, 9160 G2 Kablosuz Ağ Geçidi ile birlikte gelen Dahili Kimlik Doğrulama sunucusunu kullandığınız varsayılır. Harici RADIUS sunucusu kullanan bir AP'nin istemcilerinden birine EAP/PEAP kuruyorsanız istemci yapılandırması süreci özellikle sertifika doğrulama konusunda bu örnekten biraz daha farklı olacaktır.

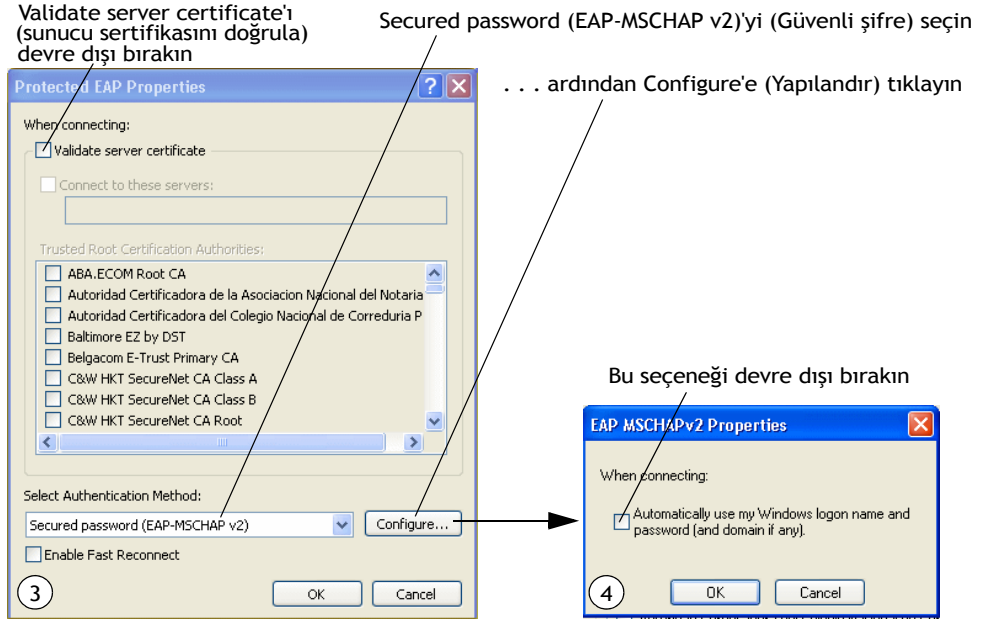
9160 G2 Kablosuz Ağ Geçidi cihazını WPA/WPA2 Kurumsal (RADIUS) güvenlik modunu ve Dahili Kimlik Doğrulama Sunucusu ya da EAP/PEAP kullanan harici bir RADIUS sunucusunu kullanmak için yapılandırdıysanız...

Basic Settings	<h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: WPA Enterprise</p> <p>WPA Versions: <input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2</p> <p><input type="checkbox"/> Enable pre-authentication</p> <p>Cipher Suites: <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> CCMP (AES)</p> <p><input checked="" type="checkbox"/> Use internal radius server</p> <p>Radius IP: 10.128.14.14</p> <p>Radius Key: ••••••••</p> <p><input checked="" type="checkbox"/> Enable radius accounting</p> <p>Update</p>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	
Events	
Transmit/Receive	
Client Associations	

...önce bu erişim noktasında kullanıcı hesapları oluşturun (*User Management* [Kullanıcı Yönetimi] sekmesine gidin)....

...ardından WPA güvenliğini PEAP kimlik doğrulamasıyla birlikte her bir istemcide şu şekilde yapılandırın:

**Ek B: Kablosuz İstemcilerde/RADIUS Sunucusunda Güvenlik Ayarları
EAP/PEAP Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci**



1. *Network Properties* (Ağ Özellikleri) iletişim kutusundaki *Association* (İlişkilendirme) ve *Authentication* (Yetkilendirme) sekmelerinde aşağıdaki ayarları yapılandırın.

Tablo B.10 İlişkilendirme Ayarları

<i>Network Authentication</i> (Ağ Kimlik Doğrulaması)	WPA
<i>Data Encryption</i> (Veri Şifreleme)	<p>Bu seçeneği erişim noktasında nasıl yapılandırdığınıza bağlı olarak TKIP ya da AES.</p> <p>Not: Erişim noktasındaki Şifre Grubu Both (İkisi de) olarak ayarlandığında geçerli bir TKIP anahtarı olan TKIP istemcileri ve geçerli bir CCMP (AES) anahtarı olan AES istemcileri erişim noktasıyla ilişkilenebilir. Daha fazla bilgi için erişim noktasındaki Çevrimiçi Yardıma göz atın.</p>

2. *Authentication* (Kimlik Doğrulama) sekmesinde bu ayarı yapılandırın.

Tablo B.11 Kimlik Doğrulama Ayarları

<i>EAP Type</i> (EAP Türü)	Protected EAP 'yi (PEAP) (Korumalı EAP) seçin
----------------------------	---------------------------------------------------------------

3. *Protected EAP Properties* (Korumalı EAP Özellikleri) iletişim kutusunu görüntülemek için **Properties** (Özellikler) seçeneğine tıklayın ve aşağıdaki ayarları yapılandırın.

Tablo B.12 Korumalı EAP Özellikleri Ayarları

<i>Validate Server Certificate</i> (Sunucu Sertifikasını Doğrula)	Bu seçeneği devre dışı bırakın (kutunun seçimini kaldırmak için tıklayın). Not: Bu örnekte AP üzerindeki Dahili Kimlik Doğrulama sunucusunu kullandığınız varsayılır. Harici RADIUS sunucusu kullanan bir AP'nin istemcilerinden birine EAP/PEAP kuruyorsanız altyapınıza bağlı olarak sertifika doğrulamayı kullanabilir ve bir sertifika seçebilirsiniz.
<i>Select Authentication Method</i> (Kimlik Doğrulama Yöntemi Seçme)	Secured password (EAP-MSCHAP v2) 'yi (Güvenli şifre) seçin.

4. *EAP MSCHAP v2 Properties* (EAP MSCHAP v2 Özellikleri) iletişim kutusunu görüntülemek için **Configure** (Yapılandır) seçeneğine tıklayın.

Bu iletişim kutusunda *Automatically use my Windows logon name* (Windows oturum açma adımı vs. otomatik olarak kullan) seçeneğini **devre dışı bırakın** (seçimini kaldırmak için tıklayın) böylece oturum açtığınızda kullanıcı adınız ve şifreniz sorulur.

Tüm iletişim kutularında **OK** (Tamam) düğmesine tıklayarak (*EAP MSCHAP v2 Properties*'den [EAP MSCHAP v2 Özellikleri] başlayarak) iletişim kutularını kapatın ve değişikliklerinizi kaydedin.

WPA/WPA2 Kurumsal (RADIUS) PEAP İstemciyle Kablosuz Ağda Oturum Açma

"WPA/WPA2 Kurumsal (RADIUS)" PEAP istemcilerinin artık erişim noktasıyla ilişkilenebilmesi gerekir. İstemci kullanıcılara ağda kimlik doğrulaması yapmak için kullanıcı adı ve şifre sorulacaktır.

B.7.2 EAP-TLS Sertifikası Kullanan WPA/WPA2 Kurumsal (RADIUS) İstemci

Genişletilebilir Kimlik Doğrulama Protokolü (EAP) *Taşıma Katmanı Güvenliği* (TLS) ya da EAP-TLS, akıllı kartların ve sertifikaların kullanımını destekleyen bir kimlik doğrulama protokolüdür. Ağınızda EAP-TLS protokolünü destekleyen harici bir RADIUS sunucunuz varsa bu protokolü hem WPA/WPA2 Kurumsal (RADIUS) hem de IEEE 802.1x modlarıyla kullanabilirsiniz.



Not: İstemcilerin kimlik doğrulaması ve yetkilendirilmesi için IEEE 802.1x modunu EAP-TLS sertifikalarıyla kullanmak istiyorsanız ağınızda yapılandırılmış harici bir RADIUS sunucunuz ve Sertifika Yetkilisi (CA) dahil Açık Anahtar Altyapısı (PKI) sunucunuz olmalıdır. RADIUS sunucusu, PKI ve CA sunucularının yapılandırılmasıyla ilgili açıklamalar bu belgenin kapsamına dahil değildir. Bu ürünlerin yapılandırılmasıyla ilgili bilgi için ürün belgelerine bakın.

Microsoft Windows PKI yazılımıyla ilgili Internette yer alan bazı faydalı başlangıç noktaları şunlardır:

"How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" (Windows 2000 için Açık Anahtar Sertifika Yetkilisini Kurma/Kaldırma):

<http://support.microsoft.com/default.aspx?scid=kb;en-us:231881> ve

"How to Configure a Certificate Server" (Sertifika Sunucusu Kurma):

<http://support.microsoft.com/default.aspx?scid=kb;en-us:318710#3>.

Bu tür bir güvenlik kullanmak için aşağıdakileri yapmanız gerekir:

1. 9160 G2 Kablosuz Ağ Geçidi cihazını RADIUS sunucu istemcileri listesine ekleyin. (Bkz. "9160 G2'yi Tanıması İçin Harici Bir RADIUS Sunucusu Yapılandırma", sayfa B-33.)
2. RADIUS sunucunuzu kullanmak için 9160 G2 Kablosuz Ağ Geçidi cihazınızı yapılandırın ("WPA/WPA2 Kurumsal (RADIUS)" güvenlik modu ayarlarının bir parçası olarak RADIUS sunucusu IP adresini sağlayarak).
3. WPA güvenlik modu ve "Akıllı Kart ve diğer Sertifikaları" kullanmak için kablosuz istemcileri bu bölümde anlatıldığı gibi yapılandırın.
4. "İstemci İçin TLS-EAP Sertifikası Edinme", sayfa B-37'te anlatıldığı gibi bu istemci için bir sertifika alın.

9160 G2 Kablosuz Ağ Geçidi cihazını, WPA/WPA2 Kurumsal (RADIUS) güvenlik modunu harici bir RADIUS sunucusuyla kullanacak şekilde yapılandırdıysanız...

Basic Settings
User Management
Cluster
Access Points
Sessions
Channel Management
Wireless Neighborhood
Security
Status
Interfaces
Events
Transmit/Receive
Client Associations

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Enterprise

WPA Versions: ☒ WPA ☒ WPA2
☐ Enable pre-authentication

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

☐ Use internal radius server

Radius IP: 10.128.14.14

Radius Key:

☒ Enable radius accounting

Update

...ardından WPA güvenliğini sertifika kimlik doğrulamasıyla birlikte her bir istemciye şu şekilde yapılandırın:

WPA'yı seçin Data Encryption (Veri Şifreleme) modu olarak TKIP ya da AES'i seçin

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☒ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

1 OK Cancel

Smart Card or other Certificate'ı seçin Certificate ve Authenticate as computer seçeneğini etkinleştirin . . . ardından Properties'e (Özellikler) tıklayın

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks:

☒ Enable IEEE 802.1x authentication for this network

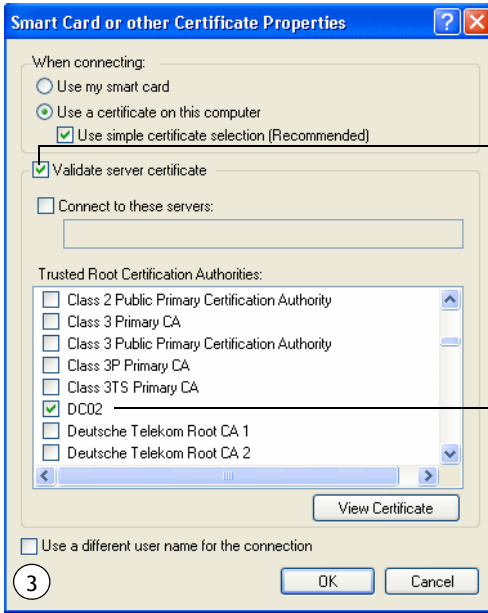
EAP type: Smart Card or other Certificate

Properties

☒ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

2 OK Cancel



Validate server certificate'ı (sunucu sertifikasını doğrula) etkinleştirin (seçmek için tıklayın)

Bu istemciye sertifikanın adını seçin (işaretleyin) (önkoşul olan bir prosedürde RADIUS sunucusundan indirilmiştir)

1. *Network Properties* (Ağ Özellikleri) iletişim kutusundaki *Association* (İlişkilendirme) sekmesinde aşağıdaki ayarları yapılandırın.

Tablo B.13 İlişkilendirme Ayarları

<i>Network Authentication</i> (Ağ Kimlik Doğrulaması)	WPA
<i>Data Encryption</i> (Veri Şifreleme)	Bu seçeneği erişim noktasında nasıl yapılandırıldığınıza bağlı olarak TKIP ya da AES . Not: Erişim noktasındaki Şifre Grubu "Both" (İkisi de) olarak ayarlandığında geçerli bir TKIP anahtarı olan TKIP istemcileri ve geçerli bir CCMP (AES) anahtarı olan AES istemcileri erişim noktasıyla ilişkilenebilir. Daha fazla bilgi için erişim noktasındaki Çevrimiçi Yardıma göz atın.

2. Bu ayarları *Authentication* (Kimlik Doğrulama) sekmesinde yapılandırın.

Tablo B.14 Kimlik Doğrulama Ayarları

<i>Enable IEEE 802.1x authentication for this network (IEEE 802.1x kimlik doğrulamayı bu ağ için etkinleştir)</i>	Bu seçeneği etkinleştirin (seçmek için tıklayın).
<i>EAP Type (EAP Türü)</i>	Smart Card or other Certificate 'ı seçin.

3. *Smart Card or other Certificate Properties* (Akıllı Kart ve Diğer Sertifika Özellikleri) iletişim kutusunu görüntülemek için **Properties** (Özellikler) seçeneğine tıklayın ve **Validate server certificate** (Sunucu sertifikasını doğrula) seçeneğini etkinleştirin.

Tablo B.15 Akıllı Kart ya da Diğer Sertifika Özellikleri Ayarları

<i>Validate Server Certificate</i> (Sunucu Sertifikasını Doğrula)	Bu seçeneği etkinleştirin (kutucuğu seçmek için tıklayın).
<i>Certificates (Sertifikalar)</i>	Görüntülenen sertifika listesinde bu istemcinin sertifikasını seçin.

Tüm iletişim kutularında **OK** (Tamam) düğmesine basarak değişikliklerinizi kaydedin ve iletişim kutularını kapatın.

4. İstemci yapılandırmasını tamamlamak için RADIUS sunucusundan bir sertifika edinmeniz ve bu istemciye yüklemeniz gerekir. Bu işlemin yapılışı hakkında bilgi için bkz. “İstemci İçin TLS-EAP Sertifikası Edinme”, sayfa B-37.

Sertifika Kullanan Bir WPA İstemciyle Kablosuz Ağda Oturum Açma

WPA istemcilerin artık TLS sertifikalarını kullanarak erişim noktasına bağlanabilmeleri gerekir. Yüklediğiniz sertifika bağlandığınız zaman kullanılmaya başlar, bu nedenle sizden oturum açma bilgileriniz istenmez. Sertifika kimlik doğrulama ve yetkilendirme için otomatik olarak RADIUS sunucusuna gönderilir.

B.8 İstemcide WPA/WPA2 Kişisel (PSK) Güvenliği Yapılandırma

Önceden Paylaşılan Anahtarlı (PSK) Wi-Fi Korumalı Erişim (WPA), Geçici Anahtar Bütünlüğü Protokolünü (TKIP), Gelişmiş Şifreleme Algoritmasını (AES) ve Sıyacı Modu/CBC-MAC Protokolü (CCMP) mekanizmalarını içeren IEEE 802.11i'nin Wi-Fi İttifakı altıdır. PSK, istemci kimlik bilgilerinin ilk kontrolü için önceden paylaşılan bir anahtar içerir.

9160 G2 Kablosuz Ağ Geçidi cihazını WPA/WPA2 Kişisel (PSK) güvenlik modunda kullanmak için yapılandırdıysanız...

Basic Settings

User Management

Cluster

Access Points

Sessions

Channel Management

Wireless Neighborhood

Security

Status

Modify Internal Network security settings

☒ Broadcast SSID ☐ Station Isolation

Mode: WPA Personal

WPA Versions: ☒ WPA ☐ WPA2

Cipher Suites: ☒ TKIP ☐ CCMP (AES)

Key: reoreore

Update

...WPA/WPA2 Kişisel (PSK) güvenliğini her istemcide aşağıdaki gibi yapılandırın.

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

☐ The key is provided for me automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

WPA-PSK'yı seçin.

Data Encryption (Veri Şifreleme) modu olarak TKIP ya da AES'i seçin.

Erişim noktasında belirtilen anahtarla eşleşen bir ağ anahtarı seçin (ve tekrar girerek onaylayın).

Tablo B.16 İlişkilendirme Ayarları

<i>Network Authentication (Ağ Kimlik Doğrulaması)</i>	WPA-PSK
<i>Data Encryption (Veri Şifreleme)</i>	Bu seçeneği erişim noktasında nasıl yapılandırdığınıza bağlı olarak TKIP ya da AES . Not: Erişim noktasındaki Şifre Grubu Both (İkisi de) olarak ayarlandığında geçerli bir TKIP anahtarı olan TKIP istemcileri ve geçerli bir CCMP (AES) anahtarı olan AES istemcileri erişim noktasıyla ilişkilenebilir. Daha fazla bilgi için erişim noktasındaki Çevrimiçi Yardıma göz atın.
<i>Network Key (Ağ Anahtarı)</i>	Kullandığınız şifre grubu için erişim noktası Güvenlik ayarlarında girdiğiniz anahtarı girin. Örneğin, erişim noktasındaki anahtar, "012345678" TKIP anahtarını kullanmaya ayarlanmıyorsa TKIP istemcisi bu dizeyi ağ anahtarı olarak belirler.
<i>The key is provided for me automatically (Anahtar bana otomatik olarak sağlandı)</i>	Bu kutucuk diğer ayarlara bağlı olarak otomatik biçimde devre dışı bırakılmalıdır.

Tablo B.17 Kimlik Doğrulama Ayarları

<i>Enable IEEE 802.1x authentication for this network (IEEE 802.1x kimlik doğrulamayı bu ağ için etkinleştir)</i>	IEEE 802.1x kimlik doğrulamanın devre dışı olduğundan (seçilmemiş olduğundan) emin olun. (Şifreleme modu WEP olarak ayarlandığında kimlik doğrulama otomatik olarak devre dışı kalır.)
-----------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Wireless Network Properties (Kablosuz Ağ Özellikleri) iletişim kutusunda **OK** (Tamam) düğmesine basarak değişikliklerinizi kaydedin ve iletişim kutusunu kapatın.

Kablosuz Ağa WPA-PSK İstemcisiyle Bağlanma

WPA-PSK istemcilerinin artık erişim noktalarıyla ilişkilenebilmesi ve kimlik doğrulamasını gerçekleştirebilmesi gerekir. İstemci olarak sizden anahtar istenmez. Bağlandığınızda istemci güvenlik ayarlarında yapılandırdığınız TKIP ya da AES anahtarı otomatik olarak kullanılır.

B.9 9160 G2'yi Tanıması İçin Harici Bir RADIUS Sunucusu Yapılandırma

Ağda çalışan harici bir *Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmeti* (RADIUS) Sunucusu, istemcilere *Açık Anahtar Altyapısında* (PKI) EAP-TLS akıllı kart/sertifika dağıtımını, EAP-PEAP kullanıcı hesabı kurulumunu ve kimlik doğrulamasını destekler. *Harici* RADIUS sunucusu, erişim noktasının dışında bir kimlik doğrulama sunucusudur. Bu, bir ağ RADIUS sunucusunu ve 9160 G2 Kablosuz Ağ Geçidi cihazındaki *Dahili Kimlik Doğrulama Sunucusunu* kullandığınız senaryolarının arasındaki farkı göstermek içindir.

Bu bölüm, "WPA/WPA2 Kurumsal (RADIUS)" ya da "IEEE 802.1x" güvenlik modları için yapılandırılmış belirli bir 9160 G2 Kablosuz Ağ Geçidi cihazının kablosuz istemcilerinden gelen TLS-EAP sertifikalarının kimlik doğrulamasını ve yetkilendirmesini gerçekleştirmek amacıyla harici bir RADIUS sunucusunun yapılandırılmasıyla ilgili bir örnek sunmaktadır. Bu bölümün amacı, bu süreçle ilgili bilgi sunmaktır. Prosedürler, kullandığınız RADIUS sunucusunun türüne ve sunucuyu nasıl yapılandırıdığınıza göre değişiklik gösterir. Bu örnekte Microsoft Windows 2003 sunucusuyla birlikte verilen Internet Kimlik Doğrulama Hizmeti kullanılmıştır.



Not: Bu belge, RADIUS sunucusunda Yönetici kullanıcıların nasıl oluşturulduğuna dair bilgi içermez. Bu örnekte, RADIUS sunucusu kullanıcı hesaplarınızın halihazırda yapılandırılmış olduğunu varsayıyoruz. Bu prosedür ve kablosuz istemciniz için nasıl sertifika edineceğinizi ve yükleyeceğinizi anlatan aşağıdaki prosedür için bir RADIUS sunucusu kullanıcı adı ve şifresine ihtiyacınız olacaktır. Kullanıcı hesapları oluşturma hakkında bilgi için RADIUS sunucusunun belgelerine göz atın.

Bu prosedürün amacı RADIUS sunucusunun 9160 G2 Kablosuz Ağ Geçidi cihazınızı "istemci" olarak tanımasını sağlamaktır. RADIUS sunucusu, bu prosedürden sonra AP'nin kablosuz istemcileri için kimlik doğrulama ve yetkilendirme işlemlerini halledebilir. Bu prosedür *her bir erişim noktası için* gereklidir. Harici bir RADIUS sunucusu kullanmayı planladığınız birden fazla erişim noktası varsa bu erişim noktalarının her biri için aşağıdaki adımları gerçekleştirmeniz gerekir.

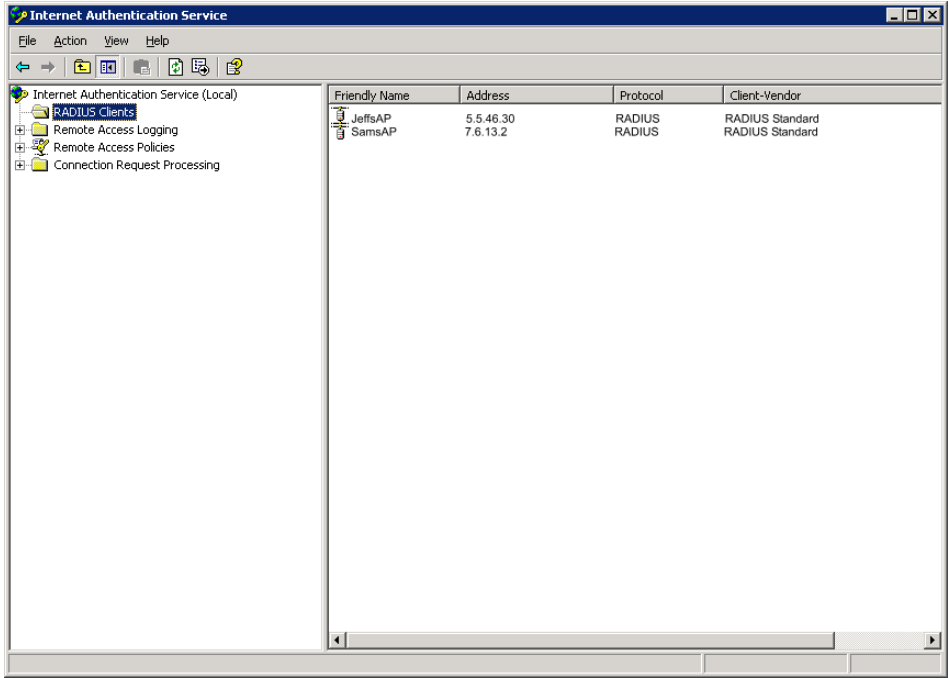
RADIUS sunucusuna erişim noktasıyla ilgili sağlamanız gereken bilgilerin erişim noktasındaki ayarlara (*Güvenlik*) karşılık geldiğini (ve tersinin de doğru olduğunu) unutmayın. RADIUS sunucusu IP Adresini AP'ye çoktan sağlamış olmalısınız. Sonraki adımlarda erişim noktası IP adresini RADIUS sunucusuna sağlayacaksınız. AP'de sağlanan RADIUS Anahtarı, RADIUS sunucusuna sağlayacağınız "ortak gizli bilgidir".

Basic Settings	<h3>Modify Internal Network security settings</h3> <p><input checked="" type="checkbox"/> Broadcast SSID <input type="checkbox"/> Station Isolation</p> <p>Mode: IEEE802.1x</p> <p><input type="checkbox"/> Use internal radius server</p> <p>Radius IP: 10.128.14.14</p> <p>Radius Key:</p> <p><input checked="" type="checkbox"/> Enable radius accounting</p> <p>Update</p>
User Management	
Cluster	
Access Points	
Sessions	
Channel Management	
Wireless Neighborhood	
Security	
Status	
Interfaces	

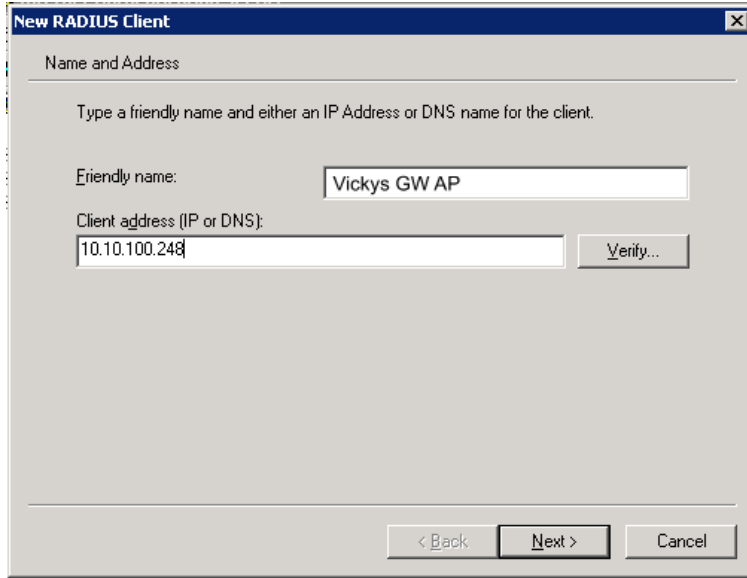


Not: RADIUS sunucusu, IP adresi ve sunduğu farklı hizmetler için kullanılan UDP bağlantı noktası numaralarıyla tanımlanır. 9160 G2 Kablosuz Ağ Geçidi'nin yeni sürümünde, erişim noktası tarafından kullanılan RADIUS sunucusu Kullanıcı Veri Bloğu Protokolü (UDP) bağlantı noktaları yapılandırılmaz. (9160 G2 Kablosuz Ağ Geçidi, kimlik doğrulama için RADIUS sunucusu UDP bağlantı noktası 1812'yi, hesaplama için 1813'ü kullanmak için doğrudan kodlanmıştır.)

1. RADIUS sunucunuzu barındıran sistemde oturum açın ve Internet Kimlik Doğrulama Hizmetini açın.



2. Soldaki panelde **RADIUS Clients** (RADIUS İstemcileri) düğümüne tıklayın ve açılır menüden **New > Radius Client'ı** (Yeni > Radius İstemcisi) seçin.
3. *New RADIUS Client* (Yeni RADIUS İstemcisi) sihirbazının ilk ekranında istemcilerinizin bağlanmasını istediğiniz 9160 G2 Kablosuz Ağ Geçidi cihazı hakkında şu bilgileri sağlayın:
 - Erişim noktası için mantıklı (uygun) bir ad. (DNS adını ya da konumunu kullanmak isteyebilirsiniz.)
 - Erişim noktasının IP adresi. **Next** (İleri) düğmesine tıklayın.



New RADIUS Client

Name and Address

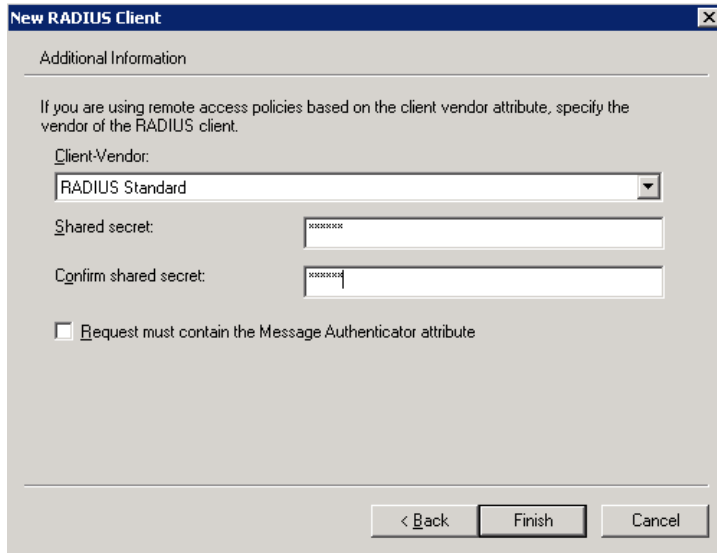
Type a friendly name and either an IP Address or DNS name for the client.

Friendly name:

Client address (IP or DNS):

< Back Next > Cancel

4. *Shared secret* (Paylaşılan gizli bilgi) için erişim noktasına (*Güvenlik* sayfasında) sunduğunuz **RADIUS Anahtarını** girin. Onaylamak için anahtarı tekrar yazın.



New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

Client-Vendor:

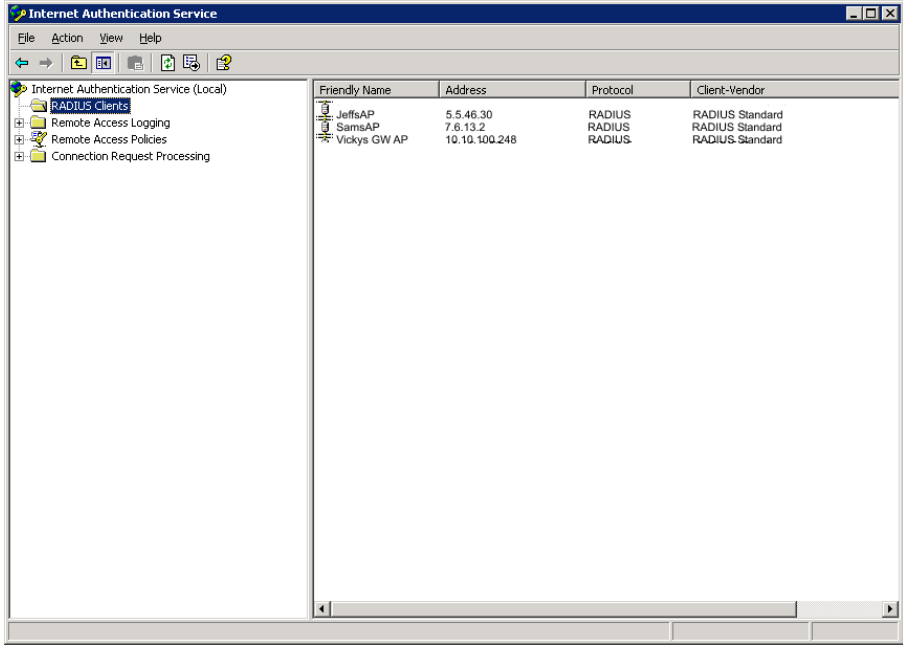
Shared secret:

Confirm shared secret:

☐ Request must contain the Message Authenticator attribute

< Back Finish Cancel

5. **Finish** (Bitir) düğmesine tıklayın. Erişim noktası, Kimlik Doğrulama Sunucusunun istemcisi olarak görüntülenir.



B.10 İstemci için TLS-EAP Sertifikası Edinme



Not: İstemcilerin kimlik doğrulaması ve yetkilendirilmesi için IEEE 802.1x modunu EAP-TLS sertifikalarıyla kullanmak istiyorsanız ağınızda yapılandırılmış harici bir RADIUS sunucunuz ve Sertifika Yetkilisi (CA) dahil Açık Anahtar Altyapısı (PKI) sunucunuz olmalıdır. RADIUS sunucusu, PKI ve CA sunucularının yapılandırılmasıyla ilgili açıklamalar bu belgenin kapsamına dahil değildir. Bu ürünlerin yapılandırılmasıyla ilgili bilgi için ürün belgelerine bakın.

Microsoft Windows PKI yazılımıyla ilgili Internette yer alan bazı faydalı başlangıç noktaları şunlardır:

"How to Install/Uninstall a Public Key Certificate Authority for Windows 2000" (Windows 2000 için Açık Anahtar Sertifika Yetkilisini Kurma/Kaldırma):

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> ve

"How to Configure a Certificate Server" (Sertifika Sunucusu Kurma):

<http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

"WPA/WPA2 Kurumsal (RADIUS)" veya "IEEE 802.1x" güvenlik modlarından birini TLS-EAP sertifikalarını destekleyen harici bir RADIUS sunucusuyla kullanmak üzere yapılandırılan kablosuz istemcilerin RADIUS sunucusundan TLS sertifikası edinmeleri gerekir.

Bu adım, yukarıda bahsedilen iki moddan birini sertifikayla kullanan her istemcinin tamamlaması gereken tek seferlik bir başlangıç adımıdır. Bu prosedürde, örnek olarak Microsoft Sertifika Sunucusu kullanılmıştır.

İstemci için sertifika edinirken şu adımları izleyin:

1. Bir web tarayıcısında şu URL'ye gidin:

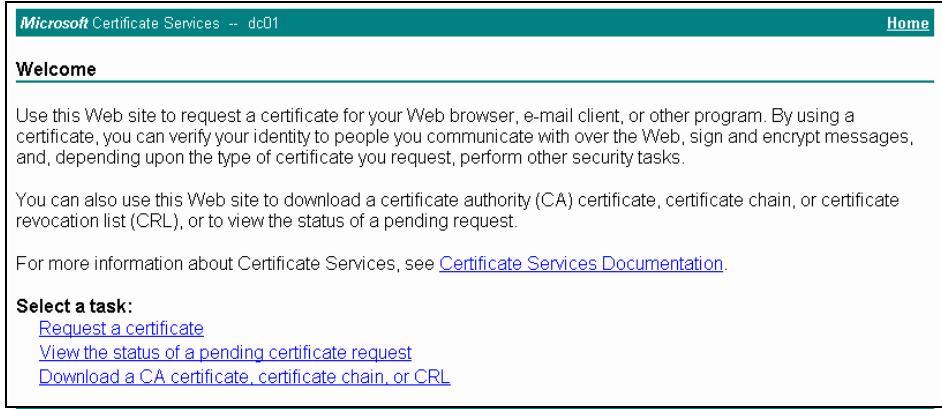
<https://SunucununIPAdresi/certsrv/>

SunucununIPAdresi, altyapınızın yapılandırmasına bağlı olarak harici RADIUS sunucunuzun ya da *Sertifika Yetkilisinin* (CA) IP adresidir.

2. Sunucunun güvenli web sayfasına gitmek için **Yes** (Evet) düğmesine tıklayın.



Tarayıcıda Sertifika Sunucusunun Karşılama ekranı görüntülenir.



Microsoft Certificate Services -- dc01 Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

3. RADIUS sunucusu oturum açma istemi almak için **Request a certificate** (Sertifika iste) seçeneğine tıklayın.
4. RADIUS sunucusuna erişmek için geçerli bir **user name** (kullanıcı adı) ve **password** (şifre) girin.



Connect to 10.10.1.9

Connecting to 10.10.1.9

User name: larry

Password:

☐ Remember my password

OK Cancel



Not: Buraya girmeniz gereken kullanıcı adı ve şifre, halihazırda kullanıcı hesapları yapılandırdığınız RADIUS sunucusuna erişmek içindir. Bu belge, RADIUS sunucusunda Yönetici kullanıcı hesaplarının nasıl oluşturulduğuna dair bilgi içermez. Bu prosedürler için RADIUS sunucunuzun belgelerine göz atın.

5. Görüntülenen sonraki sayfada **User Certificate** (Kullanıcı Sertifikası) seçeneğine tıklayın.

Microsoft Certificate Services -- dc01

Home

Request a Certificate

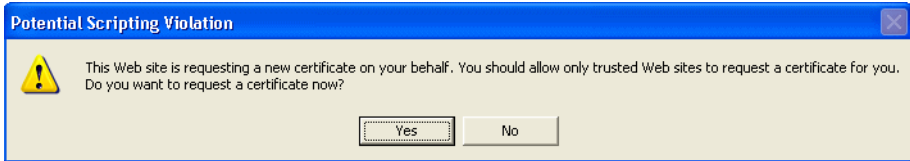
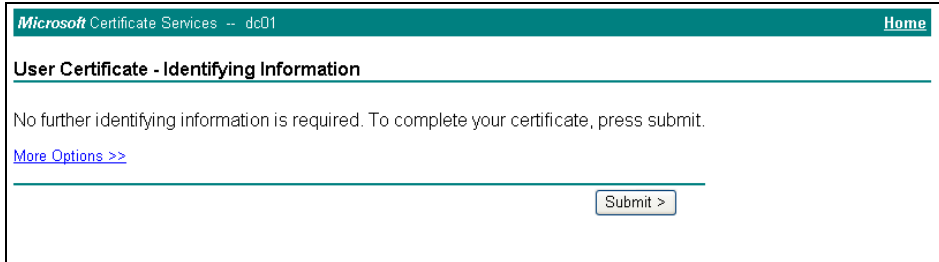
Select the certificate type:
[User Certificate](#)

Or, submit an [advanced certificate request](#).

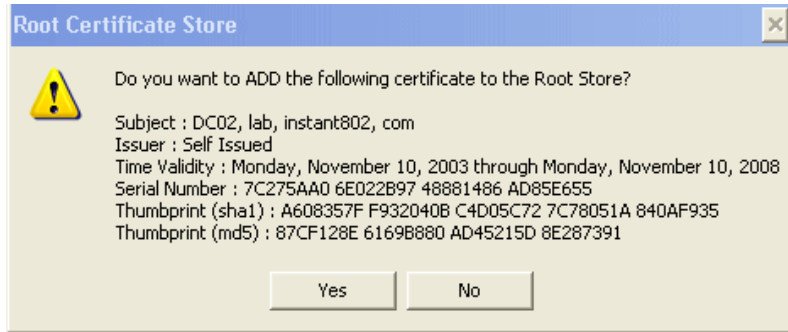
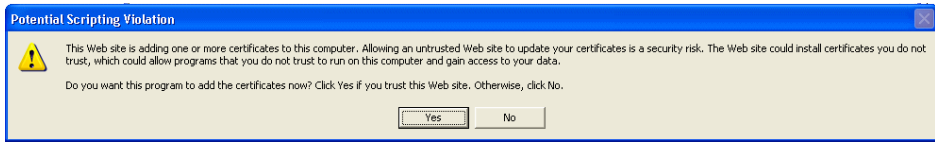
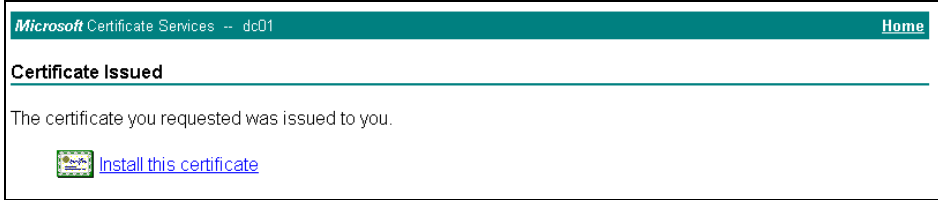
6. Sertifikayı yüklemek için, görüntülenen iletişim kutusunda **Yes** (Evet) düğmesine tıklayın.



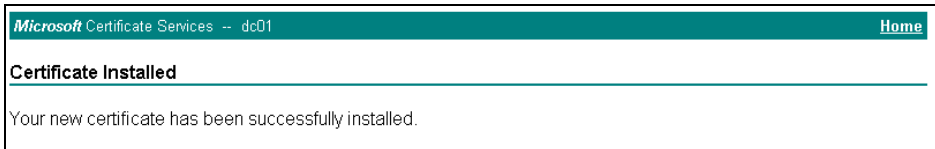
7. İşlemi tamamlamak için **Submit** (Gönder) düğmesine ve açılan iletişim kutusunda gönderme işlemi onaylamak için **Yes** (Evet) düğmesine tıklayın.



8. Size verilen sertifikayı istemci istasyonunuza yüklemek için **Install this certificate** (Bu sertifikayı yükle) seçeneğine tıklayın. (Ayrıca, yüklemeyi onaylamak ve sertifikayı Kök Depoya eklemek için **Yes** (Evet) düğmesine tıklayın.)



Sertifikanın istemciye başarıyla yüklendiğini bildiren bir mesaj görüntülenir.



B.11 VLAN etiketleri için RADIUS Sunucusu Yapılandırma

VLAN, bir anahtardaki bağlantı noktaları grubu ya da farklı anahtarlardaki bağlantı noktaları grubudur. Dinamik VLAN'lar, VLAN'a kullanıcı atamanıza izin verir. Anahtarlar da bu bilgiyi kullanarak anahtarın üzerindeki bağlantı noktasını otomatik olarak yapılandırır.

VLAN seçimi, genellikle kullanıcının kimliğine bağlıdır. RADIUS sunucusu, kimlik doğrulamanın bir parçası olarak seçili VLAN'ın NAS'ini (örneğin, erişim noktası) bilgilendirir. Böylece Dinamik VLAN kullanıcıları, müdahale gerekmeden ve anahtarlarda herhangi bir değişiklik yapmaya gerek kalmadan bir konumdan diğerine geçebilir.

9160 G2 Kablosuz Ağ Geçidi cihazında, kullanıcı harici bir RADIUS sunucusu (*Güvenlik* sayfasında yapılandırılan) kullanmayı seçtiyse harici RADIUS sunucusu, kullanıcının kimliğini doğrulamayı dener. Kullanıcının kimlik doğrulama bilgileri RADIUS sunucusuna iletilir. Bu kimlik bilgileri geçerli bulunursa NAS, bağlantı noktasını RADIUS kimlik doğrulama sunucusu tarafından belirlenen VLAN'a yapılandırır.

B.11.1 RADIUS Sunucusu Yapılandırma

Bir RADIUS Sunucusunun, seçili VLAN hakkında erişim noktasını bilgilendirmek için Erişim-Kabul mesajlarında Tünel özelliklerini kullanacak şekilde yapılandırılması gerekir. Bu özellikler RFC 2868'de tanımlanmış ve dinamik VLAN kullanımları RFC 3580'de belirtilmiştir.

FreeRADIUS sunucusunun kullanıldığı durumlarda gerekli özellikleri eklemek için kullanıcı dosyalarında şu seçenekler ayarlanabilir:

```
example-user  Auth-Type :=EAP, User-Password == "password"  
Tunnel-Type = 13,  
Tunnel-Medium-Type = 6,  
Tunnel-Private-Group-ID = 7
```

Tunnel-Type ve Tunnel-Medium-Type, tüm istasyonlar için aynı değerleri kullanır. Tunnel-Private-Group-ID, seçilen VLAN Kimliğidir ancak her kullanıcı için farklı olabilir.

SORUN GİDERME

C.1 Kablosuz Dağıtım Sistemi (WDS) Sorunları ve Çözümleri	47
C.2 Küme Kurtarma	48
C.2.1 Erişim Noktasını Yeniden Başlatma ya da Sıfırlama	48

Bu bölümde birden çok, kümelenmiş erişim noktaları tarafından sunulan ağlarda ağ yapılandırmalarını güncellerken karşılaşılabileceğiniz genel sorunların nasıl çözüleceğine dair bilgiler yer almaktadır.

C.1 Kablosuz Dağıtım Sistemi (WDS) Sorunları ve Çözümleri

Bir WDS bağlantısını yapılandırmada sorun yaşıyorsanız “WDS Ayarlarını Yapılandırma”, sayfa 207’de yer alan notları ve uyarıları okuduğunuzdan emin olun. Size kolaylık sağlamak için bu notlar aşağıda tekrar belirtilmiştir. Yöneticilerin WDS kurulumlarıyla ilgili karşılaştığı en yaygın sorun, bağlantıdaki iki erişim noktasının da aynı telsiz kanalına ve IEEE 802.11 moduna ayarlanmasının unutulmasıdır. Bu önkoşul, diğerleriyle birlikte aşağıdaki notlarda listelenmiştir.



Notlar:

*WDS’yi kullanırken WDS bağlantısına katılan **her iki** erişim noktasında da WDS ayarlarını yapılandırdığınızdan emin olun.*

Bir erişim noktası çiftinin arasında yalnızca bir WDS bağlantınız olabilir. Bunun anlamı, uzak bir MAC adresi belirli bir erişim noktası için yalnızca bir kez WDS sayfasında görünebilir.

WDS bağlantısına katılan erişim noktalarının ikisi de aynı Telsiz kanalında olmalı ve aynı IEEE 802.11 modunu kullanmalıdır. (Telsiz modunu ve kanalı yapılandırma hakkında bilgi için bkz. “Telsiz Ayarlarını Yapılandırma”, sayfa 169). IEEE 802.11h hakkında daha fazla bilgi için bkz. “802.11h Düzenleyici Etki Alanı Kontrolü”, sayfa 148.

Yayılan Ağaç Protokolünün (STP) WDS köprüleri ya da Kablolı (Ethernet) bağlantıları ile WDS köprülerinin kombinasyonunu kullanarak sonsuz döngüleri ve yol artıklığını önlemek için etkinleştirildiğinden emin olun. STP etkinse yedek bağlantılar oluşturmak için WDS’yi kullanabilirsiniz. STP devre dışıysa şu kural-lara dikkat edin:

- *Herhangi iki erişim noktası yalnızca tek bir yol kullanılarak bağlanabilir: Ya bir WDS köprüsü (kablosuz) ya da bir Ethernet bağlantısı (kablolu) kullanılır ancak ikisi birden kullanılamaz.*
- *"Yedek" bağlantılar oluşturmayın.*
- *Ethernet ya da WDS bağlantıları kombinasyonundan geçen herhangi bir AP çifti arasında birden fazla yol izlerseniz döngü oluşturmuş olursunuz.*

- *Yalnızca Dahili ya da Konuk ağını genişletebilir ya da birleştirebilirsiniz ancak bu işlemleri ikisine birden uygulayamazsınız.*

C.2 Küme Kurtarma

Bir kümedeki erişim noktalarının senkronizasyonu durduğunda ya da bir erişim noktasının bir kümeye katılamaması veya kümeden çıkarılamaması durumlarında küme kurtarma işlemi için aşağıdaki yöntemler önerilir.

C.2.1 Erişim Noktasını Yeniden Başlatma ya da Sıfırlama

Bu kurtarma yöntemleri uygulamanız gereken sırayla verilmiştir. Sonuncusu (kümelemeyi sonlandırma) hariç tüm durumlarda yapmanız gereken tek şey, yapılandırması diğer küme üyeleriyle senkronize olmayan ya da kümeye eklenemeyen/kümeden çıkarılamayan belirli erişim noktalarını sıfırlamak veya yeniden başlatmaktır.

- Güç döngüsünü gerçekleştirerek (Güç düğmesini kapatıp açarak) erişim noktasını fiziksel olarak yeniden başlatın.
- Erişim noktasını Yönetim Kullanıcı Arabiriminden sıfırlayın. Bu işlemi yapmak için:
<http://ErişimNoktasınınIPAdresi>'ne, ardından **Reset Configuration**'a (Yapılandırmayı Sıfırla) gidin ve **Reset** (Sıfırla) düğmesine tıklayın. (AP'lerin IP adresleri, her küme üyesinin Cluster > Access Points [Küme > Erişim Noktaları] sayfasında yer alır.)

SÖZLÜK

0-9 A B C Ç D E G H I K L M N O P Q R S T U V W X Y Z

0-9

802

IEEE 802 (IEEE Std. 802-2001), *LAN* üzerinden uçtan uca iletişim için kullanılan bir standart ailesidir. Bu teknolojiler ortak bir ortam kullanır ve tüm istasyonlar için bilgi yayını sağlar. Sunulan temel iletişim özellikleri paket tabanlıdır. Temel aktarım birimi, *LAN* türüne bağlı olarak belirlenen menzilde herhangi bir uzunlukta olabilen sekizli (8 bit) veri sekansıdır.

Köprüleme, yönetim ve güvenlik protokollerinin tanımları, 802 *IEEE* standartları ailesine dahildir.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001), *LAN Üzerinden EAP Kuşatma (EAPOL)* adlı bir protokol kullanılarak *EAP* paketlerini bir *802.11* kablosuz ağı üzerinden göndermek için kullanılan bir standarttır. Birden fazla kimlik doğrulama yöntemi destekleyen bir çerçeve oluşturur.

IEEE 802.1x, makinelerin değil kullanıcıların kimliklerini doğrular.

802.2

IEEE 802.2 (*IEEE Std. 802.2.1998*), *802* standart ailesi için *LLC* katmanını tanımlar.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002), *CSMA/CA* kullanan ağlar için *MAC* katmanını tanımlar. *Ethernet*, bu ağlara bir örnektir.

802.11

IEEE 802.11 (IEEE Std.802.11-1999), yerel bir alandaki sabit, taşınabilir ve hareketli istasyonlara yönelik kablosuz bağlantı için ortam erişim kontrolü (**MAC**) ve fiziksel katman (**PHY**) spesifikasyonudur. 2.4 GHz ISM bantta doğrudan sıralı geniş spektrumu (DSSS) kullanır ve 1 ve 2 Mb/sn ham veri hızlarını destekler. Resmi olarak 1997'de benimsenmiştir ancak **802.11b**, büyük oranda yerini almıştır.

IEEE 802.11, aynı zamanda kablosuz yerel alan ağları için **IEEE** standartları ailesinden bahsederken de kullanılır.

802.11a

IEEE 802.11a (IEEE Std. 802.11a-1999), ortogonal frekans bölmeli çoğullama (OFDM) kullanılarak 5 GHz U-NII bantında çalışmayı belirten bir **PHY** standardıdır. 6 - 54 Mb/sn aralığındaki veri hızlarını destekler.

802.11a Turbo

IEEE 802.11a Turbo, 802.11a standardının *Atheros Communications*'a ait özel bir türüdür. 6 - 108 Mb/sn aralığındaki hızlandırılmış veri hızlarını destekler. Atheros Turbo 5 GHz, IEEE 802.11a Turbo modundadır. Atheros Turbo 2.4 GHz, IEEE 802.11g Turbo modundadır.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999), ilk **802.11 PHY** standardının 5,5 Mb/sn ve 11 Mb/sn veri hızlarını destekleyen iyileştirilmiş versiyonudur. Daha yüksek veri hızları sunmak için 2,4 GHz ISM bandında doğrudan sıralı geniş spektrum (DSSS) ya da frekans atlama yayılma spektrumu (FHSS) ve tamamlayıcı kod anahtarı (CCK) kullanır. 1 - 11 Mb/sn aralığındaki veri hızlarını destekler.

802.11d

IEEE 802.11d, IEEE 802.11 kablosuz LAN'ların yeniden yapılandırılmadan herhangi bir ülkede çalıştırılması için standart kurallar tanımlar. Frekans atlama tabloları, kabul edilebilir kanallar ve her ülke için güç seviyeleri gibi PHY gereksinimleri sağlar. Erişim noktasında IEEE 802.11d desteğinin etkinleştirilmesi, AP'nin uyarılarının bir parçası olarak hangi ülkede çalıştırıldığını yayınlamasına yol açar. Ardından istemci istasyonları bu bilgiyi kullanır. Bu frekansların kullanımı ülkeden ülkeye büyük oranda değiştiğinden bu durum özellikle 5 GHz IEEE 802.11a bantlarında çalışan AP'ler için oldukça önemlidir.

802.11e

IEEE 802.11e, *QoS*'i desteklemek için *MAC* iyileştirmelerine yönelik gelişmekte olan bir *IEEE* standardıdır. **802.11** üzerindeki trafiğe öncelik vermek için bir mekanizma sunar. Çerçeveler Arası Karar Verme Aralığındaki izin verilen değişiklikleri, minimum ve maksimum Çatışma Penceresi boyutunu ve veri yığınlarının maksimum uzunluğunu (kμ/sn cinsinden) tanımlar.

IEEE 802.11e , halen taslak halinde olan bir *IEEE* standardıdır (en yeni sürüm: D5.0, Temmuz 2003). *Kablosuz Multimedya Geliştirmeleri (WMM)* standardı, 802.11e'nin şu anda kullanılabilen bir alt kümesidir.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003), genişletilmiş bir hizmet kümesindeki (*ESS*) erişim noktaları (kablosuz hub'lar) için erişim noktaları arası protokolü (*IAPP*) tanımlayan bir standarttır. Bu standart, erişim noktalarının mobil istasyonlarının ilişkilendirmeleri ve yeniden ilişkilendirmeleriyle nasıl iletişim kuracağını tanımlar.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003), 2,4 GHz bandında çalışan **802.11b PHY** standardının daha hızlı (54 Mb/sn'ye kadar) bir uzantısıdır. Ortogonal frekans bölmeli çoğullamayı (OFDM) kullanır. 1 - 54 Mb/sn aralığındaki veri hızlarını destekler.

802.11h

IEEE 802.11h, 802.11a standardında görülen parazit sorununu çözmek için kullanılan bir standarttır. 802.11h standardında paraziti en aza indirmek için kullanılan iki yöntem, İletim Gücü Kontrolü (TPC) ve Dinamik Frekans Seçimidir (DFS). DFS, aynı frekanstaki diğer AP'leri algılar ve başka bir kanala yönlendirir. TCP, AP'nin ağ frekansı çıkış gücünü azaltarak parazit olasılığını azaltır. Bu, Avrupa, Japonya ve ABD'de gerekli bir standarttır.

802.11i

IEEE 802.11i, kablosuz bir yerel alan ağı (*WLAN*) güvenliği için sunulan ve *Wi-Fi Korumalı Erişim 2*'yi (*WPA2*) açıklayan kapsamlı bir *IEEE* standardıdır. Bazı *WEP* zayıflıklarının önüne geçmek için *MAC* Katmanına geliştirmeler sunar. Orijinal *Wi-Fi Korumalı Erişimden (WPA)* daha güçlü şifreleme tekniklerine (Gelişmiş Şifreleme Standardı (*AES*) gibi) sahiptir. 802.11i standardının bir alt grubu olarak nitelendirilebilen orijinal *WPA*, şifreleme için *Geçici Anahtar Bütünlüğü Protokolünü (TKIP)* kullanır. *WPA2*, orijinal *WPA*'yı destekleyen ürünlerle geriye dönük uyumluluk sağlar.

IEEE 802.11i / WPA2, Haziran 2004'te son haline getirilmiş ve onaylanmıştır.

802.11j

IEEE 802.11j, 4,9 ve 5 GHz telsiz bantlarını kullanabilen yonga setlerini, iki bandı da iç mekan, dış mekan ve mobil kablosuz LAN uygulamalarına açmak için Japonya hükümeti tarafından belirlenen kurallara uygun şekilde standartlaştırır. Düzenlemeler, bu kanalların genişliğinin şirketler tarafından ayarlanmasını gerektirir. *IEEE 802.11j*, kablosuz cihazların yeni frekanslardan ve çalışma modlarından faydalanarak daha önce kullanılamayan kanallara ulaşmasına olanak sağlar. Bu özellik, bir bakıma hava dalgalarındaki yoğunlaşmayı azaltmayı amaçlar ve *IEEE 802.11h* ile çeşitli ilişkileri vardır.

802.11k

IEEE 802.11k, ağ *Kanal* seçimi, istemci *Dolaşım* ve *Erişim Noktası (AP)* kullanımının otomatik olarak yönetilmesine yardımcı olan kablosuz ağlara (*WLAN*) yönelik gelişmekte olan bir *IEEE* standardıdır. 802.11k özellikli ağlar, ağ performansını geliştirmek ve herhangi bir AP'nin az ya da fazla kullanılmasını önlemek için AP'lerin ağ trafiği yükünü otomatik olarak dengeler. 802.11k, kablosuz bir bağlantı aracılığıyla multimedya için QoS sunarak *802.11e* hizmet kalitesi (*QoS*) standardını tamamlayacaktır.

802.1p

802.1p, *IEEE 802* standardının bir uzantısıdır ve QoS sağlamadan sorumludur. 802.1p'nin temel amacı veri bağlantısı/MAC katmanındaki ağ trafiğine öncelik vermektir. 802.1p, çoklu gönderim trafiğini filtreleme özelliği sunarak 2. katmanla anahtarlanmış ağları geçmemesini sağlar. Öncelik verme şeması için etiketleme çerçevelerini kullanır.

2. katman anahtarlarının bu standartla uyumlu olması için gelen LAN paketlerini ayrı trafik sınıfları olarak gruplayabilmesi gerekir.

802.1Q

IEEE 802.1Q, kablosuz teknolojilere özel *Sanal Yerel Alan Ağları (VLAN)* için *IEEE* standardıdır. (Bkz. <http://www.ieee802.org/1/pages/802.1Q.html>.) Standart, yayın ve çoklu yayın veri trafiğinin gerektiğinden fazla bant genişliği kullanmasını önlemek için büyük ağları küçük parçalara bölme sorununa yönelir. 802.11Q, ayrıca dahili ağ bölümleri arasında daha fazla güvenlik sağlar. 802.1Q spesifikasyonu VLAN üyeliğini Ethernet çerçevelerine sokma konusunda standart bir yöntem sunar.

A

Açık Anahtar

Açık anahtar, şifresinin yalnızca alıcının özel ya da gizli anahtarıyla çözülebileceği bir mesaj şifrelemek için açık anahtarlı şifrelemede kullanılır. Açık anahtarlı şifreleme, iki anahtar kullandığı için asimetrik şifreleme ya da Diffie-Hellman şifreleme olarak da adlandırılır. Ayrıca bkz. *Paylaşılan Anahtar*.

Ad hoc Modu

Ad hoc modu, istasyonların birbiriyle doğrudan iletişim kurduğu bir **Kablosuz Ağ Çerçevesi** modudur. Biçimsel bir altyapının gerekli olmadığı durumlarda hızlıca ağ kurmak için oldukça faydalıdır.

Ad hoc modu, ayrıca *uçtan uca modu* ya da bağımsız temel hizmet kümesi (**IBSS**) olarak da bilinir.

AES

Gelişmiş Şifreleme Standardı (AES), DES şifrelemenin yerine geliştirilen simetrik 128 bit blok veri şifreleme tekniğidir. AES, aynı anda birden çok ağ katmanında çalışır.

NIST Web sitesinde daha fazla bilgi bulabilirsiniz.

Ağ Adresi

Bkz. *IP Address (IP Adresi)*.

Ağ Geçidi

Ağ Geçidi, başka bir ağa giriş görevi gören bir ağ düğümüdür. Genellikle proxy sunucusu ve güvenlik duvarı da sağlar. Ağ Geçitleri, hem paketlerin nereye gönderileceğini belirleyen başlıklar ve gönderme tabloları kullanan bir yönlendiriciyle hem de paketin ağ geçidine girip çıkması için gerçek yolu sağlayan anahtar veya köprüyle ilişkilidir.

LAN üzerideki bir ana bilgisayarın Internet'e erişmeden önce *varsayılan ağ geçidinin* adresini bilmesi gerekir.

Alt Ağ Maskesi

Alt Ağ Maskesi, bir IP adresinin hangi bölümünün ağ adresi, hangi bölümünün ağdaki ana bilgisayar adresi olduğunu tanımlayan bir sayıdır. Bu sayı, noktalı ondalık gösterim (örneğin, 24 bit maske 255.255.255.0 şeklinde gösterilir) ya da IP adresine eklenen bir sayı (örneğin, 192.168.2.0/24) şeklinde gösterilir.

Alt ağ maskesi, yönlendiricinin maskede ve IP adresinde bitlerle ilgili bir AND işlemi gerçekleştirerek bir IP adresinin yerel olup olmadığını ve iletilmesinin gerekip gerekmediğini hızla belirlemesine olanak sağlar. Örneğin, bir IP adresi 192.168.2.128 ve ağ maskesi 255.255.255.0 ise elde edilen Ağ adresi 192.168.2.0'dır.

Bitlerle ilgili AND işlemi, iki biti karşılaştırır ve yalnızca iki bit de 1 ise sonucu 1 değerini atar. Aşağıdaki tablo ağ maskesi ayrıntılarını göstermektedir:

IP adresi	192.168.2.128	11000000 10101000 00000010 10000000
Ağ maskesi	255.255.255.0	11111111 11111111 11111111 00000000
Elde edilen ağ adresi	192.168.2.0	11000000 10101000 00000010 00000000

Altyapı Modu

Altyapı Modu, kablosuz istasyonlarının önce bir *Erişim Noktası* içinden geçerek birbirleriyle iletişim kurdukları bir *Kablosuz Ağ Çerçevesi*'dir. Bu modda, kablosuz istasyonları birbirleriyle ya da kablolu bir ağda ana bilgisayarlarıyla iletişim kurabilir. Erişim noktası kablolu bir ağa bağlıdır ve bir dizi kablosuz istasyonunu destekler.

Bir altyapı modu çerçevesi tek bir erişim noktası (*BSS*) ya da çok sayıda erişim noktası (*ESS*) tarafından sağlanabilir.

Atheros XR (Uzun Menzil)

Atheros Extended Range (XR), daha uzun mesafede düşük hızlı trafik uygulamanın özel bir yöntemidir. XR etkin istemcilerde ve erişim noktalarında görünmez olacak ve 802.11g ile 802.11a modlarında 802.11 standardıyla birlikte çalışabilecek şekilde tasarlanmıştır. 802.11b, Atheros Turbo 5 GHz veya Atheros Dynamic Turbo 5 GHz'de Atheros XR desteği bulunmaz.

B

Bağlantı Noktası İletme

Bağlantı Noktası İletme, Internet erişimi olan kullanıcıların *LAN* ağındaki bilgisayarlardan birinde çalışan bir hizmete (örneğin bir web sunucusuna, FTP'ye, SSH sunucusuna ya da diğer hizmetlere) erişmesini sağlayan ve güvenlik duvarından geçen bir "tünel" oluşturur. Dışarıdaki kullanıcıların açısından bakıldığında hizmet, güvenlik duvarında çalışıyor gibi görünür.

BSS

Temel hizmet kümesi (BSS) tek bir erişim noktasına sahip bir *Altyapı Modu Kablosuz Ağ Çerçevesi*'dir. Genişletilmiş hizmet kümesine (*ESS*) ve bağımsız temel hizmet kümesine de (*IBSS*) göz atın.

BSSID

Altyapı Modu kullanılırken *Temel Hizmet Kümesi Tanımlayıcısı* (BSSID), *Erişim Noktası* kablosuz arabiriminin 48 bit *MAC* adresidir.

C

CCMP

Sayaç Modu/CBC-MAC Protokolü (CCMP) *AES* kullanan *802.11h* için bir şifreleme yöntemidir. Şifreleme ve mesaj bütünlüğü için Şifre Bloğu Zincirleme Sayaç modu (CBC-CTR) ve Şifre Bloğu Zincirleme Mesajı Kimlik Doğrulama Kodunu (CBC-MAC) birleştiren *CCM* çalıştırma modunu kullanır.

AES-CCMP'yi çalıştırmak için yardımcı bir donanım işlemcisi gerekir.

CSMA/CA

Çarpışmadan Kaçınmalı Taşıyıcı Algılamalı Çoklu Erişim (CSMA/CA), düşük seviyeli ağ karar verme/çatışma protokolüdür. İstasyon, ortamı dinler ve kanal sessizken paket aktarmayı dener. İstasyon, kanalın boş olduğunu algıladığında paketi aktarır. Kanalın meşgul olduğunu algıladığında rastgele bir süre bekledikten sonra ortama tekrar erişmeyi dener.

CSMA/CA, IEEE 802.11e Dağıtılmış Kontrol İşlevinin (**DCF**) temelidir. Ayrıca bkz. **RTS** ve **CTS**.

802.11 ağları tarafından kullanılan CSMA/CA protokolü, CSMA/CD'nin (**Ethernet** ağları tarafından kullanılır) bir varyasyonudur. CSMA/CD'de çarpışmanın *algılanması* vurgulanırken CSMA/CA'da çarpışmadan *kaçınılması* vurgulanır.

CTS

Göndermeye müsait (CTS) mesajı, *gönderme istem kodu* mesajına (**RTS**) yanıt olarak bir **IEEE 802.11** istemci istasyonu tarafından gönderilen sinyaldir. CTS mesajı, RTS mesajını gönderenin veri aktarımına başlayabilmesi için kanalın müsait olduğunu belirtir. Hava dalgalarının net olması için diğer istasyonlar bekler. Bu mesaj, IEEE 802.11 **CSMA/CA** protokolünün bir parçasıdır. (Ayrıca bkz**RTS**.)

CGI

Ortak Ağ Geçidi Arabirimi (CGI), bir **HTTP** sunucusundan harici programlar çalıştırmak için kullanılan bir standarttır. Bağımsız değişkenlerin, **HTTP** isteğinin bir parçası olarak çalışan programa nasıl iletileceğini belirler. Ayrıca bir dizi çevresel değişken de tanımlayabilir.

CGI programı, **HTTP** sunucusunun kullanıcılarla dinamik biçimde etkileşimde bulunmak için kullandığı genel bir yöntemdir. Örneğin, form içeren bir HTML, form verisini gönderildikten sonra işlemek için bir CGI programı kullanabilir.

Ç

Çerçeve

Çerçeve, kablosuz bir ağda iletilmek üzere paketlenmiş bazı açıklayıcı meta bilgilerin yanında ayrı bir veri grubundan oluşur. Her çerçevede kaynak ve hedef **MAC** adresi, protokol versiyonlu bir kontrol alanı, çerçeve türü, çerçeve sekans numarası, çerçeve gövdesi (iletilecek gerçek bilgiyle birlikte) ve hata algılama için çerçeve kontrolü sekansı vardır. Çerçeve, kavram olarak **Paket** ile benzerlik gösterir. Paketler Ağ katmanında (OSI modelinde 3. katman) çalışırken çerçeveler Veri-Bağlantı katmanında (**OSI** modelinde 2. katman) çalışır.

Çoklu gönderim

Çoklu gönderim, aynı mesajı belirli bir grup alıcıya göndermektir. Bir e-postayı e-posta listesindeki alıcılara göndermek, çoklu gönderime bir örnektir. Kablosuz ağlarda, çoklu gönderim genellikle erişim noktasının ağdaki belirli istemci istasyonu gruplarına (**MAC** adresleri) **IEEE 802.11 Çerçeve** biçiminde veri trafiği gönderdiği etkileşime denir.

Bazı kablosuz güvenlik modları, tek yönlü, çok yönlü ve yayın çerçevelerinin nasıl şifrelendiğini ya da şifrenip şifrelenmediğini ayırt eder. Ayrıca bkz. **Tek yönlü yayın** ve **Yayın**.

D

DCF

Dağıtılmış Kontrol İşlevi, IEEE 802.11e Hizmet Kalitesi (QoS) teknoloji standardının bir bileşenidir. DCF, kanal erişimi bekleme sürelerini kontrol ederek kablosuz bir ağda yer alan birden fazla istasyonun kanal erişimini koordine eder. Bekleme süreleri, minimum ve maksimum çatışma pencereleri tanımlayarak yapılandırılabilen rastgele bir geri çekilme zamanlayıcısı tarafından belirlenir. Ayrıca bkz. **EDCF**.

Desteklenen Hız Grubu

Desteklenen hız grubu, bu kablosuz ağda kullanılabilen aktarım hızlarını tanımlar. Bir istasyon, bu grupta listelenen hızlardan birinde veri alabilir. Tüm istasyonlar, **Temel Hız Kümesi** listesindeki hızlarda veri alabilmelidir.

DHCP

Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), merkezi bir sunucunun ağ yapılandırma bilgilerini istemcilere dinamik biçimde nasıl sağlayacağını belirleyen bir protokoldür. DHCP sunucusu, istemci sistemine bir "kontrat" (önceden belirlenmiş bir süreliğine [*Kiralama Süresi*]) "sunar". Sağlanan bilgiler arasında istemcinin IP adresleri, ağ maskeleri ve ayrıca *DNS* sunucularının adresleri ve *Ağ Geçidi* yer alır.

Dinamik IP Adresi

Bkz. *IP Address (IP Adresi)*.

DNS

Alan Adı Hizmeti (DNS), *tam nitelikli adların* Internet adreslerine dönüştürülmesi için kullanılan genel amaçlı bir sorgu hizmetidir. Tam nitelikli bir ad, sistemin sunucu adıyla alan adından oluşur. Örneğin, www, web sunucusunun sunucu adı, *www.psionteklogix.com* ise bu sunucunun tam nitelikli adıdır. DNS, *www.psionteklogix.com* alan adını 66.93.138.219 gibi IP adreslerine dönüştürür.

Bir *alan adı* bir ya da daha fazla IP adresi tanımlar. Diğer taraftan, bir IP adresi birden fazla alan adına eşlenebilir.

Alan adları, hangi *üst seviye alana* (TLD) ait olduklarını gösteren son eklere sahiptir. Her ülkenin kendine ait üst seviye alanı vardır. Örnek: Almanya için .de, Fransa için .fr, Japonya için .jp, Tayvan için .tw, Birleşik Krallık için .uk, ABD için .us gibi. Ayrıca, ticari kurumlar için .com, eğitim kurumları için .edu, ağ operatörleri için .net, diğer kuruluşlar için .org, ABD hükümeti için .gov ve askeri hizmetler için .mil kullanılır.

Dolaşım

IEEE 802.11 bağlamında, *gezici istemciler*, çeşitli baz istasyonu hizmet alanlarına girip çıkarken birden fazla *Erişim Noktasının* (AP) kullanılmasını gerektiren, kablosuz bir ağdaki (*WLAN*) mobil istemci istasyonları ya da cihazlardır. *IEEE 802.11f*, AP'lerin gezici istemcileri desteklemek amacıyla, ilişkilenen ve ilişkisi kesilen istemcilerle ilgili bilgileri iletebileceği bir standart tanımlar.

DOM

Belge Nesne Modeli (DOM), programların ve komut dizilerinin belgelere dinamik olarak erişmesini ve belgelerin içeriğini, yapısını ve stilini güncellemesini sağlayan bir arabirimdir. DOM; HTML ya da XML belgesindeki nesneleri (metin, bağlantılar, imajlar, tablolar) modelleyerek her nesnenin özelliklerini ve nasıl kullanılacağını tanımlamanıza olanak sağlar.

DOM ile ilgili ayrıntılı bilgi için bkz. [W3C](#).

DTIM

Teslim Trafiği Bilgi Haritası (DTIM) mesajı, bazı *Uyarı* aralıklarında yer alan bir unsurdur. Düşük güç modunda uyuyan istasyonlardan hangilerinin *Erişim Noktası* arabelleğinde alınmayı bekleyen verileri olduğunu gösterir. DTIM mesajının bir bölümü istasyonların arabellekteki verileri ne sıklıkta kontrol etmesi gerektiğini gösterir.

E

EAP

Genişletilebilir Kimlik Doğrulama Protokolü (EAP); paket anahtarlamalı devrede özel işaret kartı, Kerberos, tek kullanımlık şifreler, sertifikalar, açık anahtar kimliği doğrulama ve akıllı kartlar gibi çeşitli yöntemleri destekleyen bir kimlik doğrulama protokolüdür.

EAP'nin varyasyonları şunları içerir: EAP Cisco Kablosuz (LEAP), Korumalı EAP (PEAP), EAP-TLS ve EAP Tüneli TLS (EAP-TTLS).

EDCF

Gelişmiş Dağıtılmış Kontrol İşlevi, **DCF**'nin uzantısıdır. IEEE Kablosuz Multimedya (WMM) standardının bir bileşeni olan EDCF, kablosuz ortamına öncelikli erişim sağlar.

Erişim Noktası

Erişim noktası, kablosuz ve kablolu ağ cihazları arasında bağlantı ya da köprü sağlayan, **WLAN** üzerindeki cihazlara yönelik bir iletişim hub'ıdır. **Altyapı Modu** adlı bir **Kablosuz Ağ Çerçevesi** destekler.

Bir erişim noktası, kablolu bir ağa bağlıysa ve bir kablosuz istasyon kümesini destekliyorsa bu erişim noktasına temel hizmet kümesi (**BSS**) denir. Genişletilmiş hizmet kümesi (**ESS**), iki ya da daha fazla BSS birleştirilerek oluşturulur.

ERP

Genişletilmiş Hız Protokolü, Ortogonal Frekans Bölmeli Çoğullama (OFDM) ile eşleştiğinde **IEEE 802.11g** istasyonları tarafından (2,4 GHz'de 20 Mb/sn'den fazla aktarım hızı) kullanılan protokoldür. IEEE 802.11g istasyonlarının aynı kanaldaki IEEE 802.11b düğümleriyle etkili biçimde birlikte çalışabilmesi için ERP ve IEEE **802.11g** standardında bir şema yer alır.

Eski IEEE 802.11b cihazları, IEEE 802.11g istasyonları tarafından kullanılan ERP-OFDM sinyallerini algılayamaz; bu durum IEEE 802.11b ve IEEE 802.11g istasyonlarından gelen veri çerçeveleri arasında çarpışmaya sebep olur.

Aynı kanalda hem 802.11b hem de 802.11g düğümleri varsa IEEE 802.11g istasyonları erişim noktasındaki ERP işareti aracılığıyla bunu algılar ve veri göndermeden önce *gönderme isteği (RTS)* ve *göndermeye müsait (CTS)* korumasını etkinleştirir. Ayrıca bkz. **CSMA/CA** protokolü.

ESS

Genişletilmiş hizmet kümesi (ESS), temel hizmet kümesinden (**BSS**) daha fazla istemci destekleyebilen tek bir alt ağ oluşturan ve birden fazla erişim noktasına sahip bir **Altyapı Modu Kablosuz Ağ Çerçevesi**'dir. Her erişim noktası, ofis gibi büyük alanlar için daha geniş kablosuz kapsama alanı sunarak çok sayıda kablosuz istasyonu destekler.

Ethernet

Ethernet, 10 Mb/sn - 1 Gb/sn arası veri transferi hızlarını destekleyen bir yerel alan ağı (**LAN**) mimarisidir. Ethernet spesifikasyonu, fiziksel ve daha az yazılım katmanı belirleyen **IEEE 802.3** standardının temelidir. Eş zamanlı talepler için **CSMA/CA** erişim yöntemini kullanır.

Ethernet 10 Mb/sn veri hızını, *Hızlı Ethernet* 100 Mb/sn veri hızını ve *Gigabit Ethernet* 1 Gb/sn veri hızını destekler. Ethernet kabloları "XbaseY" şeklinde sınıflandırılır. X, Mb/sn cinsinden veri hızını, Y ise kablo kategorisini işaret eder. Orijinal kablo *10base5*'tir (Thicknet ya da "Sarı Kablo"). Diğer kablolar şunlardır: *10base2* (Cheapernet), *10baseT* (Çift Bükümlü) ve *100baseT* (Hızlı Ethernet). Son iki kablo genellikle *RJ-45* konektörlerle *CAT5* kablo kullanılarak sağlanır. Ayrıca *1000baseT* (Gigabit Ethernet) kablo da vardır.

G

Gecikme

Bekleme süresi olarak da bilinen *gecikme*, **Paket** gönderenden alıcıya aktarılırken geçen süredir. Gecikme, erişim noktasından istemciye ya da istemciden erişim noktasına veri aktarılırken oluşabilir. Ayrıca, erişim noktasından Internet'e ya da Internetten erişim noktasına veri aktarırken de oluşur. Gecikme, paketin şifrelenmesi ve şifresinin çözülmesi için gereken süre gibi *sabit ağ* faktörleri ile meşgul ya da aşırı yüklü ağlar gibi *değişken ağ* faktörlerinden kaynaklanır. **QoS** özellikleri, yüksek öncelikli ağ trafiği için gecikmeyi en aza indirmek üzere tasarlanmıştır.

H

HTML

Köprü Metni Biçimlendirme Dili (HTML), Dünya Çapında Ağda (World Wide Web) yer alan bir belgenin yapısını tanımlar. Belgenin düzeniyle ilgili ipucu verecek etiketler ve özellikler kullanır. Bir HTML belgesi <html> etiketiyle başlar ve </html> etiketiyle biter. Ayrıca, düzgün biçimlendirilmiş bir belgede, belgeyi tanımlayan meta verileri içeren <head> ... </head> bölümü ve belge içeriğinin bulunduğu <body> ... </body> bölümü yer alır. İşaretleme sistemi, *Standart Genelleştirilmiş İşaret Dilinden (SGML)* türetilmiştir.

HTML belgeleri **HTTP** aracılığıyla sunucudan tarayıcıya gönderilir. Ayrıca bkz. **XML**.

HTTP

Köprü Metni Aktarım Protokolü (HTTP), mesajların Dünya Çapında Ağda (World Wide Web) nasıl biçimlendirildiğini ve aktarıldığını tanımlar. HTTP mesajı bir **URL** ve komuttan (GET, HEAD, POST gibi ardından bir yanıtın geldiği istek) oluşur.

HTTPS

Güvenli Köprü Metni Aktarım Protokolü (HTTPS), Dünya Çapında Ağın iletişim protokolü olan HTTP'nin güvenli versiyonudur. HTTPS, tarayıcıya entegre edilir. HTTPS kullanıyorsanız tarayıcı sayfanızın alt köşesinde kapalı bir kilit simgesi görünür. HTTPS ile gönderilen tüm veriler şifrelendiğinden yapılan işlemler güvenlidir.

I

IAPP

Erişim Noktaları Arası Protokol (IAPP), bir "dağıtım sisteminde" erişim noktaları arasındaki iletişimi tanımlayan bir **IEEE** standardıdır (**802.11f**). Mobil istasyonlarla ilgili bilgi alışverişi, köprü gönderme tablolarının bakımı ve erişim noktaları arasındaki iletişimin korunması da dahildir.

IBSS

Bağımsız temel hizmet kümesi (IBSS), istasyonların doğrudan birbirleriyle iletişim kurdukları bir **Ad hoc Modu Kablosuz Ağ Çerçevesi**'dir.

IEEE

Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), çok çeşitli teknolojiler için 802 ağ ve kablosuz standartlar ailesi gibi endüstri standartları geliştiren ve oluşturan uluslararası bir standartlar kuruluşudur. (Bkz. **802**, **802.11**, **802.11**, **802.11a**, **802.11b**, **802.11e**, **802.11f**, **802.11g** ve **802.11h**.)

IEEE işlem grupları ve standartları hakkında daha fazla bilgi için bkz. <http://standards.ieee.org/>.

IP

İnternet Protokolü (IP), veri birimi olarak da bilinen paket biçimlerini ve adresleme düzenini belirler. IP; bağlantısız, en iyi çaba paket anahtarlama protokolüdür. Paket yönlendirme, bölme ve tekrar bir araya getirme işlevlerini sunar. Hedef ve kaynak arasındaki sanal bağlantıyı kurmak için **TCP** ya da **UDP** gibi yüksek seviyeli protokollerle birleştirilir.

Şu anki IP sürümü *IPv4*'tür. IPv6 ya da IPng olarak adlandırılan yeni sürüm yapım aşamasındadır. IPv6, IP adreslerinin eksikliklerini gidermeyi amaçlar.

IP Address (IP Adresi)

Sistemler, her ana bilgisayarı İnternette benzersiz şekilde tanımlayan dört baytlık (sekizli) bir sayı olan *IP adresleriyle* tanımlanır.

IP adresleri genellikle şu şekildedir: 192.168.2.254. Buna, noktalı ondalık gösterim denir. IP adresleri iki parçadan oluşur: ağ ön eki ve o ağdaki ana bilgisayar numarası. Parçaları tanımlamak için **Alt Ağ Maskesi** kullanılır. İki özel ana bilgisayar numarası vardır:

- **Ağ Adresi**, tamamen sıfırlardan meydana gelen bir ana bilgisayar numarasından oluşur (örneğin, 192.168.2.0).
- **Yayın Adresi**, tamamen birlerden meydana gelen bir ana bilgisayar numarasından oluşur (örneğin, 192.168.2.255).

Sınırsız sayıda IP numarası olabilir. Bu yüzden, yerel bir alan ağı, özel ağlar için **IANA** tarafından belirlenen adres aralıklarından birini kullanır. Bu adres aralıkları şunlardır:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Dinamik IP Adresi, **DHCP** sunucusu ya da benzer bir mekanizma tarafından bir ana bilgisayara otomatik olarak atanan IP adresidir. Her bağlantı kurduğunuzda size farklı bir IP adresi atanabileceği için bu IP adresine dinamik IP adresi denir.

Statik IP Adresi, belirli bir ana bilgisayarın sabit IP adresidir. Web sunucusu gibi bir sunucu çalıştıran her ana bilgisayar için genellikle bir statik adres gerekir.

IPSec

IP Güvenliği (IPSec), **IP** katmanında güvenli paket alışverişini desteklemek için kullanılan bir dizi protokoldür. Paylaşılan açık anahtarları kullanır. İki şifreleme modu vardır: Taşıma ve Tünel.

- **Taşıma** modu, yalnızca her paketin veri bölümünü (faydalı yükü) taşır; başlıklara dokunmaz.
- Daha güvenli olan **Tünel** modu, hem başlığı hem de faydalı yükü şifreler.

ISP

Internet Servis Sağlayıcısı (ISP), bireylere ve şirketlere Internet erişimi sağlayan şirkettir. Sanal barındırma, ağ danışmanlığı, web tasarımı gibi ilgili hizmetler de sunabilir.

K

Kablosuz Ağ Çerçevesi

Kablosuz ağları düzenlemenin iki yolu vardır:

- İstasyonlar, bağımsız temel hizmet kümesi (**IBSS**) olarak da bilinen bir **Ad hoc Modu** ağında birbirleriyle doğrudan iletişim kurar. İstasyonlar, **Altyapı Modu** ağında **Erişim Noktası** aracılığıyla iletişim kurar.
- Tek bir erişim noktası, bir altyapı temel hizmet kümesi (**BSS**) oluştururken birden fazla erişim noktası genişletilmiş bir hizmet kümesi (**ESS**) oluşturur.

Kanal

Kanal, telsizin alma/verme için kullandığı telsiz spektrumu kısmını tanımlar. Her bir **802.11** standardı, spektrumun *Federal İletişim Komisyonu (FCC)*, *Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI)*, *Kore İletişim Komisyonu* ya da *Telecom Mühendislik Merkezi (TELECOM)* gibi ulusal ya da uluslararası otoriteler tarafından nasıl lisanslandığına bağlı olarak pek çok kanal sunar.

Kiralama Süresi

Kiralama Süresi, **DHCP** Sunucusunun istemcilerine **IP Address (IP Adresi)** ve diğer gerekli bilgileri verdiği süreyi belirtir. Kiralama süresi bittiğinde istemcinin yeni bir kiralama süresi istemesi gerekir. Kiralama süresi kısa bir süreye ayarlandıysa ağ bilgilerinizi güncelleyebilir ve istemcilere sunulan bilgileri vaktinde yayabilirsiniz.

Köprü

Ethernet ya da **IEEE 802.11** gibi aynı protokolü kullanan iki yerel alan ağı (**LAN**) arasındaki bağlantı.

L

LAN

Yerel Alan Ağı (LAN), evinizde aynı ağa bağlamak istediğiniz bilgisayarlar ya da aynı binadaki birkaç kat gibi sınırlı bir alanı kapsayan bir iletişim ağıdır. LAN, birden fazla bilgisayar ile depolama cihazları ve yazıcılar gibi diğer ağ cihazlarını birbirine bağlar.

Ethernet, LAN'ı uygulayan en yaygın teknolojidir. Kablosuz Ethernet (**802.11**) de bir diğer LAN teknolojisidir (ayrıca bkz. **WLAN**).

LDAP

Hafif Dizin İletişim Protokolü (LDAP), çevrimiçi dizin hizmetlerine erişim için kullanılan protokoldür. Kimlik doğrulama mekanizması sağlamak için kullanılır. X.500 standardı temeline dayanır ancak onun kadar karmaşık değildir.

LLC

Mantıksal *Bağlantı Denetimi* (LLC) katmanı, çerçeve senkronizasyonunu, akış denetimini ve hata kontrolünü denetler. **MAC** katmanı ile birlikte çalışan LLC, **PHY** katmanından daha yüksek seviyeli bir protokoldür.

M

MAC

Ortam Erişim Denetimi (MAC) katmanı, paylaşılan bir kanalda veri paketlerinin **NIC** arasında gidip gelmesini yönetir. **PHY** katmanından daha yüksek seviyeli bir protokoldür. Sinyallerin çarpışmasını önlemek için bir karar verme mekanizması sunar.

Ağın her bir düğümünü benzersiz biçimde tanımlayan *MAC adresi* olarak bilinen bir donanım adresi kullanır. **IEEE 802** ağ cihazları ortak bir 48 bit MAC adresi formatı kullanır. Bu adres FE:DC:BA:09:87:65 örneğinde olduğu gibi iki nokta işaretiyle ayrılan onaltılık düzendeki on iki (12) haneden oluşur.

MDI ve MDI-X

Ortama Bağlı Arabirim (MDI) ve *MDI çapraz kablo* (MDIX), donanım cihazlarında Ethernet bağlantı noktaları için kullanılan çift bükümlü kablo teknolojileridir. Dahili çift bükümlü kablo ve otomatik algılama, aradaki bağlantının standart bir Ethernet kablosu kullanan cihazlardaki gibi olmasını sağlar. (Örneğin, bir kablosuz erişim noktası MDI/MDIX'i destekliyorsa çapraz kablo kullanmanıza gerek kalmadan Ethernet kablosuyla bu erişim noktasına ve bir bilgisayara sorunsuz bir şekilde bağlanabilirsiniz).

MIB

Yönetim Bilgi Tabanı (MIB), ağ yönetimi için kullanılan nesnelerin sanal veri tabanıdır. MIB'de tanımlanan ağ cihazlarını izlemek için **SNMP** araçları ve diğer SNMP araçları kullanılabilir.

MSCHAP V2

Microsoft Karşılıklı Kimlik Doğrulama İletişim Kuralı Sürüm 2 (MSCHAP V2), Windows tabanlı bir bilgisayar ile **Erişim Noktası** veya diğer ağ erişim cihazları arasındaki **PPP** bağlantılarını için kimlik doğrulaması sağlar.

MTU

Maksimum Aktarım Birimi, bir ağın aktarabileceği en büyük (bayt cinsinden) paket boyutudur. MTU'dan daha büyük mesajlar gönderilmeden önce küçük paketlere bölünür.

N

NAT

Ağ Adresi Değişimi, **LAN** ağında kullanılan dahili IP adreslerini maskeleyen bir Internet standardıdır. Bir ağ geçidinde çalışan NAT sunucusu, giden isteklerdeki tüm dahili IP adreslerini kendi adresine eşleyen ve gelen tüm istekleri doğru dahili ana bilgisayarlara dönüştüren bir tablo içerir.

NAT sunucularının üç temel amacı vardır: dahili IP adreslerini gizleyerek güvenliği gizlilikle sağlamak, diğer kuruluşların kullandığı IP adresleriyle çakışma korkusu olmadan çok çeşitli dahili IP adreslerinin kullanılmasını sağlamak ve tek bir Internet bağlantısının kullanılmasını sağlamak.

NIC

Ağ Arabirim Kartı, fiziksel olarak bir ağa bağlanmak için bilgisayarların için yerleştirilen bir adaptör ya da genişletme kartıdır. NIC'lerin çoğu belirli bir ağ, protokol ve ortam (**Ethernet** ya da kablosuz gibi) için tasarlanmıştır.

NTP

Ağ Zaman Protokolü, bilgisayara ağlarındaki sistem saatlerinin tam senkronizasyonunu sağlar. NTP sunucuları, istemci sistemlerine *Eşgüdümlü Evrensel Zaman* (UTC, *Greenwich Saati* olarak da bilinir) aktarır. NTP istemcisi, saatini ayarlamak için, dönen zaman damgasını kullanarak sunuculara periyodik zaman istekleri gönderir.

0

OSI

Açık Sistem Bağlantısı (OSI) referans modeli, ağ tasarımı için kullanılan bir çerçevedir. OSI modelinin yedi katmanı vardır:

- 1. Katman olan Fiziksel katman, düğümler arası iletişim için kullanılan fiziksel ortamı tanımlar. Kablosuz ağlarda fiziksel ortam havadır ve telsiz frekansı (RF) dalgaları fiziksel katmanın bileşenleridir.
- 2. Katman olan Veri-Bağlantı katmanı, aktarılabacak verilerin iletişim ve adreslemeye yönelik düşük seviyeli protokollerle birlikte nasıl yapılandırılacağını ve biçimlendirileceğini tanımlar. Örneğin, *CSMA/CA* gibi protokoller, *MAC* adresleri gibi bileşenler ve *Çerçeveler*, Veri-Bağlantı katmanının bir parçası olarak tanımlanır ve yönetilir.
- 3. Katman olan Ağ katmanı, ağın bir ucundan diğerine giden bilgiler için en iyi yolun nasıl belirleneceğini tanımlar. *Paket* ve mantıksal *IP Address (IP Adresi)*, ağ katmanında çalışır.
- 4. Katman olan Taşıma katmanı, *TCP* ve *UDP* gibi bağlantı odaklı protokolleri tanımlar.
- 5. Katman olan Oturum katmanı, ağdaki iletişim ve işlemleri başlatmak, sürdürmek ve bitirmek için kullanılan protokolleri tanımlar. Ağ dosya sistemi (NFS) ve yapılandırılmış sorgu dili (SQL), bu katmanda çalışan başlıca protokollere örnektir. Ayrıca, tekli mod (bilgi yığını gönderen cihaz), yarı iki yönlü mod (sırayla bilgi yığınları aktaran cihazlar) ve tam iki yönlü mod (interaktif, aynı anda bilgi alıp veren cihazlar) gibi iletişim akışları bu katmanın bir parçasıdır.
- 6. Katman olan Sunum katmanı, bilgilerin uygulamaya nasıl sunulduğunu tanımlar. Verilerin nasıl şifreleneceği/şifresinin çözüleceği ve sıkıştırılacağı/açılacağı hakkındaki meta verileri içerir. JPEG ve TIFF dosya formatları, bu katmandaki protokollere örnektir.
- 7. Katman olan Uygulama katmanı, köprü metni aktarım protokolü (*HTTP*), basit posta aktarım protokolü (SMTP) ve dosya aktarım protokolü (FTP) gibi protokolleri içerir.

P

Paket

Veriler ve medya öğeleri, bir ağdaki düğümler arasında *paketler* halinde aktarılır. Veriler ve multimedya içerikleri, bölünür ve *pakatlere* ayrılır. Paketler, hedef adres ile gönderen adresi arasında gönderilecek küçük içerik parçaları içerir. Paketler ağa atılır ve her bir düğüm tarafından incelenir. Paketin gönderildiği düğüm, son alıcıdır.

Paket Kaybı

Paket Kaybı, hedef adresine ulaşamayan paketlerin yüzdesini belirtir. Yüzde 0 paket kaybı, aktarım sırasında hiç paket kaybı olmadığını gösterir. **QoS** özellikleri, paket kaybını en aza indirmek için tasarlanmıştır.

Paylaşılan Anahtar

Paylaşılan anahtar, bir anahtarın hem şifreleme hem de şifre çözme için kullanıldığı geleneksel şifreleme yönteminde kullanılır. *Gizli anahtar* ya da *simetrik anahtar* şifreleme de denir. Ayrıca bkz. **Açık Anahtar**.

PHY

Fiziksel Katman (PHY), ağ katman modelindeki en düşük katmandır (bkz. **OSI**). Fiziksel Katman, bit akışını (elektriksel vuru, ışık ya da telsiz sinyali), elektrik ve mekanik seviyede ağa iletir. Kablo, **NIC** ve fiziksel özellikler tanımlama gibi, bir ortamda veri alma ve gönderme için donanımsal yollar sunar.

Ethernet ve **802.11** ailesi, fiziksel katman bileşenleriyle kullanılan protokollerdir.

PID

İşlem Tanımlayıcı (PID), bir işlemi benzersiz biçimde tanımlamak için Linux tarafından kullanılan bir tam sayıdır. PID, fork() sistem çağrısı tarafından döndürülür. Belirli bir süreçte işlem yapmak için wait() ya da kill() tarafından kullanılabilir.

PPP

Noktadan Noktaya Protokolü, ağ katmanı veri birimlerini (**IP** paketleri) noktadan noktaya seri bağlantılar üzerinden aktarmak için kullanılan bir standarttır. PPP, hem asenkron bağlantılar hem de bit odaklı senkronize sistemler üzerinde çalışacak şekilde tasarlanmıştır.

PPPoE

Ethernet Üzerinden Noktadan Noktaya Protokolü (PPPoE), **LAN** ağındaki kullanıcıları tek DSL ya da kablolu modem hattı gibi genel bir geniş bant ortamı aracılığıyla Internet'e bağlamak için kullanılan bir spesifikasyondur.

PPtP

Noktadan Noktaya Tünelleme Protokolü (PPtP), *Noktadan Noktaya Protokolü (PPP)* içinde *Sanal Özel Ağ (VPN)* oluşturmak için kullanılan bir teknolojidir. Bir VPN düğümünden diğerine aktarılan verilerin güvenli olduğundan emin olmak için kullanılır.

Proxy

Proxy, bir istemci uygulaması ile gerçek bir sunucu arasında yer alan sunucudur. Kendisi gerçekleştirmeyi amaçladığı için istekleri durdurur. Durduramazsa gerçek sunucuya iletir. Proxy sunucularının iki temel amacı vardır: istekleri birkaç makineye dağıtıp performansı artırmak ve belirli sunuculara ya da hizmetlere erişimi önlemek için istekleri filtrelemek.

PSK

Önceden Paylaşılan Anahtar (PSK), bkz. *Paylaşılan Anahtar*.

Q

QoS

Hizmet Kalitesi (QoS), bir ağ hizmetinin garantili verim, geçiş bekleme süresi ve öncelik kuyrukları gibi performans özelliklerini tanımlar. QoS; *Gecikme*, *Sapma*, *Paket Kaybı* ve ağ tıkanıklığını en aza indirmek ve yüksek öncelikli ağ trafiğine özel bant genişliği ayırma yolları sağlamak için tasarlanmıştır.

QoS'i kablosuz ağlarda uygulamak için tasarlanan **IEEE** standardı çalışmaları, **802.11e** işlem grubu tarafından halen sürdürülmektedir. **802.11e** özelliklerinin bir alt grubu, **WMM** özelliklerinde açıklanmaktadır.

R

RADIUS

Arayan Kullanıcının Uzaktan Kimliğini Doğrulama Hizmeti (RADIUS), kimlik doğrulama ve hesaplama sistemi sunar. Pek çok **ISP** için popüler bir kimlik doğrulama mekanizmasıdır.

RC4

Simetrik şifre dizisi, RSA Güvenliği tarafından sağlanır. Bayt odaklı işlemlerle birlikte değişken anahtar boyutlu bir şifre dizisidir. 2048 bit uzunluğa kadarki anahtarları kabul eder.

RSSI

Alınan Sinyal Gücü Göstergesi (RSSI), alınan sinyalin gücüne göre voltaj hesaplayan bir 802.11 değeridir. RSSI, *telsiz frekansı* (RF) sinyal gücünü ölçmek ve göstermek için kullanılan çeşitli yollardan biridir. Sinyal gücü, mW (miliwatt), dBms (desibel miliwatt) ve yüzde değeriyle de ölçülebilir.

RTP

Gerçek Zamanlı Aktarım Protokolü (RTP), ses ve video gibi gerçek zamanlı verileri aktarmak için kullanılan bir Internet protokolüdür. Bu protokol, verilerin teslimini garanti etmez ancak alıcı ve verici uygulamaların veri akışını gerçekleştirebilmesi için destek mekanizmaları sağlar. RTP, genellikle **UDP** protokolünün üzerinde çalışır ancak diğer aktarım protokollerini de destekler.

RTS

Gönderme isteği (RTS) mesajı, bir veri paketi göndermek için izin istemek ve diğer kablosuz istemci istasyonlarının telsiz dalgalarını yakalaması önlemek için istemci istasyonu tarafından erişim noktasına gönderilen sinyaldir. Bu mesaj, IEEE 802.11 **CSMA/CA** protokolünün bir parçasıdır. (Ayrıca bkz. **RTS Eşiği** ve **CTS**).

RTS Eşiği

RTS eşiği, aktarımı (**RTS**) göndermek için isteğin paket boyutunu belirler. Bu da, erişim noktalarına doğru olan trafik akışının kontrol edilmesine yardımcı olur ve özellikle çok istemcili erişim noktalarında performans ayarı yaparken faydalıdır.

S

Sapma

Sapma, ağ içinde bir düğümden diğerine yapılan paket aktarımlarındaki bekleme süreleri arasındaki farktır. Paketler, tutarlı bir hızda aktarılmazsa (**Gecikme** dahil) bazı veri türleri için **QoS** olumsuz yönde etkilenebilir. Örneğin, tutarsız aktarım hızları VoIP ve medya akışlarında bozulmalara yol açabilir. **QoS**, sapmayı ve ağ performansını etkileyen diğer faktörleri azaltmak için tasarlanmıştır.

SNMP

Basit Ağ Yönetimi Protokolü (SNMP), bir ağdaki düğümleri yönetmek ve izlemek için geliştirilmiştir. **TCP/IP** protokol setinin bir parçasıdır.

SNMP, yönetilen cihazlar, bu cihazların araçları ve bir yönetim sisteminden oluşur. Araçlar, *Yönetim Bilgi Tabanlarında (MIB)* cihazlarıyla ilgili bilgileri saklar ve istendiğinde bu bilgileri SNMP yönetim sistemine verir.

SNMP Tuzakları

SNMP tuzakları, ağ cihazlarından yönetilen araçlara doğru asenkron iletişimin gerçekleşmesini sağlar. SNMP tuzakları, gereksiz SNMP isteklerini ortadan kaldırır ve ağ kaynaklarında tasarruf sağlar.

SSID

Hizmet Kümesi Tanımlayıcı (SSID), kablosuz bir yerel alan ağını benzersiz biçimde tanımlayan 32 karakterlik alfanümerik bir anahtardır. *Ağ Adı* olarak da bilinir. SSID'de kullanılacak karakterlerle ilgili bir kısıtlama yoktur.

Statik IP Adresi

Bkz. *IP Address (IP Adresi)*.

STP

Yayılan *Ağaç Protokolü* (STP), yol artıklığını yöneten ve istemci istasyonları arasındaki birden fazla etkin yolun oluşturduğu istenmeyen döngüleri önleyen *MAC* köprüleri için kullanılan bir IEEE 802.1 standardı protokolüdür (ağ yönetimiyle ilgili). Erişim noktaları arasında birden fazla yol olduğunda döngüler meydana gelir. STP, tüm anahtarları genişletilmiş bir ağa yayan ve gereksiz yolları bekleme ya da engelli moduna sokan bir ağaç oluşturur. STP iki ağ cihazı arasında tek seferde yalnızca bir etkin yola izin verir (böylece döngüleri önler) ancak ilk kullanılan bağlantının başarısız olması durumunda devreye sokmak için gereksiz bağlantıları yedek olarak tutar. STP maliyeti değişirse ya da STP'deki bir ağ bölümüne ulaşılamazsa yayılan ağaç algoritması, yayılan ağaç yapısını yeniden yapılandırır ve bekleme modundaki yolu etkinleştirerek bağlantıyı yeniden kurar. STP olmadığında iki bağlantı da eş zamanlı olarak kullanılabilir; bu da LAN üzerinde sonsuz bir trafik döngüsüne neden olur.

SVP

SpectraLink Ses Önceliği (SVP) Wi-Fi kullanımına yönelik bir QoS (Hizmet Kalitesi) yaklaşımıdır. SVP, IEEE 802.11b standardıyla uyumlu olan açık bir özelliktir. SVP, Kablosuz LAN'daki bekleme süresini en aza indirir ve veri paketleri yerine ses paketlerine öncelik vererek daha iyi ağ performansı elde edilmesinin olasılığını artırır.

T

TCP

Aktarım Kontrol Protokolü (TCP), Internet Protokolüne (*IP*) dayanır. Güvenilir iletişim (veri teslimini garanti eder), akış kontrolü, çoğullama (aynı anda birden fazla bağlantı) ve bağlantı odaklı aktarım (alıcının paketi aldığına dair göndereni bilgilendirmesini gerektirir) ekler. Ayrıca paketlerin gönderildikleri sırayla teslim edilmesini garanti eder.

TCP/IP

İnternet ve yerel alan ağlar bir dizi protokol tarafından tanımlanır. Bunların en önemlisi, fiili standart protokolü olan *İnternet Protokolü Üzerinden Aktarım Kontrolü Protokolüdür* (TCP/IP). TCP/IP, ilk olarak İleri Savunma Araştırma Projeleri Ajansı (DARPA, ARPA olarak da bilinen ABD Savunma Bakanlığı'nın bir ajansı) tarafından geliştirilmiştir.

TCP ve **IP** iki ayrı protokol olsa da, ICMP, ARP, **UDP** ve diğerlerinin yanı sıra telnet ve FTP gibi TCP ve IP ile çalışan uygulamalar dahil bu iki protokolü temel alan protokol setinin tamamını ifade etmek için TCP/IP kullanılır.

Tek yönlü yayın

Tek yönlü yayın, mesajları yalnızca belirli bir alıcıya gönderir. Kablosuz ağlarda, tek yönlü yayın genellikle erişim noktasının ağdaki tek bir istemci istasyonu **MAC** adresine **IEEE 802.11 Çerçeve** biçiminde veri trafiği gönderdiği etkileşime denir.

Bazı kablosuz güvenlik modları, tek yönlü, çok yönlü ve yayın çerçevelerinin nasıl şifrelendiğini ya da şifrelenip şifrelenmediğini ayırt eder.

Ayrıca bkz. **Çoklu gönderim** ve **Yayın**.

Temel Hız Kümesi

Temel hız kümesi, bu kablosuz ağa katılmak isteyen tüm istasyonlar için zorunlu olan aktarım hızlarını tanımlar. Tüm istasyonlar, bu kümede listelenen hızlarda veri alabilmelidir.

TKIP

Geçici *Anahtar Bütünlüğü Protokolü* (TKIP), genişletilmiş 48 bit başlatma vektörü, paket başı anahtar yapılandırma ve dağıtma, Mesaj Bütünlüğü Kodu (MIC, bazen "Michael" de denir) ve yeniden anahtarlama mekanizması sunar. Aktarımdan önce her **802.11** çerçevesinin gövdesini ve CRC'sini şifrelemek için **RC4** şifre dizisi kullanır. **WPA** ve **802.11h** güvenlik mekanizmalarının önemli bir bileşenidir.

ToS

TCP/IP paket başlıkları, uygulama geliştiricisi tarafından ayarlanan, paketteki veriler için uygun hizmet türünü belirten 3-5 bitlik bir *Hizmet Türü* (ToS) alanıdır. Bitlerin ayarlanma biçimi, veri gerekliliklerine bağlı olarak paketin minimum bekleme süresiyle, maksimum verimle, düşük maliyetle ya da orta seviyeli "en iyi çaba" ayarlarıyla gönderilmek için kuyruğa alındığını belirler. ToS alanı 9160 G2 Kablosuz Ağ Geçidi tarafından, AP'den istemci istasyonuna aktarılan verilerin *Hizmet Kalitesi (QoS)* kuyruklarında yapılandırma denetimi sağlamak için kullanılır.

U

UDP

Kullanıcı Veri Birimi Protokolü (UDP), basit ama güvenilir olmayan veri birimi hizmetleri sunan bir taşıma katmanı protokolüdür. **IP** paketine bağlantı noktası adres bilgileri ve toplam değerini ekler.

UDP, veri teslimini garanti etmez ve herhangi bir bağlantı gerektirmez. Hafif ve etkilidir. Tüm hata işleme ve yeniden aktarma işlemleri uygulama programı tarafından yapılmalıdır.

URL

Tek Düzen Kaynak Bulucu (URL), dosya ya da haber grubu gibi Internette yer alan nesnelerin konumunu belirlemek için kullanılan bir standarttır. URL'ler ağırlıklı olarak HTML dosyalarında, bir köprü bağlantısının hedefini belirlemek için kullanılır. Hedef, genellikle başka bir HTML dosyasıdır (bu dosya olasılıkla başka bir bilgisayarda depolanır). URL'nin ilk bölümü hangi protokolün kullanılacağını, ikinci bölümü ise kaynağın bulunduğu IP adresini ya da etki alanı adını belirtir.

Örneğin, <ftp://ftp.devicescape.com/downloads/myfile.tar.gz> URL'si, FTP protokolü kullanılarak erişilecek bir dosyayı; <http://www.devicescape.com/index.html> URL'si ise **HTTP** protokolü kullanılarak erişilecek bir web sayfasını belirtir.

UTC

Eşgüdümlü Evrensel Zaman (UTC), Greenwich Saati olarak da bilinir.

Uyarı

Uyarı anonsları, ağların varlığını duyurarak ve istasyonların düzenli biçimde iletişim kurmasını ve bu iletişimi sürdürmesini sağlayarak **WLAN**'ların "temelini" oluşturur. Şu bilgileri taşır (bazıları isteğe bağlıdır):

- *Zaman damgası*, istasyonlar tarafından yerel saatlerini güncellemek için kullanılır; tüm ilişkili istasyonlar arasında senkronizasyon sağlar.
- *Uyarı aralığı*, aktarım yapan uyarı anonsları arasındaki süreyi tanımlar. Bir istasyon, güç tasarrufu moduna girmeden önce, uyarı almak üzere ne zaman uyanacağını bilmek için uyarı aralığına ihtiyaç duyar.
- *Özellik Bilgisi*, **WLAN** ağına katılmak isteyen istasyonların gerekliliklerini listeler. Örneğin, tüm istasyonların **WEP** kullanması gerektiğini belirtir.
- *Hizmet Kümesi Tanımlayıcı (SSID)*.
- *Temel Hız Kümesi*, **WLAN** ağının desteklediği hızları listeleyen bir bit eşlemdir. İsteğe bağlı *Parametre Kümeleri*, kullanılan belirli sinyal gönderme yöntemlerinin (frekans atlama yayılma spektrumu, doğrudan sıralı yayılma spektrumu vb.) özelliklerini belirtir.
- İsteğe bağlı *Trafik Gösterge Haritası (TIM)*, güç tasarrufu modunu kullanan ve veri çerçeveleri kuyruğa alınmış olan istasyonları tanımlar.

V

VLAN

Sanal LAN VLAN, bir ağdaki cihazların tek bir fiziksel ağa bağlı olmasalar bile o şekilde davranmalarını sağlayan yazılım tabanlı ve mantıklı bir şekilde bir araya getirildiği cihazlar grubudur. VLAN'daki düğümler, kaynakları ve bant genişliğini paylaşır ve o ağda izole biçimde yer alır. 9160 G2 Kablosuz Ağ Geçidi, kablosuz VLAN yapılandırmasını destekler. "Sanal" konuk ağ özelliği için erişim noktasında bu teknolojiye yararlanılır.

VPN

Sanal Özel Ağ (VPN), düğümlerini bağlamak için Interneti kullanan bir ağıdır. Yalnızca yetkili kullanıcıların düğümlerine erişebilmesini ve verilerin durdurulmamasını sağlamak için şifreleme ve diğer mekanizmaları kullanır.

W

WAN

Geniş Alan Ağı (WAN), bir kilometreden fazla mesafeye kadar genişleyebilen büyük coğrafi alanları kapsayan bir iletişim ağıdır. WAN, genellikle telefon sistemi gibi genel ağlar aracılığıyla bağlanır. Ayrıca, özel hat ve uydular aracılığıyla da bağlanabilir.

Internet, çok geniş bir WAN'dır.

WDS

Kablosuz Dağıtım Sistemi (WDS), tamamen kablosuz bir altyapının oluşturulmasını sağlar. *Erişim Noktası*, genellikle kablolu bir *LAN* ağına bağlıdır. WDS, erişim noktalarının kablosuz olarak bağlanmasına olanak sağlar. Erişim noktaları kablosuz yineleyiciler ya da köprüler olarak işlev görebilir.

WEP

Kablolu Eş Değer Gizlilik (WEP), **802.11** kablosuz ağlar için bir veri şifreleme protokolüdür. Ağdaki tüm kablosuz istasyonlar ve erişim noktaları, veri şifreleme için statik 64 bit (40 bit gizli anahtar + 24 bit başlatma vektörü (IV)) ya da 128 bit (104 bit gizli anahtar + 24 bit IV) *Paylaşılan Anahtar* ile yapılandırılır. Aktarımdan önce her **802.11** çerçevesinin gövdesini ve CRC'sini şifrelemek için **RC4** şifre dizisi kullanır.

Wi-Fi

Kâr amacı gütmeyen ticari bir kuruluş olan *Wi-Fi İttifakı* tarafından tanıtılan, **IEEE 802.11** standardına dayanan *WLAN* ürünlerinin birlikte çalışabilirliğine dair test ve sertifika.

WINS

Windows Internet Adlandırma Servisi (WINS), Windows tabanlı bilgisayar adlarını IP adreslerine dönüştürmek için kullanılan bir sürücü işlemidir. Bu sistemlerin *Ağ Komşularını* kullanarak uzak ağları taramasına izin veren bilgileri sağlar.

WLAN

Kablosuz Yerel Alan Ağı (WLAN), düğümleri arasında iletişim kurmak için kablo kullanmak yerine yüksek frekanslı telsiz dalgaları kullanan bir *LAN* ağıdır.

WMM

Kablosuz Multimedya (WMM), kablosuz bir ağdaki ses, video ve multimedya uygulamalarının kalitesini geliştirmek üzere tasarlanan bir **IEEE** teknolojisi standardıdır. Hem erişim noktaları hem de kablosuz istemciler (dizüstü bilgisayarlar, tüketici elektroniği ürünleri) WMM etkin olabilir. WMM özellikleri, **WLAN IEEE 802.11e** taslak spesifikasyonunun bir alt ağını temel alır. Standartlara uygun biçimde üretilen ve bir dizi kalite testinden geçen kablosuz ürünler, diğer ürünlerle birlikte çalışabilirliklerini gösteren "WMM için Wi-Fi sertifikalıdır" etiketini taşır. Daha fazla bilgi için Wi-Fi İttifakı web sitesinin WMM sayfasına göz atın: <http://www.wi-fi.org/OpenSection/wmm.asp>.

WPA

Wi-Fi Korumalı Erişim (WPA), taslak **IEEE 802.11h** standardının *Wi-Fi* İttifakı versiyonudur. **WEP**'den daha karmaşık bir veri şifreleme hizmeti sunar ve ayrıca kullanıcı kimliği doğrulama hizmeti de sağlar. WPA, **TKIP** ve 802.11 mekanizmalarını içerir.

WPA2

Wi-Fi Korumalı Erişim (WPA2), veri şifreleme için Gelişmiş Şifreleme Standardını (**AES**) kullanan, **IEEE 802.11h** standardında açıklanan gelişmiş bir güvenlik standardıdır.

Orijinal **WPA**, veri şifreleme için Geçici Anahtar Bütünlüğü Protokolünü (**TKIP**) kullanır. WPA2, orijinal **WPA**'yı destekleyen ürünlerle geriye dönük uyumluluk sağlar.

WPA2, orijinal **WPA** gibi *Kurumsal* ve *Kişisel* sürümü destekler. Kurumsal Sürüm, IEEE 802.11 güvenlik özelliklerinin ve **RADIUS** sunucusuyla birlikte *Genişletilebilir Kimlik Doğrulama Protokolü* (**EAP**) kimlik doğrulamasının kullanılmasını gerektirir.

Kişisel sürüm IEEE 802.11 ya da **EAP** gerektirmez. Kimlik doğrulama için gereken anahtarları oluşturmak için *Önceden Paylaşılan Anahtar* (**PSK**) şifresi kullanır.

WRAP

Kablosuz Güvenli Kimlik Doğrulama Protokolü (WRAP), **AES** kullanan ancak şifreleme ve bütünlük için başka bir şifreleme modu (**OCB**) kullanan **802.11h** standardına yönelik bir şifreleme yöntemidir.

X

XML

Genişletilebilir Biçimlendirme Dili (XML), *W3C* tarafından geliştirilen bir spesifikasyondur. XML, özellikle elektronik yayınlar için tasarlanan *Standart Genelleştirilmiş Biçimlendirme Dilinden (SGML)* türetilmiş basit, esnek bir metin biçimidir.

Y

Yayın

Yayın, aynı anda herkese aynı mesajı gönderir. Kablosuz ağlarda, yayın genellikle erişim noktalarının ağdaki tüm istemci istasyonlarına *IEEE 802.11 Çerçeve* biçiminde veri trafiği gönderdiği bir etkileşimi ifade eder.

Bazı kablosuz güvenlik modları, tek yönlü, çok yönlü ve yayın çerçevelerinin nasıl şifrelendiğini ya da şifrenip şifrelenmediğini ayırt eder.

Ayrıca bkz. *Tek yönlü yayın* ve *Çoklu gönderim*.

Yayın Adresi

Bkz. *IP Address (IP Adresi)*.

Yetkisiz Giriş Algılama

Yetkisiz Giriş Algılama Sistemi (IDS), gelen tüm ağ etkinliklerini kontrol eder ve sisteme izinsiz giriş yapmaya çalışan birinin ağ ya da sistem saldırısı olabilecek şüpheli durumları raporlar. Desteklenmeyen ya da güvenli olmadığı bilinen protokollerle yapılan erişim denemelerini raporlar.

Yönlendirici

Yönlendirici, paketleri ağlar arasında aktaran bir ağ cihazıdır. Genellikle iki yerel alan ağı (*LAN*) ya da *LAN* ile Internet gibi geniş alan ağları (*WAN*) olmak üzere en az iki ağa bağlıdır. Yönlendiriciler, iki ya da daha fazla ağın bağlandığı yer olan ağ geçitlerinde bulunur.

Yönlendirici, paketleri iletmek için en iyi yolu belirlemek amacıyla başlık içeriklerini ve tablolarını kullanır. İki ana bilgisayar arasındaki en iyi rotayı yapılandırmak amacıyla diğer yönlendiricilerle iletişim kurmak için Internet Mesaj Erişim Protokolü (ICMP), Yönlendirme Bilgi Protokolü (RIP), Internet Yönlendirici Bulma Protokolü (IRDP) gibi protokoller kullanır. Yönlendirici, ilettiği verilerde çok az filtreleme yapar.

#

- 10BaseT Ethernet 21, B-3
- 100Base-FX fiber optik bağlantı noktası 22
- 100BaseT Ethernet 21, B-3
- 3274/Telnet 258–273
 - Protokolü 271
- 5250 Emülasyon 274–289
- 7 Biti 8 Bite Dönüştür**
 - ANSI Emülasyonu 292
- 802.IQ
 - Otomatik Başlama** 303
 - protokole genel bakış 303
 - Terminal Çevrimdışı Zaman Aşımı** 304
 - Uyarı Süreci** 304
- 802.IQv1
 - açıklama 303
 - İlk RTT** 306
 - Özellikler Menüsü** 307
 - Protokol Türü Kimliği** 306
 - Uyarı Arabirimleri** 307
 - Yalnızca 802.IQ Paketlerini İlet** 306
- 802.IQv2
 - açıklama 303
 - Özellikler Menüsü** 307
 - Uyarı UDP Bağlantı Noktası** 307
- 802.Ip etiketler 192
- 802.11 Ayarları(Kablosuz Ayarları sayfası) 147, 152
- 802.11 Gelişmiş Ayarlar(Telsiz Ayarları sayfası) 167, 173
- 802.11A/G telsiz 324
- 802.11G telsiz 324
- 9010 / TCP/IP, baz istasyonu
 - yapılandırması 248, 256
- 9010 Emülasyonu 249
- 9010 Yapılandırma 249
- 9500 İletişim Sunucusu, hücresel mod 243

A

- açıklanan fabrika varsayılanları 27
- ağ arabirimleri 324
- ağ, özelliklere genel bakış 13
- ağa başlama 50
- AIAG**
 - 3274 Emülasyonu 263
 - 5250 Emülasyonu 280
- aktarım gücü, yapılandırma 169
- Aktarma Satırı**
 - 3274 Emülasyonu 263
 - 5250 Emülasyonu 279
- Alan Ek Yüğü**
 - 3274 Emülasyonu 268
 - 5250 Emülasyonu 284
- Alan Vurgusunu Yeniden Ayarlama**
 - 5250 Emülasyonu 275
- Alarm**
 - 3274 Emülasyonu 259
 - 5250 Emülasyonu 275
- alma/verme bilgisi 127
- Ana Bilgisayar**
 - Bağlantı Noktası**
 - ANSI Telnet Protokolü 293
 - 3274 Telnet Protokolü 269
 - 5250 Telnet Protokolü 285
 - Yazdır**
 - 3274 Emülasyonu 261
 - 5250 Emülasyonu 277
 - Zaman Aşımı**
 - ANSI Emülasyonu 290
- Ana Bilgisayar Başlatma Verisi, ANSI Emülasyonu** 293
- Ana bilgisayar Fujitsu mu**
 - 3274 Emülasyonu 258
- ANA BİLGİSAYAR MENÜSÜ**
 - mini yapılandırması 258
- Ana Bilgisayar Numarası, baz istasyonu
 - yapılandırması 248, 256

Ana Bilgisayarla Etkin Biçimde Görüşme3274 *Telnet Protokolü* 2705250 *Telnet Protokolü* 286**ANA BİLGİSAYARLAR**

mini denetleyici yapılandırma 254

Ana Bilgisayarlar (baz istasyonu yapılandırması) 246–249

anahtar yönetimi, güvenlik 94

ANSI Emülasyonu 289–299

ANSI, bağlanma terminali 23

anten gereksinimleri 19, 20

Arabirim renkleri ve stili 50

Arabirimdeki simgeler 50

arabirimler, ağ 324

Atheros Turbo modları 8, 167

Ayarlanabilir sorgulama/çatışma protokolü 222

B**Bağlanılacak Yerel IP Adresi***ANSI Telnet Protokolü* 2943274 *Telnet Protokolü* 2705250 *Telnet Protokolü* 286

bağlanma

ANSI uyumlu terminaller 23

Ethernet 21

konsol 23

video ekranı terminali 23

bağlantı bütünlüğünü izleme 130

Bağlantı Menüleri 246, 249

bağlantı noktaları

donanım 37

işlev şemaları

konsol bağlantı noktası *B-1*RJ-45 konektör (10BaseT) *B-3*

konum 20

Bağlantı Noktası, RA1001A

parametreleri 231

Bağlantı Seçenekleri

Baz İstasyonu Modu 225

RRM Modu 231

bağlı portal 157

bakım gereksinimleri 18

Barkod3274 *Emülasyonu* 2675250 *Emülasyonu* 284

Basit Ağ Yönetimi Protokolü (SNMP) 213

başlangıç sorunlarını giderme 42

baz istasyonu

Ad 234

Ana Bilgisayar Numarası 248, 256

Ana Bilgisayarlar 246–249

Bağlantı Menüleri 231–249

Baz İstasyonu Numarası 233

Çevrimiçi/Çevrimdışı Yok,

9010/TCP/IP ana bilgisayarı 249

dar bant telsiz menüleri 222–231

genel bakış 221

İlk Terminal 256**İlk Terminal**, 9010 /TCP/IP ana bilgisayarı 248

IP Adresi 234

İşletim Modu 226**Mesaj Boyutu** 234**Monitör Sorgusu**, 9010/TCP/IP ana bilgisayarı 249**Otomatik Başlama** 226, 234**Paylaşılan Kanal** 227**Son Terminal**, 9010 /TCP/IP ana bilgisayarı 248**Son Terminal** ana bilgisayar 256

yapılandırma 219–249

9010 /TCP/IP ana bilgisayarı 248, 256

baz istasyonu yapılandırması 249

bellek 324

Bitiş Süresi, Telsiz Bağlantı Özellikleri 245

bölme eşiği, yapılandırma 169

Boş**Pencere Faktörü**

RRM grubu 238

Pencere Faktörü, dar bant telsiz 229**Boş karaktere izin ver**3274 *Emülasyonu* 2585250 *Emülasyonu* 274**Büyük Harf Kümesi (GL), ANSI***Emülasyonu* 292**C-Ç****Cihaz Adı Ön Eki**5250 *Telnet Protokolü* 288**Cihaz Adlarını Yapılandır**3274 *Telnet Protokolü* 287

Çekirdek Mesajlar İçin Günlük Aktarma

Sunucusu , Olay Günlükleri 125

çevresel gereksinimler 17

bağlı nemde çalıştırma 323

çalışma sıcaklığı 323
 genel bakış 17
 saklama sıcaklığı 323
 çevrimiçi/çevrimdışı mesajlar 249
Çevrimiçi/Çevrimdışı Yok, 9010/TCP/IP
 emülasyonu 249
**Çift Baytlık Karakterlerle Sayfa Kay-
 detme**, *ANSI Emülasyonu* 292
 çok yönlü anten 19
Çağrı
 Dizesi
 RRM grubu 239
 Dizesi, dar bant telsiz 229
 Süreci
 RRM grubu 238
 Süresi, dar bant telsiz 229
 çalışma
 bağıl nem 323
 çalıştırma sıcaklığı 323
Çarpışma
 Boyutu
 dar bant telsiz 228
 RRM grubu 238
D
 Dahili Arabirim Ayarları, Ethernet Ayarları
 141
 dar bant telsiz
 Bağlantı Noktası parametre 231
 Bağlantı Seçenekleri, Baz İstasyonu
 Modu 225
 Bağlantı Seçenekleri, RRM Modu 231
 Etkin Kanal parametresi 230
 Sorgulama Protokolü Parametreleri
 227
 Telsiz Parametreleri 229
 yapılandırma ayarları 222, 231
 2 seviyeli modülasyon 230
 4 seviyeli modülasyon 230
 DCF
 QoS ile ilgili 190
 Rastgele Geri Çekilme Zamanlayıcısı
 191
 DEC VT220, bağlanma 23
 Derinlik, Olay Günlükleri 124
 desteklenen platformlar
 istemci 32
 yönetici 30

DHCP, kendi kendine yönetilen AP
 açısından anlama 32
**Dikkat Tuşu Olarak IAC Break Gön-
 derme**, 3274 *Telnet Protokolü* 272
 DNS Ana Bilgisayar Adı, Ethernet
 Ayarları 138
Doğrudan Geçiş
 3274 *Emülasyonu* 260
 5250 *Emülasyonu* 276
**Doğrudan TCP Kontrolü Yinelenen Ter-
 minal Numarası**, Telsiz Bağlantı
 Özellikleri 244
 donanım bağlantıları 38
 döngüler, WDS 205
 DSCP
 etiketler 192
 Öncelik 193
 DTIM süreci, yapılandırma 169
 durum göstergeleri (LED'ler) 22
 düz metin güvenlik modu
 istemci yapılandırması C-11
 ne zaman kullanılmalı? 94
 yapılandırma 102
 düzenleyici özelliklerine genel bakış 12

E
 EAP-PEAP
 IEEE 802.1x istemcide yapılandırma
 C-15
 WPA/WPA2 Kurumsal (RADIUS)
 istemcide yapılandırma C-22
 elektrik güvenliği onayları xv
 Emisyon Bilgileri, Kanada xv
Emülasyon
 mini denetleyici yapılandırması 257
 emülasyon
 genel bakış 253
 emülasyonlar
 ANSI 289–299
 3274/Telnet 258–273
 5250 274–289
 9010/TCP/IP 249
 erişim noktası
 Ethernet (kablolu) ayarları 135
 güvenlik 91
 izleme 119
 kablosuz ayarları 145
 konuk ağı 153
 kullanıcı yönetimi 65

kümeleme 56
 MAC filtreleme 175
 QoS 185
 telsiz 165
 WDS köprüleme 201
 yük dengeleme 179

Eşik
ANSI Emülasyonu 290

Ethernet
 adaptör kartları 324
 ayarlar 135, 159
 bağlantılar 21, 38
 baz istasyonu 233
 durum göstergesi LED 22
 kablo uzunlukları 22
 10BaseT 21
 işlev şemaları B-3
 100Base-FX fiber optik 22
 100BaseT 21
 işlev şemaları B-3

Ethernet Üzerinden Güç teknik özellikleri 323

Etkin Kanal
 RA1001A parametreleri 230
 RRM Grubu 240

F
 farklı güvenlik modlarında şifreleme 94
 fiber optik Ethernet bağlantı noktası 22
 Firefox 23
 fiziksel
 açıklama 323
 teknik özellikler 323
 Flash ROM 324

G
Genel Parametreler, dar bant telsiz 225
Giriş Satırı
 3274 *Emülasyonu* 267
 5250 *Emülasyonu* 284
 giriş voltajı (güç gereksinimleri) 18, 323
Gizli Eşleşme Karakteri
 3274 *Emülasyonu* 266
 5250 *Emülasyonu* 283
Görünür Eşleşme Karakteri
 3274 *Emülasyonu* 265
 5250 *Emülasyonu* 281
Grup Parametreleri
 , RRM Grubu 240

güç
 bağlantılar 38
 gereksinimler 18, 323

güvenlik
 düz metin (hiçbiri için yapılandırma yok) 102
 erişim noktasında yapılandırma 100
 farklı modların artı ve eksi yönleri 93
 IEEE 802.1x 108
 istemcideki sertifikalar C-37
 kablosuz istemcilerde yapılandırma C-5
 kimlik doğrulama sunucusu C-33
 konuk ağı 102
 modların karşılaştırılması 94
 onaylar xv
 özelliklere genel bakış 11
 statik WEP 103
 talimatları xvii
 WPA/WPA2 Kişisel (PSK) 111
 WPA/WPA2 Kurumsal (RADIUS) 113
 yapılandırma 91–118
 güvenlik modları için kimlik doğrulama 94

H
 harici cihazlar 20
Hata Kodu Yaz, 5250 *Emülasyon* 274
 hizmet kalitesi 185
 Hizmet Türleri *Bkz. ToS* 188
 hücresel
 baz 222, 243
 geçiş 221
Hücresel Modda Çalışma, Telsiz Bağlantı Özellikleri 243

I-İ
 IEEE 802.1x
 güvenlik modu
 ne zaman kullanılmalı? 96
 yapılandırma 108
 security mode
 client configuration C-15
 IEEE 802.11
 hız grubu, yapılandırma 169
 standartları desteği 10
 telsiz modu, yapılandırma 169
 IEEE 802.11a
 yapılandırma 169

IEEE 802.11b
yapılandırma 169
IEEE 802.11g
yapılandırma 169
Internet Explorer 23
IP Adresi (baz istasyonu) 234
IP adresleri
erişim noktalarını görüntülemek için 55, 62, 85
gitme 61
kendi kendine yönetilen AP ilkelerini anlama 32
9160 G2 21
IP üzerinden Ses
QoS ile gelişmiş hizmet 185
ilişkili kablosuz istemciler 129
İlk RTT, 802.IQv1 306
İlk Terminal 248, 256
İlk Terminal Dinleme Bağlantı Noktası
ANSI Telnet Protokolü 294
3274 Telnet Protokolü 270
5250 Telnet Protokolü 286
İlk Yerel Terminal Bağlantı Noktası
ANSI Telnet Protokolü 294
3274 Telnet Protokolü 270
5250 Telnet Protokolü 286
işlemci 324
İşletim Modu, baz istasyonu 226
işlev şemaları Bkz. bağlantı noktaları
işlev şemaları
İşlev Tuşlarını Yeniden Ayarlama, ANSI Emülasyonu 291
İstasyon Ayırma 101
istasyonlar
izin verilen maksimumu yapılandırma 169
Ayrıca bkz. istemci
istemci
bağlantı bütünlüğünü izleme 130
güvenlik C-5
ilişkiler 129
oturum, tanım 63
oturumlar 62
platform 32
Ayrıca bkz. istasyonlar 169

K

kablolar
koaksiyel 20
konsol bağlantı noktası No. 19387 B-2
seri açıklamalar B-1
kablolu ayarları 135, 159
kablosuz
AP özelliklerine genel bakış 7
ayarlar 145
komşuluk 83
Kaçış Zaman Aşımı, ANSI Emülasyonu 290
kanal, telsiz yapılandırma 169
kimlik doğrulama sunucusu
IEEE 802.1x için, güvenlik modu 108
WPA Kurumsal güvenlik modu 113
Kombinasyon, RRM Grubu 240
Komşu 85
komşu erişim noktaları 130
Komut Bölgesi
3274 Emülasyonu 268
5250 Emülasyonu 284
konektörler
RJ-45 B-3
konsol
bağlanma 23
bağlantı noktası
işlev şemaları B-1
kablo No. 19387 B-2
Konuk Ağı güvenliği 102
Konuk Arabirim Ayarları, Ethernet Ayarları 143
konuk arabirimi
açıklama 155
özelliklere genel bakış 12
VLAN'lar 156
yapılandırma 155
Konuk Erişimi, Ethernet Ayarları 138
konum, tanımlama 60
köprüler, WDS 203
Küçük Harf Kümesi (GL), ANSI Emülasyonu 292
küçük takılabilir modül 22
kullanıcı
hesaplar
yedekleme ve geri yükleme 71
yerleşik doğrulama sunucusu için 65

kimlik doğrulama
 IEEE 802.1x istemcide
 yapılandırma C-15
 WPA/WPA2 Kurumsal (RADIUS)
 istemcide yapılandırma C-22
**Kullanıcı Etkinliği Olmadan Otomatik
 Telnet**
ANSI Telnet Protokolü 298
3274 Telnet Protokolü 272
5250 Telnet Protokolü 287
**Kullanıcı Etkinliği Zamanlama Bekleme
 Süresi Olmadan Otomatik Telnet**
ANSI Telnet Protokolü 298
 küme
 anlama 56
 boyut 56
 boyut ve üyelik 58
 desteklenen erişim noktası türleri 56
 erişim noktası ekleme 60
 güvenlik 58
 kanal yönetimi 73
 komşular 83, 85
 kümelemeyi durdurma 61
 oluşum 58
 otomatik senkronizasyon 58
 sorun giderme D-48
 tanım 56
 küme senkronizasyonu 58
 kümelenen AP'lerin kanal yönetimi
 anlama 75
 gelişmiş ayarlar 80
 gitme 75
 kilitleri görüntüleme/ayarlama 78
 önerilen kanal atamaları 79
 örnek 76
 kurulum
 antenler 21
 çevresel gereksinimler 17, 323
 güç kablosu 21
 güvenlik xvii
 LAN 21
 kurulumlar
 LAN 21
 kuyruklar, QoS için yapılandırma 194

L

LAN kurulumları 21
 LED'ler 22
LU Adı Ön Eki
3274 Telnet Protokolü 271
LU Adlarını Yapılandır
3274 Telnet Protokolü 271

M

MAC filtreleme, yapılandırma 178
Maksimum
Ekran Boyutu, ANSI Emülasyonu
 289
Mesaj Bölüm Boyutu
 RRM grubu 238
Mesaj Bölüm Boyutu, dar bant telsiz
 228
**Maksimum Otomatik Telnet Yeniden
 Deneme Sayısı**
ANSI Telnet Protokolü 298
 mapRF
 802.IQv2 303
Mesaj
Boyutu(baz istasyonu) 234
Modu Sınırı
 RRM grubu 238
Modu Sınırı, dar bant telsiz 229
 metin kuralları 7
 MIB'ler *Bkz. Yönetim Bilgi Tabanları*
 213
 Microsoft Internet Explorer 23
 mini denetleyici
 ağlar 253
 emülasyonlar 253
 yapılandırma 251–299
 modülasyon seviyeleri, dar bant telsiz 230
Monitör Sorgusu, 9010/TCP/IP
 emülasyonu 249

N

n İşlev Tuşu
İşlev Tuşu Eşleme Ekranları
 ANSI 299
 3274 273
 5250 289
 NTP sunucusu
 erişim noktasını kullanmak için
 yapılandırma 312

O-Ö

Otomatik Başlama

(baz istasyonu) 234
RRM grubu 237
802.IQ 303

Otomatik Başlama, baz istasyonu modu 226

otomatik küme senkronizasyonu için
bekleme süresi 58
otomatik küme senkronizasyonu için ilerleme çubuğu 58

Otomatik Oturum Açma, ANSI Telnet

Otomatik Telneti/Oturum Açmayı
Etkinleştir 295

Otomatik oturum açma, ANSI Telnet

Kullanıcı Kimliği 297
oturum açma başarısız 297
Şifre 297

Otomatik telnet

3274 Telnet Protokolü 272
5250 Telnet Protokolü 286

Otomatik Telnet Ana Bilgisayarı

3274 Telnet Protokolü 272
5250 Telnet Protokolü 287

Otomatik telnet, ANSI Telnet

Ana Bilgisayar 296
Otomatik Telneti/Oturum Açmayı
Etkinleştir 295
Terminal İstemi 296

Otomatik Telsiz Adresi Atama Aralığı,

Telsiz Bağlantı Özellikleri 244

Otomatik Terminal Sayısı, Telsiz Bağlantı

Özellikleri 245, 246

Oturum Döngüsü Tuşu, ANSI Telnet

Protokolü 294

oturum izleme
bilgileri yenileme 64
gitme 62
hakkında 62
oturum bilgisi görüntüleme 64

Oturumlar 62

Ok Tuşlarını Yeniden Ayarlama, ANSI

Emülasyonu 291

Olaylar 122
olaylar
günlük 122
izleme 122
onaylar xv

Önem Derecesi, Olay Günlükleri 124
özelliklere genel bakış 10

P

paket artırma
QoS ile ilgili 191
parametreler
web tarayıcıyla değiştirme 23

Paylaşılan Kanal

RRM grubu 237

Paylaşılan Kanal, baz istasyonu 227

PEAP

IEEE 802.1x istemcide yapılandırma
C-15

WPA/WPA2 Kurumsal (RADIUS)
istemcide yapılandırma C-22

platform
istemci gereksinimleri 32
yönetici gereksinimleri 30

Prosedürler

3274 Emülasyonu 261
5250 Emülasyonu 277

Protokol

Türü Kimliği, 802.IQv1 306

protokol
ayarlanabilir sorgulama/çatışma 222
telsiz
ayarlanabilir sorgulama/çatışma 222
hücrese geçiş 221
zaman çoklama 221

Q

QoS Bkz. hizmet kalitesi 185
QoS ile ilgili çerçeveler arası boşluklar 190
QoS ile ilgili ToS 188

R

RADIUS server
See also authentication server

RADIUS sunucusu
erişim noktalarını tanımak için
yapılandırma C-33

RA1001A dar bant telsiz
teknik özellikler 324
yapılandırma 222

RA1001A Telsiz Parametreleri 224

RJ-45 konektör işlev şemaları (10BaseT
Ethernet) B-3

RLE, ANSI Emülasyonu 292

rogue erişim noktası 130

RRM Grubu

Boş Pencere Faktörü 238

Çağrı Dizesi 239

Çağrı Süreci 238

Çarpışma Boyutu 238

Etkin Kanal 240

Kombinasyon 240

Maksimum Mesaj Bölüm Boyutu
238

Mesaj Modu Sınırı 238

Otomatik Başlama 237

Paylaşılan Kanal 237

RRM Grup Numarası 236

Senkronizasyon Bekleme Süresi 239

Sorgulama Grubu Parametreleri 237

Sorgulama Penceresi Boyutu 238

Sorgulama Penceresi Sayısı 237

Uzak Telsiz Modülleri 241

Uzak Txon 239

Yeniden Deneme Sayısı 238

RRM Grupları yapılandırma ayarları 234

RRM modu 231

RTS eşiği, yapılandırma 169

S-S

Sanal Cihaz Adlarını Etkinleştir, 5250

Telnet Protokolü 287

Sayfa Kaydetme

ANSI Emülasyonu 291

Sayfalar

3274 Emülasyonu 262

5250 Emülasyonu 279

SDRAM 324

Senkronizasyon Bekleme Süresi

dar bant telsiz 230

RRM grubu 239

seri

durum göstergesi LED 22

Seri G/C

3274 Emülasyonu 267

5250 Emülasyonu 283

veri hızı 23

sertifika

IEEE 802.1x istemci için güvenlik
C-18

istemci için TLS-EAP sertifikası alma
C-37

WPA/WPA2 Kurumsal (RADIUS)

istemci için güvenlik C-26

şifre

Temel Ayarlarda 49

yönetici için ağ ayarı 49

Sistem İsteği Olarak IAC İşlemi Durdur

İsteği Gönderme 271

SNMP Bkz. *Basit Ağ Yönetimi*

Protokolü 213

Son Etkin Oturum Tuşu, *ANSI Telnet*

Protokolü 295

Sorgu Kimliği, Telsiz Bağlantı Özellikleri
243

Sorgu Penceresi Boyutu

dar bant telsiz 228

Sorgu Penceresi Sayısı, dar bant telsiz 227

Sorgulama Penceresi Boyutu

RRM grubu 238

Sorgulama Penceresi Sayısı

RRM grubu 237

Sorgulama Protokolü Parametreleri

RA1001A 227

RRM Grubu 237

Sorgulama Protokolü Terminal Zaman

Aşımı, Telsiz Bağlantı Özellikleri 243

SSID Yayını 101

standartlar 10

statik WEP güvenlik modu

ne zaman kullanılmalı? 95

WDS bağlantıları üzerinde 205

yapılandırma 103

Sürekliliği Etkinleştirme ya da Devre Dışı

Bırakma, Olay Günlükleri 123

T

TCP Oturumlarına İzin Ver, ANSI

Telnet 298

TCP Oturumu İstek Tuşu, *ANSI Telnet*

Protokolü 294

teknik özellikler

fiziksel 323

RA1001A dar bant telsiz 324

802.11A/G telsiz 324

802.11G telsiz 324

TekTerm Doğrudan TCP Bağlantıları,

Telsiz Bağlantı Özellikleri 244

TekTerm, Telsiz Bağlantı Özellikleri 244

telsiz

açma ya da kapatma 169

- aktarım gücü 169
- bir ya da iki telsizli AP yapılandırma 169
- Bitiş Süresi** 245
- bölme eşiği 169
- DTIM süreci 169
- durum göstergesi LED'leri 22
- hız grupları 169
- IEEE 802.11 modu 169
- kümelenen AP'lerin kanal yönetimi 73
- kurulum ve antenler 18
- maksimum istasyon 169
- Otomatik Telsiz Adresi Atama Aralığı** 244
- Otomatik Terminal Sayısı** 245, 246
- protokoller (ayarlanabilir sorgulama, IEEE 802.11) 222
- RA1001A dar bant 324
- RTS eşiği 169
- Sorgu Kimliği** 243
- Sorgulama Protokolü Terminal Zaman Aşımı** 243
- SuperAG 169
- teknik özellikler 324
- Turbo yayın modu, önerilmez 8, 167
- uyarı aralığı 169
- yapılandırma ayarları 169
- yüklü yapılandırma 9
- Yüzde Sorgulama Protokolü Terminal Zaman Aşımı** 244
- 802.11A/G telsiz 324
- 802.11G telsiz 324
- Telsiz Bağlantı Özellikleri**, yapılandırma ayarları 241–246
- Telsiz Kartı Durumu**
- dar bant telsiz yapılandırma menüsü 223
- Telsiz Parametreleri**
- RA1001A 229
- RRM Grubu 239
- temel ayarlar, görüntüleme 41
- Temizle**
- 3274 Emülasyonu 259
- 5250 Emülasyonu 276
- Terminal**
- Çevrimdışı Zaman Aşımı**
- 802.IQ 304
- Tür**
- ANSI Telnet Protokolü 293
- 3274 Telnet Protokolü 269
- 5250 Telnet Protokolü 285
- terminal
- video ekranına bağlanma 23
- terminal aralığı, *Ana Bilgisayarlar* menüsü 256
- terminal aralığı, *Ana Bilgisayarlar* menüsü (9010 emülasyon) 248
- terminal aralığı, *Ana Bilgisayarlar* menü 256
- terminal aralığı, *Ana Bilgisayarlar* menüsü (9010 emülasyon) 248
- Terminal Başına Maksimum Oturum Sayısı**
- ANSI Telnet Protokolü 294
- 3274 Telnet Protokolü 269
- 5250 Telnet Protokolü 285
- Terminal Başlatma Verisi, ANSI Emülasyonu** 293
- Terminal Sıfırlanırken Ana Bilgisayar Oturumlarını Kapat**
- ANSI Telnet Protokolü 294
- TLS-EAP
- IEEE 802.1x istemcide yapılandırma C-18
- istemci için sertifika alma C-37
- WPA/WPA2 Kurumsal (RADIUS) istemcide yapılandırma C-26
- Turbo yayın modu, önerilmez 8, 167
- U-Ü**
- Uyarı**
- Arabirimleri**, 802.IQv1 307
- Süreci**
- 802.IQ 304
- UDP Bağlantı Noktası**, 802.IQv2 307
- uyarı aralığı, yapılandırma 169
- Uzak Telsiz Modülleri**, RRM Grubu 241
- Uzak Txon**
- dar bant telsiz 230
- RRM grubu 239
- Uzaktan Yazdırma**
- 3274 Emülasyonu 262
- 5250 Emülasyonu 279
- Uluslararası EBCDIC'yi Kullan**
- 3274 Emülasyonu 258
- 5250 Emülasyonu 274
- Ürün Yazılımı Yükseltme 9

V

varsayılan ayarlar, 9160 G2 Kablosuz Ağ Geçidi için 27
varsayılan yapılandırma, geri yükleme 249, 257
veri hızı, seri 23
video ekranı terminali, bağlanma 23

VLAN

dahili ve konuk arabirimi için 156
Öncelik 193
voltaj, giriş 18, 323
VWN (Sanal Kablosuz Ağlar), Ethernet Ayarları 140

W**WDS**

açıklama 203
kurallar 208
örnek 209
yapılandırma 207
WDS köprülemeyle ayarlanan genişletilmiş servis 203
web tarayıcı 23
WEP güvenlik modu
istemci yapılandırması C-12
ne zaman kullanılmalı? 95
yapılandırma 103
Wi-Fi uyumluluğu 10
WPA Kişisel güvenlik modu
ne zaman kullanılmalı? 97
yapılandırma 111
WPA Kurumsal güvenlik modu
ne zaman kullanılmalı? 98
yapılandırma 113
WPA/WPA2 Kişisel (PSK) güvenlik modu
istemci yapılandırması C-30
WPA/WPA2 Kurumsal (RADIUS) güvenlik modu istemci yapılandırması C-22

Y

Yalnızca 802.IQ Paketlerini İlet, 802.IQ 306

Yansıtma

ANSI Emülasyonu 290
yapılandırma
mini denetleyici 251–299

Yazdırma Biçimi Uzunluğu

3274 Emülasyonu 267
5250 Emülasyonu 283

Yazdırma Satırı

3274 Emülasyonu 267
5250 Emülasyonu 283

yazılım yükseltmesi

802.IQv2 303

yedekleme

bağlantılar, WDS 205

kullanıcı hesapları veritabanı 71

Yeniden Deneme

Sayısı, dar bant telsiz 228

Yeniden Deneme, Sayısı 228

Yeniden Deneme Sayısı

RRM grubu 238

Yerel

3274 Emülasyonu 261

5250 Emülasyonu 277

yönetici

platform 30

şifre

Temel Ayarlarda 49

Yönetim Bilgi Tabanları (MIB'ler) 213

yönetim web sayfalarında oturum açma 40

yönlü anten 19

yük dengeleme, yapılandırma 183

Yüzde Sorgulama Protokolü Terminal

Zaman Aşımı, Telsiz Bağlantı

Özellikleri 244

Z

Zaman ayarları 311

zaman çoklama 221

Zaman Dilimi 312

zaman, NTP sunucusu kullanmak için AP'yi

yapılandırma 312