

# RFC 2821

## Basit Posta Aktarım Protokolü (SMTP)

Düzenleyen:  
**J. Klensin**  
AT&T Laboratories

Çeviren:  
**Sanem Uçan**  
ÇOMÜ, Bilgisayar Mühendisliği öğrencisi

Düzenleyen:  
**Nilgün Belma Bugüner**  
belgeler.org

Mayıs 2006

### Özet

Bu belge Genel Ağ'da elektronik posta aktarımı için kullanılan temel protokolün müstakil belirtimidir. Aşağıdaki mevcut işlevselliği pekiştirir, günceller ve artırır, fakat yeni bir işlevsellik eklemeyi veya olanı değiştirmeyi amaçlamaz:

- özgün RFC 821 [30] SMTP (Simple Mail Transfer Protocol) belirtimi,
- RFC 1035 [22] ve RFC 974'teki [27] posta aktarımı için alan adı sistemi ile karşılıklı gereksinimler,
- RFC 1123'ten [2] artırımlar ve uygulanabilirlik beyanları ve
- SMTP Eklenti mekanizmalarından [19] süzölmüş bileşenler.

RFC 821 ve RFC 974'ü geçersiz bırakırken RFC 1123'ü günceller (RFC 1123'ün posta aktarım bileşenlerini değiştirir). Bununla birlikte, RFC 821, bazı ek aktarım modellerinde (eklerde bahsedildi) ve 1990'ların ortalarından beri Genel Ağ'da pek kullanılmamış olan bazı özellikleri belirtir. Bu bölümler temizlik, sadelik ve kısalık açısından buraya dahil edilmemiştir; bunları okuma ihtiyacı duyanlar RFC 821'e başvurabilirler.

Ayrıca RFC 1123'ün güçlendirilmesi gereken bazı ek bileşenlerini de içerir. Bu bileşenler çeşitli yollarla, çoğunlukla çeşitli listeler ve haber gruplarındaki şiddet izlenerek ve SMTP eklentilerinin konuşlandırılmaları gereği olarak ortaya çıkan yararsız okuma ve yorumlama sorunlarıyla betimlenebilir. Bu belirtim pekiştirmenin ötesine geçtiği noktada hem metinsel hem de teknik olarak önceki belgelerden farklı olmaktan başka onların da yerini alır.

SMTP'nin bir posta aktarım ve teslim etme protokolü olarak tasarlanmış olmasının yanında, bu belirtim bundan başka POP [3, 26] ve IMAP [6] için önerildiği gibi bir posta teslim alma protokolü olarak kullanımı açısından önem kazanan bilgileri de içerir. Postanın teslim alınması ile ilgili konulara RFC 2476'da da [15] ayrıca değinilmiştir.

*Terminoloji* (sayfa: 9) bölümünde bu belgeye özgü terminolojiye yer verilmiştir. Tarihsel terminolojinin artırım için gerekli olması dışında bu belgedeki istemci ve sunucu terimleri sırasıyla, SMTP gönderim ve alım süreçlerini betimlemek için kullanılmıştır.

Bir eş belge olarak [32] ileti başlıkları, ileti gövdeleri ve bunların yapıları ve biçimleri ile aralarındaki ilişkileri açıklar.

## Konu Başlıkları

<b>1. Giriş</b>	6
<b>2. SMTP Modeli</b>	6
2.1. Temel Yapı	6
2.2. Eklenti Modeli	7
2.2.1. Arkaplan	8
2.2.2. Eklentilerin Tanımlanması ve Kayda Geçirilmesi	8
2.3. Terminoloji	9
2.3.1. Posta Nesneleri	10
2.3.2. Göndericiler ve Alıcılar	10
2.3.3. Posta Aracıları ve İleti Depoları	10
2.3.4. Konak	10
2.3.5. Alan	10
2.3.6. Tampon ve Durum Tablosu	11
2.3.7. Satırlar	11
2.3.8. Oluşturucu, Teslimatçı, Röle ve Ağgeçidi Sistemler	11
2.3.9. İleti İçeriği ve Posta Verisi	11
2.3.10. Posta Kutuları ve Adresler	12
2.3.11. Yanıt	12
2.4. Sözdizimsel Genel Prensipler ve Harekât Modeli	12
<b>3. SMTP Yordamları: Bir Bakış</b>	13
3.1. Oturum İklendirme	13
3.2. İstemci İklendirme	14
3.3. Posta Aktarım Harekâtı	14
3.4. Adres Düzeltmek veya Güncellemek için Yönlendirme	16
3.5. Adres Hatalarını Ayıklama Komutları	16
3.5.1. Genel Bakış	16
3.5.2. VRFY için Normal Yanıt	18
3.5.3. VRFY veya EXPN için Başarılı Yanıtın Anlamı	18
3.5.4. EXPN Uygulamaları ve Anlamsallık	18
3.6. Alanlar	19
3.7. Röleleme	19
3.8. Postanın Ağgeçitlerinden Geçirilmesi	20
3.8.1. Ağgeçitlerinden Geçişte Başlık Alanları	20
3.8.2. Ağgeçitlerinden Geçişte Alınan Satırlar	20
3.8.3. Ağgeçitlerinden Geçişte Adresler	21
3.8.4. Ağgeçitlerinden Geçişte Diğer Başlık Alanları	21
3.8.5. Ağgeçitlerinden Geçişte Zarflar	21
3.9. Oturumların ve Bağlantıların Sonlandırılması	21
3.10. Postalama Listeleri ve Rumuzlar	22
3.10.1. Takma Adlar	22
3.10.2. Listeler	22
<b>4. SMTP Belirtimi</b>	22
4.1. SMTP Komutları	22
4.1.1. Komut Sözdizimi ve Anlamlandırma	22
4.1.1.1. Ayrıntılı Selamlama (EHLO) veya Sade Selamlama (HELO)	23
4.1.1.2. Posta' (MAIL komutu)	24
4.1.1.3. Alıcının Belirtilmesi (RCPT komutu)	24
4.1.1.4. Posta Verisi (DATA komutu)	25
4.1.1.5. Sıfırlama (RSET komutu)	26

4.1.1.6. Posta Kutusu Doğrulama (VRFY komutu)	26
4.1.1.7. Liste ve Üyelik Doğrulama (EXPN komutu)	26
4.1.1.8. Yardım (HELP komutu)	26
4.1.1.9. Eylemsizlik (NOOP komutu)	27
4.1.1.10. Çıkış (QUIT komutu)	27
4.1.2. Komut Argümanlarının Sözdizimi	27
4.1.3. IP Kodlu Adlar	29
4.1.4. Komutların Sırası	29
4.1.5. Özel Kullanımlı Komutlar	30
4.2. SMTP Yanıtları	30
4.2.1. Yanıt Kodlarının Önemleri ve Kuram	31
4.2.2. İşlev Gruplarına göre Yanıt Kodları	33
4.2.3. Numara Sırasıyla Yanıt Kodları	34
4.2.4. 502 Yanıt Kodu	34
4.2.5. <CRLF>.<CRLF>'in Ardından DATA Komutuna Yanıt	34
4.3. Komutların ve Yanıtların Sıralanışı	35
4.3.1. Sıralanışa Genel Bakış	35
4.3.2. Komut–Yanıt Sıralanışı	36
4.4. İzleme Bilgisi	37
4.5. Gerçeklenimle İlgili Ek Hususlar	39
4.5.1. Asgari Gerçeklenim	39
4.5.2. Şeffaflık	40
4.5.3. Boyutlar ve Zamanaşlımları	40
4.5.3.1. Boyut sınırları ve asgari değerler	40
4.5.3.2. Zamanaşlımları	42
4.5.4. Yanıt Stratejileri	43
4.5.4.1. Gönderme Stratejisi	43
4.5.4.2. Alım Stratejisi	44
4.5.5. Dönüş yolu boş olan iletiler	44
<b>5. Adres Çözümleme ve Posta Yönetimi</b>	44
<b>6. Sorun Saptama ve Giderme</b>	45
6.1. Güvenilir Teslimat ve Eposta Yanıtları	45
6.2. Döngü Algılama	46
6.3. Düzensizliklerin Giderilmesi	46
<b>7. Güvenlik Kaygıları</b>	47
7.1. Posta Güvenliği ve Yanıltma	47
7.2. "Gizli" Kopyalar	48
7.3. VRFY, EXPN ve Güvenlik	48
7.4. Duyurularda Bilgi İfşası	48
7.5. İzleme Alanlarında Bilginin İfşası	48
7.6. İleti Yönlendirmede Bilginin İfşası	49
7.7. SMTP Sunucularının Harekat Alanı	49
<b>8. IANA Değerlendirmeleri</b>	49
<b>9. Kaynakça</b>	49
<b>10. Yazarın Adresi</b>	52
<b>11. Teşekkür</b>	52
<b>A. TCP İletim Hizmeti</b>	53
<b>B. SMTP Komutlarının RFC 822 Başlıklarından Üretilmesi</b>	53
<b>C. Kaynak Rotalar</b>	53
<b>D. Senaryolar</b>	54

<i>D.1. Tipik bir SMTP Aktarım Senaryosu</i>	54
<i>D.2. Sıfırlanan bir SMTP Aktarım Senaryosu</i>	55
<i>D.3. R�leli Posta Senaryosu</i>	55
<i>D.4. Doğrulama ve Gönderme Senaryosu</i>	56
<b>E. Diğer Ağgeçidi Konuları</b>	57
<b>F. RFC 821'in Önerilmeyen Özellikleri</b>	57
<b>G. Tam Telif Hakkı Beyanı</b>	58

## Geçmiş

1.1	Ağustos 2006	NBB
Çeviriye *ZORUNLU*, *ÖNERİ* ve *SEÇİMLİK* imlerini yerleştirdi ve çeviri metninin bazı yerlerini buna göre düzeltti.		
1.0	Mayıs 2006	SU
İlk çeviri		
Standart Aday Adayı	Nisan 2001	JK
Özgün sürüm		

## Sürüm Bilgileri

Ağ Çalışma Grubu  
Açıklama İsteği: 2821  
Geçersiz kıldığı RFC'ler: 821, 974, 1869  
Geçersiz kıldığı STD: 10  
Güncellediği RFC: 1123  
Durumu: Standart Aday Adayı

## Yasal Uyarı

RFC'lerin yazarlarının hakları [BCP 78<sup>\(B1\)</sup>](#) ile düzenlenmiştir. Dolayısıyla RFC çevirilerinin çevirmenlerinin haklarını da BCP 78'in düzenlediği kabul edilmiştir.

Bu belge [IETF<sup>\(B3\)</sup>](#) tarafından yayınlanan resmi RFC2821'in **gayriresmi** çevirisidir ve aslının yerine kullanılamaz. Bu çevirinin hiçbir bağlamda ya da koşulda hükmü yoktur. Bu çeviri, anadili Türkçe olan Genel Ağ kullanıcılarının bu RFC hakkında fikir edinebilmelerini sağlamak amacıyla hazırlanmıştır.

BU BELGE "ÜCRETSİZ" OLARAK RUHSATLANDIĞI İÇİN, İÇERDİĞİ BİLGİLER İÇİN İLGİLİ KANUNLARIN İZİN VERDİĞİ ÖLÇÜDE HERHANGİ BİR GARANTİ VERİLMEMEKTEDİR. AKSİ YAZILI OLARAK BELİRTİLMEDİĞİ MÜDDETÇE TELİF HAKKI SAHİPLERİ VE/VEYA BAŞKA ŞAHISLAR BELGEYİ "OLDUĞU GİBİ", AŞIKAR VEYA ZIMNEN, SATILABİLİRLİĞİ VEYA HERHANGİ BİR AMACA UYGUNLUĞU DA DAHİL OLMAK ÜZERE HİÇBİR GARANTİ VERMEKSİZİN DAĞITMAKTADIRLAR. BİLGİNİN KALİTESİ İLE İLGİLİ TÜM SORUNLAR SİZE AİTTİR. HERHANGİ BİR HATALI BİLGİDEN DOLAYI DOĞABİLECEK OLAN BÜTÜN SERVİS, TAMİR VEYA DÜZELTME MASRAFLARI SİZE AİTTİR.

İLGİLİ KANUNUN İCBAR ETTİĞİ DURUMLAR VEYA YAZILI ANLAŞMA HARİCİNDE HERHANGİ BİR ŞEKİLDE TELİF HAKKI SAHİBİ VEYA YUKARIDA İZİN VERİLDİĞİ ŞEKİLDE BELGEYİ DEĞİŞTİREN VEYA YENİDEN DAĞITAN HERHANGİ BİR KİŞİ, BİLGİNİN KULLANIMI VEYA KULLANILAMAMASI (VEYA VERİ KAYBI OLUŞMASI, VERİNİN YANLIŞ HALE GELMESİ, SİZİN VEYA ÜÇÜNCÜ ŞAHISLARIN ZARARA UĞRAMASI VEYA BİLGİLERİN BAŞKA BİLGİLERLE UYUMSUZ OLMASI) YÜZÜNDEN OLUŞAN GENEL, ÖZEL, DOĞRUDAN YA DA DOLAYLI HERHANGİ BİR ZARARDAN, BÖYLE BİR TAZMİNAT TALEBİ TELİF HAKKI SAHİBİ VEYA İLGİLİ KİŞİYE BİLDİRİLMİŞ OLSA DAHİ, SORUMLU DEĞİLDİR.

Tüm telif hakları aksi özellikle belirtilmediği sürece sahibine aittir. Belge içinde geçen herhangi bir terim, bir ticari isim ya da kuruma itibar kazandırma olarak algılanmamalıdır. Bir ürün ya da markanın kullanılmış olması ona onay verildiği anlamında görülmemelidir.

## Bu Belgenin Durumu

Bu belge Genel Ağ topluluğu yararına standartlaşma sürecine girmiş bir protokolü belirtir ve geliştirilmesi için tartışılmayı ve öneriler almayı bekler. Bu protokolün standartlaşma sürecinde bulunduğu aşama ve durum için lütfen "Genel Ağ Resmi Protokol Standartları" (STD1) isimli belgenin son yayımına bakınız. Bu belgenin dağıtımına sınırlama konmamıştır.

Copyright (C) The Internet Society (2001). All Rights Reserved.

Telif Hakkı © The Internet Society (2001). Tüm Hakları Saklıdır.

## 1. Giriş

Basit Posta İletim Protokolü'nün (SMTP – Simple Mail Transfer Protocol) amacı, postanın verimli ve güvenli bir şekilde aktarımıdır.

SMTP, bellibaşlı aktarım altsistemlerinden bağımsız olup sadece düzenli çalışan bir veri akımı kanalı gerektirir. Bu belge aktarım için TCP'den bahsederse de diğer aktarım yöntemleri de mümkündür. Eklerdeki RFC 821 ile ilgili bölümde bunların bazılarından bahsedilmiştir.

SMTP'nin önemli bir özelliği, çoğunlukla "SMTP posta rölelemesi" denilen yöntemle (bkz. [Postanın Ağgeçitlerinden Geçirilmesi](#) (sayfa: 20)) ağ üzerinden posta aktarımı yapma yeteneğidir. Bir ağ Genel Ağ'da karşılıklı olarak TCP üzerinden erişilebilen konaklardan oluşabileceği gibi bir güvenlik duvarı ile yalıtılmış bir TCP/IP ağında karşılıklı olarak TCP üzerinden erişilebilen konaklardan veya başka bir geniş veya yerel ağ ortamında TCP-dışı bir aktarım protokolü kullanan konaklardan da oluşabilir. SMTP kullanarak, bir süreç aynı ağ içindeki başka bir sürece posta aktarabileceği gibi aynı ağ veya başka bir ağdaki başka bir sürece de aynı anda bir röle veya ağgeçidi üzerinden posta aktarılabilir.

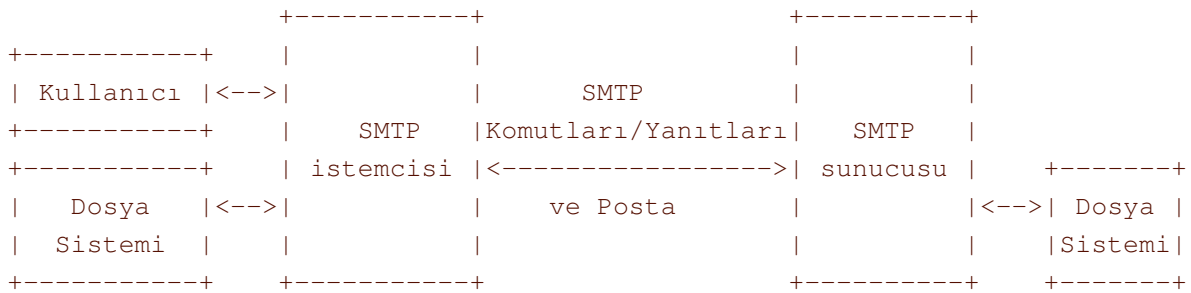
Bir posta iletisi göndericisinden nihai alıcısına giderken yolu bazı röle veya ağgeçidi konaklardan geçebilir. Alan adı sisteminin posta aktarımcı (MX) mekanizmaları [22, 27] (ve bu belgenin [Adres Çözümleme ve Posta Yönetimi](#) (sayfa: 44) bölümü) bir iletinin aktarılacağı sonraki en uygun sıçrama noktasını tayin etmekte kullanılır.

## 2. SMTP Modeli

### 2.1. Temel Yapı

SMTP tasarımı şöyle resmedilebilir:

Şekil 1.



SMTP istemcisinin iletilmek üzere bir iletisi olduğunda, bir SMTP sunucusuna iki yönlü bir aktarım kanalı kurar. SMTP istemcisinin sorumluluğu, posta iletilerini bir veya daha fazla sayıda SMTP sunucusuna aktarmak ve eğer varsa hataları raporlamaktır.

Bir posta iletinin SMTP istemcisine sunulması ve istemci tarafından hangi posta iletilerinin hangi alan isimlerine aktarılacağına tespiti yerel konulardan olup bu belgede bu konulara değinilmeyecektir. Bazı durumlarda, alan isimlerinin SMTP istemcisine aktarılması ya da istemci tarafından saptanması durumlarında posta iletinin son hedefini SMTP istemcisi tayin edecektir. SMTP istemcisinin yalıtılmış bir aktarım hizmeti ortamının içinde kaldığı veya POP [3, 26] veya IMAP [6] gerçekleştirmeleri ile ilişkili SMTP istemcileriyle ortaklaşılan bazı durumlarda, saptanan alan ismi tüm posta iletilerinin rölelenmesini sağlayan ara hedefi tayin edecektir. Tek tek iletilerle ilişkilendirilmiş hedef alan isimlerine bakmaksızın tüm trafiği aktaran veya dahili olarak tamamlanamayan aktarımlara iletileri yeniden göndermek için kuyruklar sağlayan SMTP istemcileri, bu protokola bir şekilde uyum sağlayabilir fakat tamamen yetkin sayılmazlar. Tamamen yetkin SMTP gerçekleştirmelerinin, daha az yetkin olanlardan röleme kullananlar da dahil olmak üzere, bu belirtimde açıklanan tüm kuyruklama, yeniden gönderme ve diğer adres işlevlerini destekleyeceği umulur.

Bir SMTP istemcisinin, bir hedef alan ismi saptayıp, iletinin bir kopyasının aktarılacağı SMTP sunucusunun kimliğini saptaması ve aktarımı gerçekleştirmesi bu belgenin kapsamına girmektedir. Bu anlamda, bir SMTP sunucusuna bir posta aktarımı için bir SMTP istemcisi SMTP sunucusuna iki yönlü bir aktarım kanalı kurar. SMTP istemcisi bir SMTP sunucusu çalıştıran uygun bir konağın adresini, bir ara posta aktarımcısı (MX) veya son alıcı konağın alan adı olarak çözümleyerek saptar.

Bir SMTP sunucusu ya bir nihai hedef ya bir ara "röle" (iletiyi aldıktan sonra aktaran bir SMTP istemcisinin rölesi olarak da kabul edilebilir) ya da bir "ağgeçidi" olabilir (iletiyi SMTP dışında bir protokol kullanarak aktaran anlamında ele alınabilir). SMTP komutları SMTP istemcisi tarafından üretilir ve SMTP sunucusuna gönderilir. SMTP yanıtları ise SMTP sunucusundan SMTP istemcisine komutlara yanıt olarak gönderilir.

Başka bir deyişle, ileti aktarımı özgün SMTP göndericisi ile nihai SMTP alıcısı arasındaki tek bir bağlantıda oluşabileceği gibi bir sürü ara bağlantı üzerinden hoplaya hoplaya da gerçekleşebilir. Her iki durumda da, biçimsel olarak iletinin sorumluluğunun terki durumu ortaya çıkar: protokol, ya bir iletinin teslimi ya da yapamıyorsa başarısızlığın düzgün olarak raporlanması anlamında bir sunucunun sorumluluğu kabul etmesini gerektirir.

Aktarım kanalı kurulup ilk el sıkışma tamamlandıktan sonra, SMTP istemcisi normal olarak posta aktarımını başlatır. Böyle bir hareket, postanın oluşturucusu ve hedefi ile iletinin kendisinin (başlıklar ve bir takım başka yapıları da içererek) aktarımını belirten bir sürü komuttan oluşur. Aynı ileti çok sayıda alıcıya gönderildiği zaman, bu protokol, aynı hedef konaktaki (veya ara rölelerdeki) tüm alıcılar için verinin sadece tek bir kopyasının aktarımını destekler.

Sunucu her komutu bir cevapla yanıtlar; yanıtlar, komutların kabul edildiğini, ek komutların beklendiğini veya bir geçici yahut kalıcı bir hata durumunun mevcut olduğunu belirtebilir. Gönderici veya alıcı belirtilerek komutlarda *Eklenti Modeli* (sayfa: 7) bölümünde açıklandığı gibi sunucu izinli SMTP ek hizmet istekleri bulunabilir. Komut borulama [13] gibi ek isteklerde bulunarak karşılıklı kabullerle değiştirilebilir olsa bile görüşme, amaca uygun olarak her seferinde tek bir adımı gerçekleştirmek biçiminde yapılır.

Bir posta ileti aktarımının bitmesinin ardından istemci bağlantının kapatılmasını isteyebileceği gibi başka bir postanın aktarımını da başlatabilir. Ek olarak, bir SMTP istemcisi bir SMTP sunucusuyla olan bağlantıyı, eposta adreslerinin doğrulanması veya posta listesinin üye adreslerinin alınması gibi yan hizmetler için de kullanabilir.

Yukarıda değinildiği gibi, bu protokol posta aktarımı için mekanizmaları sağlar. Bu aktarım normal olarak, gönderen kullanıcının konağı ile alan kullanıcının konağı arasında ancak her iki konak da aynı aktarım hizmetine bağlı olduğunda doğrudan doğruya gerçekleşir. Aynı aktarım hizmetine bağlı olmadıkları takdirde, aktarım bir veya daha fazla SMTP sunucusunun postayı rölelemesi ile mümkün olur. Bir SMTP rölesi veya başka aktarım ortamlarına bir ağgeçidi olarak davranan bir ara konak genellikle alan adı hizmetinin (DNS) posta aktarımcısı mekanizması (MX) kullanılarak seçilir.

Çoğunlukla ara konaklar açıkça "kaynak" yönlendirme ile değil, DNS MX kaydı sayesinde tespit edilirler (*Adres Çözümleme ve Posta Yönetimi* (sayfa: 44), *Kaynak Rotalar* (sayfa: 53) ve *Kaynak Yönlendirme* (sayfa: 57) bölümlerine bakınız).

## 2.2. Eklenti Modeli

### 2.2.1. Arkaplan

1990'da başlayıp, RFC 821'in tamamlanmasından sonraki 10 yılın çalışmalarıyla protokol bir "hizmet ekleri" modeliyle değişikliğe uğratıldı. Bu model istemci ve sunucuya özgün SMTP gereksinimlerinin ötesinde, paylaşımlı işlevsellikten yararlanmayı kabul etmeye izin vermektedir. SMTP eklenti mekanizması eklentili SMTP istemcisi ve sunucusunun birbirlerini tanıyabilecekleri ve sunucunun desteklediği hizmet eklentileri hakkında istemciyi bilgilendirebileceği bir yapı tanımlar.

Çağdaş SMTP gerçekleştirmelerinin temel eklenti mekanizmalarını desteklemesi gerekir \*ZORUNLU\*. Örneğin, herhangi bir özel eklenti gerçekleştirmeler bile, sunucuların **EHLO** komutunu desteklemeleri ve istemcilerin de ayrıcalıklı olarak **HELO** komutundan ziyade **EHLO** komutundan yararlanmaları gerekir \*ZORUNLU\*. (Bununla birlikte, eski gerçekleştirmelerle uyumluluk açısından SMTP istemcilerinin ve sunucularının bir son çare olarak **HELO** mekanizmasını da desteklemesi gerekir \*ZORUNLU\*.) **HELO** komutunun farklı karakteristikleri birlikte çalışabilirlik amacıyla betimlenmiş olmadıkça, bu belgede sadece **EHLO** komutundan bahsediliyor olunacaktır.

SMTP'nin geniş çapta uygulanmış ve yüksek kaliteli gerçekleştirmelerinin çok sağlam olacağı ortaya çıkmıştır. Yine de, Genel Ağ topluluğu bazı hizmetlerin şimdilerde, protokol ilk tasarlandığında umulmayan bir öneme kavuştuğunu düşünmektedir. Eğer bu hizmetler için destek eklenecek olursa, bunun eski gerçekleştirmelerin çalışmaya devam etmesine izin verecek bir yolla yapılması gerekir. Eklentilerle ilgili şöyle bir çerçeve çizilebilir:

- Eski SMTP komutu **HELO**'nun yerini **EHLO** komutunun alması,
- SMTP hizmet eklentilerinin bir kaydının tutulması,
- SMTP **MAIL** ve **RCPT** komutlarına ek parametreler ve
- ASCII olmayan [33] aktarımlardaki **DATA** komutundaki gibi bu protokolde tanımlanmış komutlar için isteğe bağlı değişiklikler.

SMTP'nin gücü, öncelikle basitliğinden gelmektedir. Protokollerle ilgili deneyimler, az seçenekli protokollerin her yerde hazır ve nazır olurken, çok seçenekli protokollerin pek ortalıkta görünmediklerini ortaya koymuştur.

Getirilerine bakmaksızın her eklenti gerek gerçekleştirmeler gerek konuşulmuş gerekse birlikte çalışabilirlik maliyetleri bakımından ayrı ayrı dikkatle irdelenmelidir. Çoğu durumda, SMTP hizmetinin eklentilerle genişletilmesinin maliyeti beklenen yarardan ağır olmaktadır.

### 2.2.2. Eklentilerin Tanımlanması ve Kayda Geçirilmesi

IANA, SMTP hizmet eklentilerinin bir kaydını tutar. Her eklenti uygun bir **EHLO** anahtar sözcük değeri ile ilişkilendirilir. IANA ile kayda geçirilmiş her hizmet eklentisi biçimsel olarak standartlaşma aşamalarında bulunan bir protokol belgesinde ya da IESG onaylı bir deneysel protokol belgesinde tanımlanmış olmalıdır. Bu tanım şunları içermelidir:

- SMTP hizmet eklentisinin açık ismi;
- eklenti ile ilişkili **EHLO** anahtar sözcük değeri;
- **EHLO** anahtar sözcük değeri ile ilişkili parametrelerin sözdizimi ve tek tek olası değerleri;
- eklenti ile ilgili ilave SMTP fiilleri (ilave fiiller genelde olur, ama olması gerekli değildir, tıpkı **EHLO** anahtar sözcük değeri gibi);
- **MAIL** veya **RCPT** fiilleri ile ilişkili eklentilerin tek tek yeni parametreleri;
- bir sunucu ve istemci SMTP'nin davranışını etkileyen bu eklentinin nasıl destekleneceğinin bir açıklaması; ve
- **MAIL** ve/veya **RCPT** komutlarının azami uzunluğunu arttıran eklentinin bu standartta belirtilene ne kadar daha artış getirdiği.



Ek olarak, büyük veya küçük harf olarak bir "X" ile başlayan herhangi bir **EHLO** anahtar sözcük değeri, özellikle iki taraflı uzlaşma üzerinden kullanılan yerel bir SMTP eklentisi belirtir. "X" ile başlayan anahtar sözcükler kayıtlı bir hizmet eklentisinde kullanılmamalıdır **\*ZORUNLU\***. Aksine, **EHLO** yanıtlarında sunulmuş anahtar sözcük değerlerinden "X" ile başlamayanların standart, standart aday, standart aday veya IESG onaylı deneysel bir protokolle tanımlanmış ve IANA ile kayda geçirilmiş bir SMTP hizmet eklentisine karşılık olması gerekir **\*ZORUNLU\***. Uyumlu bir sunucunun, "X" ile başlamayan ve kayıtlı bir eklentide açıklanmamış bir anahtar sözcük değeri sunmaması gerekir **\*ZORUNLU\***.

Ek fiiller ve parametre isimleri **EHLO** anahtar sözcüğüne uygulanan kurallara tabidirler; özellikle, "X" ile başlayan fiiller yerel eklentilerden olup kayıtlı veya standartlaştırılmış olamazlar. Ancak, "X" ile başlamayan fiillerin daima kayda geçirilmiş olmaları gerekir.

## 2.3. Terminoloji

Özgün İngilizce metindeki "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" ve "OPTIONAL" anahtar sözcüklerinin yerine kullanılan Türkçe karşılıklar ve bunlarla belgede karşılaşıldığında nasıl yorumlanmaları gerektiği aşağıda açıklanmıştır. Dilimizde fiillerin çekimleri için ayrı birer sözcük bulunmadığından bunların geçtiği cümleler aşağıdaki gibi imlenmiştir.

### **\*ZORUNLU\***

Bu imleme özgün metindeki MUST, REQUIRED veya SHALL terimlerinin yerine kullanılmıştır ve belirtimdeki bahse konu niteliğin mutlaka gerçekleşmesi gereken bir nitelik olduğunu belirtir.

### **\*YASAK\***

Bu imleme özgün metindeki MUST NOT veya SHALL NOT terimlerinin yerine kullanılmak için tasarlanmış ama yerine **\*ZORUNLU\*** imi kullanılmıştır (olumsuz cümleyi olumlamaması için) ve belirtimdeki bahse konu niteliğin kesinlikle gerçekleşmemesi gereken bir nitelik olduğunu belirtir.

### **\*ÖNERİ\***

Bu imleme özgün metindeki SHOULD veya RECOMMENDED terimlerinin yerine kullanılmıştır ve belli durumlarda belli bir önerinin yoksayılmasını gerektiren geçerli sebeplerin elbette varolabileceği ancak farklı bir rota seçmeden önce tüm olasılıkların anlaşılması ve ağırlıklarının dikkatle gözden geçirilmesinin de gerekliliğini belirtir.

### **\*ÖNERİLMEZ\***

Bu imleme özgün metindeki SHOULD NOT veya NOT RECOMMENDED terimlerinin yerine kullanılmak için tasarlanmış ama yerine **\*ÖNERİ\*** imi kullanılmıştır (olumsuz cümleyi olumlamaması için) ve belli bir davranışın kabul edilebilir hatta yararlı olduğu belli durumlarla ilgili geçerli sebeplerin tabii ki varolabileceği ancak bahse konu davranış gerçekleşmeden önce tüm olasılıkların anlaşılması ve ağırlıklarının dikkatle gözden geçirilmesinin de gerekliliğini belirtir.

### **\*SEÇİMLİK\***

Bu imleme özgün metindeki MAY veya OPTIONAL terimlerinin yerine kullanılmıştır ve belirtimdeki bahse konu niteliğin gerçekleşmesinin gerçekten isteğe bağlı olduğunu belirtir. Bir üretici belli bir seçeneği pazar onu istiyor diye ya da başka bir üreticinin bu seçeneği sağlamayan bir ürününe üstün olması için ürününde bulundurmamayı isteyebilir. Belli bir seçeneği içermeyen bir gerçekleşimin aynı seçeneği içeren bir gerçekleşimle, hatta işlevselliği azaltarak olsa bile, birarada çalışabilmeye hazır olması gerekir **\*ZORUNLU\***. Aynı minvalde, belli bir seçeneği

içeren bir gerçekenimin de aynı seçeneği içermeyen bir gerçekenimle birarada çalışabilmeye hazır olması gerekir \*ZORUNLU\* (tabii ki seçeneği sağlayan özellik için değil).

### 2.3.1. Posta Nesneleri

SMTP posta nesnesi aktarır. Bir posta nesnesi ise bir zarf ve zarfın içindekilerden oluşur.

SMTP zarfı ardarda uygulanan SMTP protokol birimleriyle gönderilir (*SMTP Yordamları: Bir Bakış* (sayfa: 13) bölümünde açıklanmıştır). Zarf, bir tasarlayıcı adresi (hatalar ona raporlanır), en az bir tane alıcı adresi ve isteğe bağlı protokol eklenti bileşenlerinden oluşur. Geçmişte, gönderici adresini belirten komutun (**RCPT TO**) çeşitli şekilleri, hemen bakıverme gibi başka teslimat kiplerini belirtmekte kullanılırdı; bu kullanım şekilleri artık önerilmemektedir (*RFC 821'in Önerilmeyen Özellikleri* (sayfa: 57) ve *Postalamayıp Gönderivermek* (sayfa: 58) bölümlerine bakınız).

SMTP içeriği, SMTP **DATA** protokolü biriminde gönderilir ve iki kısımdan oluşur: başlıklar ve gövde. Eğer içerik diğer çağdaş standartlarla uyumluysa, başlıklar, ileti biçimi belirtimindeki [32] gibi bir isim/değer çiftleri listesi şeklinde olur; gövde ise, eğer yapılandırılmışsa, MIME'ye [12] uygun olarak tanımlanmıştır. İçerik metinsel bir doğaya sahip olup, US-ASCII karakter kümesi [1] kullanılarak oluşturulur. SMTP eklentileri ("8BITMIME" [20] gibi) içerik gövdesi açısından bu sınırlamaları esnetebildiğinden, içerik başlıkları daima US-ASCII karakter kümesi kullanılarak kodlanır. US-ASCII karakter kümesi dışındaki başlık değerlerini US-ASCII karakter kümesini kullanarak ifade edebilmek için bir MIME eklentisi [23] olarak bir algoritma tanımlanmıştır.

### 2.3.2. Göndericiler ve Alıcılar

RFC 821'de SMTP aktarımının taraflarını oluşturan iki konak "SMTP-gönderici" ve "SMTP-alıcı" olarak açıklanmıştı. Bu belgede şu an ki endüstri terminolojisini yansıtmak için bu kullanım değiştirilmiş olup, bunlardan bahsedilirken sırasıyla "SMTP istemcisi" (bazan sadece "istemci") ve "SMTP sunucusu" (veya sadece "sunucu") terimleri kullanılmıştır. Belirtilen konağın bir röle olması durumunda, konak hem sunucu hem istemci olarak davranabildiğinden yapılane açıklık getirmek amacıyla hala "alıcı" ve "gönderici" terminolojisi de kullanılmaktadır.

### 2.3.3. Posta Aracıları ve İleti Depoları

Ek posta sistemi terminolojisi RFC 821 yayınlandıktan sonra yaygın duruma geldi ve uygun düştükçe de bu belirtimde kullanıldı. Kısmen, SMTP sunucuları ve istemcileri bir posta aktarım hizmeti sağlamaları nedeniyle "Posta Aktarım Aracıları" (MTA – Mail Transfer Agent) gibi davranırlar. "Posta Kullanıcı Aracıları" (MUA veya UA – Mail User Agent) ise postanın kaynakları ve hedefleri olarak düşünülürler. Kaynakta, MUA'lar bir kullanıcıdan aktarılmış olan postayı toplarlar ve bir MTA'ya bırakırlar; nihai ("teslimatçı") MTA'lar ise postayı bir MUA'ya bırakan araçlar olarak (veya en azından örneğin iletiyi bir "ileti deposu"na emanet eden bir posta aktarma sorumlusu olarak) düşünülür. Bununla birlikte, bu terimler başka yerlerde en azından görünürde oldukça kesin tanımlıymış gibi kullanılmasına rağmen MUA'lar ve MTA'lar arasında varolduğu öngörülen sınır çizgisi, Genel Ağ postasıyla ilgili kabullere/standartlara uyan ortak pratiklere genellikle tam olarak uymaz. Dolayısıyla okuyucu, bu terimlerin geçtiği diğer yerlerde yapılan öngörülere bağlı olarak kavramlar arasında sıkı ilişkiler ve sorumluluklar olduğu sonucunu kolayca çıkarmamalıdır.

### 2.3.4. Konak

Bu belirtimin amacına uygun olarak, bir konak Genel Ağ'a (veya bazı durumlarda, özel bir TCP/IP ağına) bağlı ve SMTP protokolünü destekleyen bir bilgisayar sistemidir. Konaklar isimleriyle bilinirler (bkz: "Alan"; hemen aşağıda...); sayısal adreslerle tanımlamaktan artık vazgeçilmiştir.

### 2.3.5. Alan

Bir alan (veya alan adı) noktalarla ayrılmış bileşenlerden oluşur. Bu bileşenlerde (DNS terminolojisinde [22] "yaftalar") SMTP'nin amacına uygun olarak sadece ASCII karakter kümesindeki [1] harfler, rakamlar ve tire işaretleri kullanılabilir. Alan isimleri konakların ve alan adı hiyerarşisindeki diğer öğelerin isimleri olarak kullanılırlar. Örneğin, bir alan, bir rumuza (bir CNAME kaydı) atıf yapabileceği gibi bir konak ismini göstermek yerine postayı teslim almakta kullanılan posta aktarımcı (MX) yaftasına da atıf yapılabilir. [22] ve bu belirtimin *Adres Çözümleme ve Posta Yönetimi* (sayfa: 44) bölümüne bakınız.

Alan adı bu belgede ve [22] belgesinde açıklandığı gibi bir bütündür ve tamamen nitelikli bir isimdir (İngilizce "Fully-Qualified Domain Name", kısaca "FQDN" olarak bilinir). FQDN biçiminde olmayan bir alan adı bir yerel rumuzdan başka birşey değildir. Yerel rumuzlar herhangi bir SMTP aktarımında görünmemelidir \*ZORUNLU\*.

### 2.3.6. Tampon ve Durum Tablosu

SMTP oturumları, mevcut durumun ortak bir görünümünü her iki tarafında dikkatle sürdürmesi bakımından durumsaldır. Bu belgede, bu durumu sunucu üstündeki bir sanal "tampon" ve bir "durum tablosu"na göre modelleyeceğiz. Bu durum aynı zamanda bir istemci tarafından da örneğin "tamponu temizle" veya "durum tablosunu sıfırla" şeklinde, tampondaki bilginin iptal edilmesinin ve önceki durumlardan birine dönülmesinin sağlanması biçiminde kullanılabilir.

### 2.3.7. Satırlar

SMTP komutları ile bir hizmet eklentisi tarafından değiştirilmedikçe ileti verisi "satırlar" halinde aktarılır. Satırlar, ASCII karakterlerinden sırayla "CR" (onaltılık kodu: 0D) ve "LF" (onaltılık kodu: 0A) ile biten sıfır veya daha fazla veri karakterinden oluşur. Bu satır sonlandırma dizgesini bu belgede <CRLF> biçiminde kullanacağız. Uyumlu gerçekleştirmelerin bir satır sonlandırıcı olarak başka bir karakter dizisi üretmemeleri veya bunları tanımamaları gerekir \*ZORUNLU\*. Satır uzunluğu ile ilgili sınırlar konusunda sunucular zorlayıcı olabilir \*ÖNERİ\* (*Boyutlar ve Zamanışım* (sayfa: 40) bölümüne bakınız).

Ek olarak, "CR" ve "LF" karakterlerinin metin içinde "çıplak" olarak (yani diğeri olmaksızın) görünmesinin, posta sistemini bir araç olarak kullanan posta gerçekleştirmeleri ve uygulamalarında yolaçtığı sorunlarla ilgili uzun bir geçmiş vardır. SMTP istemci gerçekleştirmeleri, satır sonlandırıcı olarak kullanmak dışında, bu karakterleri aktarmamalıdır \*ZORUNLU\* ve yukarıda değinildiği gibi sadece bir <CRLF> dizgesi olarak aktarmalıdır \*ZORUNLU\*.

### 2.3.8. Oluşturucu, Teslimatçı, Röle ve Ağgeçidi Sistemler

Bu belirtim, SMTP sistemlerinin dört türü arasında elektronik posta aktarımında oynadıkları rollere göre bir ayrıma gider. "Oluşturucu" sistem (bazan SMTP oluşturucu da denir) postayı Genel Ağ'a veya daha da genel olarak bir aktarım hizmeti ortamına salan sistemdir. "Teslimatçı" SMTP sistemi, postayı bir aktarım hizmeti ortamından alıp ya bir posta kullanıcısı aracısına aktarır ya da posta kullanıcı aracısının bir ara uğrayıp alacağını umduğu bir ileti deposuna emanet eder. "Röle" SMTP sistemi (genellikle sadece "röle" denir), postayı bir SMTP istemcisinden alır ve izleme bilgisi eklemek dışında ileti verisine dokunmaksızın, tekrar rölelenmek veya teslim edilmek üzere başka bir SMTP sunucusuna aktarır. "Ağgeçidi" SMTP sistemi (genellikle sadece "ağgeçidi" denir) ise, bir aktarım ortamındaki bir istemci sistemden postayı alır ve başka bir aktarım ortamındaki bir sunucu sisteme aktarır.

Protokollerin veya iletilerin anlambilimsel yapılarının aralarındaki, bir ağgeçidinin her iki tarafındaki aktarım ortamlarındaki farklarından dolayı, SMTP röleleme sistemleri söz konusu olduğunda izin verilmeyen ileti dönüşümlerinin ağgeçidi sisteminde uygulanması gerekebilir. Bu belirtimin amaçları gereği, adresleri yeniden yazan güvenlik duvarları, her iki tarafında da SMTP kullanılıyor olsa bile, ağgeçitleri olarak ele alınırsa daha iyi olur [11].

### 2.3.9. İleti İçeriği ve Posta Verisi

**DATA** komutundan sonra kabul edilmiş ama veri sonu belirticiden önce aktarılmış olan malzemeyi betimlemek için "ileti içeriği" ve "posta verisi" terimleri bu belgede birbirlerinin yerine kullanılmıştır. İleti içeriği ileti başlıklarını ve "yapılandırılmış olması olası" ileti gövdesini içerir. MIME belirtimi [12] yapılandırılmış ileti gövdeleri ile ilgili standart mekanizmaları sağlar.

### 2.3.10. Posta Kutuları ve Adresler

Bu belirtimdeki kullanımına göre, bir "adres" postanın gönderileceği kullanıcıyı veya postanın emanet edileceği yeri betimleyen bir karakter dizisidir. "Posta kutusu" terimi ise, bu emanet yerini ifade eder. Bu iki terim, postanın bırakılacağı yer (posta kutusu) ile teslim alacak kullanıcı (adres) arasındaki farkın önemli olması dışında, genel olarak birbirlerinin yerlerine kullanılırlar. Bir adres normalde kullanıcı ve alan belirtilmelerinden oluşur. Standart posta kutusu isimlendirme uzlaşımı "yerel-kısım@alan" biçiminde tanımlanmıştır: çağdaş kullanım basit "kullanıcı isimlerinden" çok daha geniş bir uygulama kümesine izin verir. Bu sebeple ve ara konakların aktarımı eniyilemeye çalışmak adına değişiklik yapmaları sebebiyle ortaya çıkan sorunların uzun bir geçmişe sahip olmasından dolayı, yerel-kısımın, sadece adresin alan parçasında belirtilen konak tarafından atanan ve yorumlanan anlamsal biçimde olması/kalması gerekir \*ZORUNLU\*.

### 2.3.11. Yanıt

Bir SMTP yanıtı, bir komuta cevap olarak aktarım kanalı üzerinden alıcıdan göndericiye gönderilen bir (olumlu veya olumsuz) alındır. Bir yanıtın genel biçimi (başarı veya başarısızlık belirten) bir sayısal tamamlama kodu ile başlayan bir metin dizgesidir. Kodlar programlar tarafından kullanılmak için, metin ise normal olarak insan kullanıcılar için tasarlanmıştır. En son çalışmada [34] ek ve daha özel tamamlama kodları da dahil olmak üzere yanıt dizgelerinin böyle bir yapılandırması belirlenmiştir.

## 2.4. Sözdizimsel Genel Prensipler ve Harekât Modeli

SMTP komutlarının ve yanıtlarının sözdizimleri katı kurallara sahiptir. Tüm komutlar bir komut fiiliyle başlar. Tüm yanıtlar ise üç hanelik bir sayısal kod ile başlar. Bazı komutlarda ve yanıtlarda argümanlar varsa bunların fiil veya yanıt kodundan hemen sonra olmaları gerekir \*ZORUNLU\*. Bazı komutlar (fiilden sonra) argüman kabul etmezler ve bazı yanıt kodlarından sonra, bazan isteğe bağlı olarak, serbest biçimli metin olabilir. Her iki durumda da, bir metin olduğunda, metin fiil veya yanıt kodundan bir boşluk karakteri ile ayrılır. Komutların ve yanıtların tanımlarının tamamını *SMTP Belirtimi* (sayfa: 22) bölümünde bulabilirsiniz.

Fiiller ve argüman değerleri (**RCPT** komutundaki "TO:" veya "to:" ve eklenti ismi anahtar sözcükleri gibi), bu belirtimdeki bir posta kutusunun *yerel-kısım* belirtimi ile ilgili biricik istisna dışında, harf büyüklüğüne duyarsızdır (SMTP Eklentileri açıkça harf büyüklüğüne duyarlı bileşenler belirtebilirler). Yani, bir komut fiili, posta kutusu *yerel-kısım*'ı hariç bir argüman değeri ve serbest biçimli metin, tamamen büyük harflerden, tamamen küçük harflerden veya her ikisinin karışımından oluşabilir \*SEÇİMLİK\* ve bu bir anlam değişikliğine yolaçmaz. Bu, bir posta kutusunun *yerel-kısım*'ını belirtirken geçerli değildir. Bir posta kutusunun *yerel-kısım*'ı harf büyüklüğüne duyarlı olmalıdır \*ZORUNLU\*. Bundan dolayı, SMTP gerçekleştirmeleri posta kutularının *yerel-kısım*'larını bu bakımdan korumaya dikkat etmelidir \*ZORUNLU\*. Posta kutusu alan'ları harf büyüklüğüne duyarlı değildir. Bazı konaklarda, bazan "smith" kullanıcısı ile "Smith" kullanıcısı farklı olabilmektedir. Bununla birlikte, posta kutusu *yerel-kısım*'larının harf duyarlılığının istismar edilmesi birlikte çalışabilirliği sekte vurmaktadır ve cesaret kırıcıdır.

Birkaç SMTP sunucusu, bu belirtime (ve RFC 821'e) aykırı olarak, komut fiillerinin istemciler tarafından büyük harflerle kodlanmasını gerektirmektedir. Gerçekleştirmeler isterlerse bu sunucuları da kapsamak için bu kodlamaya da destek verebilirler \*SEÇİMLİK\*.

Argüman alanları uzunluğu ile ilgili bir sınırlama olmayan ve satır sonlandırıcı ile yani, <CRLF> ile biten bir karakter dizisinden oluşur. Alıcının bu dizilim alınana kadar hiçbir şey yapmaması gerekir.

Her komutun sözdizimi o komutun açıklaması ile birlikte gösterilmiştir. Ortak bileşenler ve parametreler ise *Komut Argümanlarının Sözdizimi* (sayfa: 27) bölümünde gösterilmiştir.

Komutlar ve yanıtlar, ASCII karakter kümesinin [1] karakterlerinden oluşur. 8 bitlik baytlar (sekizli) kullanan bir aktarım kanalı sağlayan bir aktarım hizmetinin varlığı halinde, her 7 bitlik karakter, sekizli içinde sağa yanaştırılıp, sekizlinin yüksek biti sıfır yapılarak aktarılır. Hatta özellikle, eksiz (yalın) SMTP hizmeti sadece 7 bitlik aktarım sağlar. Belli bir sunucuya ilgili eklentiyi başarıyla müzakere edemeyen (böyle bir yeteneği olmadığı için) bir oluşturucu SMTP istemcisi, iletileri sekizlinin yüksek bitindeki bilgiyle (yüksek biti sıfırlamadan) aktarmamalıdır \*ZORUNLU\*. Böyle iletiler bu kurala aykırı olarak aktarılıyorsa, alıcı SMTP sunucuları yüksek biti temizleyebilir veya iletiyi geçersiz olduğu gerekçesiyle reddedebilir \*SEÇİMLİK\*.

Genelde, bir röle SMTP aldığı iletinin içeriğinin geçerli olduğunu varsaymalı ve zarfın bunu yapmasına izin verdiği varsayımıyla içeriğini incelemeksizin rölelemelidir \*ZORUNLU\*. Şüphesiz, eğer içerik yanlış etiketlenmişse ve veri yolu asıl içeriği kabul edemiyorsa, bu, eninde sonunda alıcıya birkaç bozuk ileti teslimatıyla sonuçlanabilir. Hiçbir SMTP sistemi zarf komutlarını US-ASCII'den farklı bir karakter kümesinde göndermeye izin vermemelidir; alıcı sistemler böyle komutları, normalde, "500 syntax error – invalid character" (sözdizimi hatası – geçersiz karakter) yanıtlarıyla reddetmelidir \*ZORUNLU\*.

Bir istemci bir sunucudan, sekiz bitlik ileti içeriğinin ek SMTP oluşumları, özellikle de "8BITMIME" eklentisi [20] kullanılarak aktarılmasını isteyebilir \*SEÇİMLİK\*. 8BITMIME, SMTP sunucuları tarafından desteklenmelidir \*ZORUNLU\*. Bununla birlikte, bu kural, sekiz bitlik malzemenin koşulsuz aktarılmasına izin varmış gibi yorumlanamaz \*ZORUNLU\*. Göndericilerin, MIME biçiminde olmayan ama uygun bir içerik aktarım kodlaması kullanılarak hazırladıkları yüksek bitli malzeme için 8BITMIME isteği yapmamaları gerekir \*ZORUNLU\*; sunucular böyle iletileri reddedebilirler \*SEÇİMLİK\*.

Bu belgede kullanılan dilötesi gösterim Genel Ağ posta sistemi belgelerinde kullanılan "Arttırımlı BNF"ye karşılıktır. Bu sözdizimine aşına olmayan okuyucuların ABNF belirtimini [8] incelemeleri iyi olur. Metin üzerinde kullanılan dilötesi terimler aralık amacıyla açılı ayraçlarla sarmalanmıştır (<CRLF> gibi).

### 3. SMTP Yordamları: Bir Bakış

Bu kısım SMTP'de kullanılan yordamların açıklamalarını içermektedir: oturum ilklendirme, posta aktarım harekâtı, postanın sevki, posta kutusu isimlerinin doğrulanması, postalama listelerinin genişletilmesi, alışverişin açılması ve kapatılması. Röleme ile ilgili açıklamalar, posta alanları üzerine bir bilgi ve değişen rollerle ilgili bir açıklama ise bu bölümün sonundadır. *Senaryolar* (sayfa: 54) bölümünde ise tam senaryo örneklerine yer verilmiştir.

#### 3.1. Oturum İlklendirme

İstemci sunucuya bir bağlantı açıp sunucu da bir karşılama iletiyle bunu yanıtladığında bir SMTP oturumu ilklendirilmiş olur.

SMTP sunucu gerçeklemleri, 220 kodundan sonraki selamlama yanıtında yazılımın ismini ve sürüm bilgilerini bulundurabilirler \*SEÇİMLİK\*. Bu, sorunları yalıtma ve çözmede daha etkin bir uygulama sağlar. Güvenlik kaygılarıyla gerçeklemler tedbirli davranarak SMTP sunucuların yazılım ve sürüm bilgisi göstermesini iptal edebilirler \*SEÇİMLİK\*. Bazı sistemler ayrıca olası posta sorunları için bir başvuru noktası tanımlasalar dahi, bu, gerekli olan "postmaster" adresinin yerine geçmez (bkz, *Asgari Gerçeklemler* (sayfa: 39)).

SMTP protokolü ilk bağlantıya izin vererek bir aktarımın usulen reddedilmesini şöyle sağlar: ilk bağlantı açılış ileti olarak 220 kodlu bir yanıt yerine 554 kodlu bir yanıt verilebilir \*SEÇİMLİK\*. Böyle bir davranışı seçen sunucu bağlantıyı kapatmadan önce yine de istemcinin bir **QUIT** komutu göndermesini beklemelidir \*ZORUNLU\* (bkz, *Çıkış (QUIT komutu)* (sayfa: 27)); bu arada gelen komutlara "503 bad sequence of commands" (komut sıralaması hatalı) yanıtını verebilir \*ÖNERİ\*. Böyle bir sisteme bir SMTP bağlantısı yapmaya çalışmak belki de bir hataya yol

açacağından, bağlantı açılışında 554 yanıtı döndüren sunucu, yanıt metninde gönderen sistemin hata ayıklama oluşturmalarına yeterli bilgiyi sağlarsa iyi olur \*ÖNERİ\*.

### 3.2. İstemci İklendirme

Sunucunun hizmete hazır olduğunu belirten iletisini göndermesi ve istemcinin de bunu almasının ardından, istemci normal olarak, kimliğini belirten bir **EHLO** komutu gönderir. **EHLO** kullanımı oturum açılışına ek olarak, istemcinin sunucuya işleyebildiği hizmet eklentilerini belirtip sunucudan desteklediği eklentilerin listesini istemesini sağlar. Posta oturumunu iklendirmede hizmet eklentilerinin belirtilmesini gerektirmeyen ve çağdaş istemcilerle hizmet eklentilerini destekleyemeyen eski SMTP sistemleri **EHLO** komutu yerine **HELO** kullanabilirler \*SEÇİMLİK\*. Sunucular **HELO** komutlarına genişletilmiş **EHLO** tarzı yanıtlar döndürmemelidir \*ZORUNLU\*. Özellikle bir bağlantı çabasında, eğer sunucu **EHLO** komutuna "command not recognized" (komut bilinmiyor) gibisinden bir yanıt döndürüyorsa, istemci son çare olarak bir **HELO** komutu gönderirse iyi olur \*ÖNERİ\*.

**EHLO** komutunda komutu gönderen konak kendini tanıtır; komutun yaptığı iş şöyle bir söylemle açıklanabilir: "Merhaba, ben falanca.alan" (**EHLO** komutuna özgü olarak ayrıca şöyle bir söylem de eklenebilir: "ve hizmet eklentisi isteklerini destekliyorum").

### 3.3. Posta Aktarım Harekâtı

SMTP posta aktarım harekâtı üç aşamada gerçekleşir. Harekat, göndericiyi tanıtan bir **MAIL** komutu ile başlar. (Genelde, **MAIL** komutu sadece hiçbir posta aktarımı olmayacağı zaman da gönderilebilir; bkz, *Komutların Sırası* (sayfa: 29).) Bunu alıcıların bilgilerini veren bir veya daha fazla **RCPT** komutu izler. Ardından da posta verisinin aktarımını başlatıp sonunda "posta sonu" veri belirteci ile aktarımı sonlandırmakla ayrıca aktarım onayını da sağlayan **DATA** komutu gelir.

Süreçteki ilk adım **MAIL** komutudur.

**MAIL FROM:** <dönüş-yolu> [ BOŞKRK <posta-parametreleri> ] <CRLF>

Bu komut SMTP alıcısına yeni bir posta aktarım harekâtının başladığını, alıcılar ve posta verisi dahil olmak üzere tüm durum tablolarını ve tamponları sıfırlamasını söyler. <dönüş-yolu> kısmı ilk, belki de tek argümandır ve hataları raporlamakta kullanılacak kaynak posta kutusunu ( "<" ve ">" arasında) içerir (hataları raporlama ile ilgili olarak *SMTP Yanıtları* (sayfa: 30) bölümüne bakınız). Eğer kabul edilirse, SMTP sunucusu bir 250 OK yanıtı gönderir. Eğer posta kutusu belirtimi bazı sebeplerle kabul edilebilir değilse, sunucu hatanın kalıcı mı yoksa geçici mi olduğunu belirten bir yanıt vermelidir \*ZORUNLU\* (kalıcı ise kalıcı olduğunu belirtmelidir ki, istemci aynı adresi tekrar denerse hatanın tekrarlanacağını bilsin; geçici ise geçici olduğunu belirtmelidir ki, istemci bir süre sonra tekrar denediğinde postanın kabul edilebileceğini bilsin). Bu gereksinimin böylesine apaçık oluşuna rağmen, dönüş yolunun kabul edilebilirliğinin bir veya daha fazla sevk yolu (**RCPT** komutlarında bulunur) incelenebilir olana kadar saptanabilir olmayacağı bazı durumlar vardır. Bu durumlarda, sunucu makul olanı yapıp dönüş yolunu (bir 250 yanıtı ile) kabul edebilir ve sevk yollarını alıp inceledikten sonra sorunu raporlayabilir \*SEÇİMLİK\*. Normalde, başarısızlık 550 ve 553 yanıtları üretir.

Tarihsel olarak, <dönüş-yolu> tek bir posta kutusundan fazlasını içerebilir, ancak, çağdaş sistemler kaynak yönlendirmesini kullanmasalar iyi olur \*ÖNERİ\* (bkz, *Kaynak Rotalar* (sayfa: 53)).

İsteğe bağlı <posta-parametreleri> uzlaşılacak SMTP hizmet eklentileri ile ilgilidir (bkz, *Eklenti Modeli* (sayfa: 7)).

Sürecin ikinci adımını **RCPT** komutu oluşturur.

**RCPT TO:** <sevk-yolu> [ BOŞKRK <alım-parametreleri> ] <CRLF>

Bu komutun ilk, belki de tek argümanı bir alıcıyı betimleyen sevk yolunu içerir (normalde, bir posta kutusu ve alan'dan oluşur ve daima "<" ile ">" arasında belirtilir). Eğer kabul edilirse, SMTP sunucusu bir 250 OK yanıtı



gönderir ve sevk yolunu bir yere kaydeder. Eğer alıcının teslimat yapılabilir bir adres olmadığı biliniyorsa, SMTP sunucusu bir 550 koduyla genellikle posta kutusu için "no such user – " (böyle bir kullanıcı yok – ...) gibisinden bir dizge içeren bir yanıt yollar (başka durumlar ve yanıt kodları mümkündür). Harekâtın bu aşaması defalarca yinelenebilir.

*<sevk-yolu>* tek bir posta kutusundan fazlasını içerebilir. Tarihsel olarak, *<sevk-yolu>* konakların ve hedef posta kutularının oluşturduğu bir kaynak yönlendirme listesi olabilir, yine de, çağdaş SMTP istemcileri kaynak rotaları dikkate almasalar daha iyi olur \*ÖNERİ\* (bkz, *Kaynak Rotalar* (sayfa: 53)). Sunucuların bir kaynak rota listesi karşılamaya hazır olmalarının gerekmesine \*ZORUNLU\* karşın, bu rotaları yoksaymaları daha iyidir \*ÖNERİ\*, hatta ifade ettikleri rölelemeyi desteklemeyi reddedebilirler \*SEÇİMLİK\*. Benzer şekilde, sunucular başka konakları ve sistemleri hedefleyen postaları kabul etmeyi reddedebilirler \*SEÇİMLİK\*. Bu kısıtlamalar bir sunucuyu, SMTP işlevselliğini tamamen desteklemeyen istemciler için bir röle olarak kullanışsız yapar. Sonuç olarak, yetenekleri kısıtlı istemciler, Genel Ağ'daki herhangi bir SMTP sunucusunu kendi posta işleme (röleleme) siteleri gibi kullanabileceklerini varsaymamalıdır \*ZORUNLU\*. Eğer bir **RCPT** komutu evveliyatında bir **MAIL** komutu olmaksızın alınmışsa, sunucunun 503 koduyla bir "Bad sequence of commands" (Komut sıralaması hatalı) yanıtı vermesi gerekir \*ZORUNLU\*. İsteğe bağlı *<alın-parametreleri>* uzlaşılacak SMTP hizmet eklentileri ile ilgilidir (bkz, *Eklenti Modeli* (sayfa: 7)).

Sürecin üçüncü adımını **DATA** komutu oluşturur (veya bir hizmet eklentisinde belirtilmiş bir eşdeğeri).

**DATA** <CRLF>

Kabul edilirse, SMTP sunucu 354 koduyla bir aracı yanıt gönderir ve tüm başarılı satırların üstesinden gelebileceğini fakat ileti metninde olası bir posta verisi sonu belirtecinin buna dahil olmadığını varsayar. Metin sonu başarılı şekilde alındığında ve kaydedildiğinde SMTP alıcısı 250 OK yanıtını gönderir.

Posta verisi aktarım kanalı üzerinden gönderildiğinden, posta verisi sonu belirtilmelidir ki, komut ve yanıt alışverişi kaldığı yerden devam edebilsin. SMTP, posta verisinin sonunu sadece tek bir nokta (".") içeren bir satır göndererek belirtir. Bunun kullanıcı metniyle etkileşime girmesini engellemek için şeffaf bir yordam kullanılır (bkz, *Şeffaflık* (sayfa: 40)).

Posta verisi sonu belirteci ayrıca posta aktarımının onaylanması anlamına gelir ve SMTP sunucusuna kayıtlı alıcıları ve posta verisini artık işleme sokmasını söyler. Kabul edilirse, SMTP sunucu bir 250 OK yanıtı gönderir.

**DATA** komutu protokol alışverişinde sadece iki noktada başarısız olabilir:

- Ne **MAIL** ne de **RCPT** komutu varsa veya böyle tüm komutlar reddedilmişse, sunucu **DATA** komutuna yanıt olarak 503 koduyla bir "command out of sequence" (komut sıra dışı) veya 554 koduyla bir "no valid recipients" (alıcılar geçersiz) yanıtı gönderebilir \*SEÇİMLİK\*. Bu yanıtlardan biri (veya 5yz kodlu başka bir yanıt) alındığında, istemcinin ileti verisini göndermemesi gerekir \*ZORUNLU\*; daha genel olarak, ileti verisi bir 354 yanıtı alınmadıkça gönderilmemelidir \*ZORUNLU\*.
- Eğer fiil baştan kabul edilmiş ve 354 yanıtı verilmişse, **DATA** komutu sadece, posta aktarımı tamamlanmamışsa (örn, alıcılar yoktur) veya özkaynaklar kullanımdışıysa (sunucunun beklenmedik şekilde kullanımdışı kalmasını da dahil ederek) ya da iletinin kural ihlali veya başka bir sebeple reddedildiği sunucu tarafından saptanmışsa başarısız sayılır.

Bununla birlikte, bazı sunucular uygulamada, ileti metni alınana kadar alıcı varlık doğrulaması yapmaya çalışmazlar. Bu sunucular bir veya daha fazla alıcı için bir başarısızlığı bir "ardçıl başarısızlık" olarak ele almaları ve *Sorun Saptama ve Giderme* (sayfa: 45) bölümünde açıklandığı gibi bir posta iletisi göndermeleri daha iyi olur \*ÖNERİ\*. "550 mailbox not found" (posta kutusu yok) veya eşdeğeri bir yanıt kodunun veri kabul edildikten sonra kullanımı, istemci açısından hangi alıcının başarısız olduğunun saptanmasını zor hatta imkansız hale getirir.

RFC 822 biçimi [7, 32] kullanıldığında, posta verisi bilgi neviinden *Date*, *Subject*, *To*, *Cc*, *From* gibi başlık öğeleri içerir. Sunucu SMTP sistemleri, RFC 822 veya MIME [12] ileti başlığı veya ileti gövdesin-

deki farkedilir kusurlara dayalı iletileri reddetmeseler iyi olur \*ÖNERİ\*. Özellikle, `Resent-fields` sayısının uyuşmadığı veya `Resent-to`'nun `Resent-from` ve/veya `Resent-date` olmaksızın görüldüğü iletileri reddetmemeleri gerekir \*ZORUNLU\*.

Posta aktarım harekâtı komutları yukarıdaki sırasıyla kullanılmalıdır \*ZORUNLU\*.

### 3.4. Adres Düzeltmek veya Güncellemek için Yönlendirme

Yönlendirme desteği en sık adresleri bir girişime göreli olarak veya onunla birleştirmek ve basitleştirmek için ve daha az sıklıkla bir şahsın eski bir adresiyle yeni bir adresi arasında bağ kurmak için gerekir. İletilerin sessizce yönlendirilmesi (sunucu tarafından gönderici bilgilendirilmeyerek), güvenlik veya ifşa etmeme kaygılarıyla günümüzde çok kullanılan bir Genel Ağ uygulamasıdır.

Hem girişim hem de "yeni adres" durumlarında, bilgi gizleme (ve bazan güvenlik) kaygısı, yönlendirme işleminin bir yan etkisi olarak SMTP üzerinden "son" adresin ifşasıyla kendini gösterir. Bu özellikle son adresin gönderici tarafından yine de erişilebilir olmadığı zaman önemli olur. Bu sebepten, RFC 821'in 3.2 numaralı bölümünde açıklanan "sevk" mekanizması ve özellikle **RCPT** komutuna verilen 251 (düzeltilmiş hedef) ve 551 yanıt kodları gerçeklenimciler ve sistemleri yapılandıranlar tarafından dikkatle değerlendirilmelidir.

#### Özellikle:

- Sunucular adres değişikliğinden haberdar olduklarında iletileri yönlendirebilirler \*SEÇİMLİK\*. Bunu yaparken, bir 251 koduyla adres güncelleme bilgisi sağlayabilecekleri gibi iletiyi "sessizce" yönlendirip bir 250 kodu gönderebilirler \*SEÇİMLİK\*. Fakat, eğer bir 251 kodu kullanılmışsa, istemcinin adres bilgisini güncelleyeceği hatta bunu kullanıcıya bildireceği varsayılmamalıdır \*ZORUNLU\*.

#### Diğer yandan,

- İletiler adreslerine teslim edilemiyorsa sunucular bunları reddedebilir veya geri gönderebilir \*SEÇİMLİK\*. Sunucular bunu yaparken, bir 551 koduyla adres güncelleme bilgisi sağlayabilecekleri gibi bir 550 koduyla teslim edilemediği gerekçesiyle iletiyi reddedebilirler \*SEÇİMLİK\*. Fakat, eğer bir 551 kodu kullanılmışsa, istemcinin adres bilgisini güncelleyeceği hatta bunu kullanıcıya bildireceği varsayılmamalıdır \*ZORUNLU\*.

251 ve/veya 551 yanıt kodlarını destekleyen SMTP sunucu gerçeklenimleri, istenmeyen biçimde bilgi ifşa ettiği sonucuna varılan siteleri iptal edilebilmek veya kullanımlarını kısıtlayabilmek için yapılandırma mekanizmaları sağlamak konusunda hararetle özendirilirler.

### 3.5. Adres Hatalarını Ayıklama Komutları

#### 3.5.1. Genel Bakış

SMTP kullanıcı adını doğrulamak ve posta listesi içeriğini elde etmek için komutlar da sağlar. Bunu karakter dizisi argümanlar alan **VERFY** ve **EXPN** komutları ile yapar. Gerçeklenimler **VERFY** ve **EXPN** komutlarını desteklerlerse iyi olur \*ÖNERİ\* (yine de, *VERFY için Normal Yanıt* (sayfa: 18) ve *VERFY, EXPN ve Güvenlik* (sayfa: 48) bölümlerine bakınız).

**VERFY** komutu için dizge bir kullanıcı ismi veya bir kullanıcı ismi ve alandır (aşağıya bakınız). Eğer normal bir yanıt (250 gibi) geliyorsa, yanıt kullanıcının posta kutusunu içermek zorundayken \*ZORUNLU\* kullanıcının tam ismini de içerebilir \*SEÇİMLİK\*. Dizge şu biçimlerden biri olmalıdır \*ZORUNLU\*:

```
Kullanıcının Adı ve Soyadı <yerel-kısım@alan>
yerel-kısım@alan
```



**VRFY** komutunun argümanı olan isim birden fazla posta kutusunu betimleyebildiği takdirde, sunucu ya belirsizliğe dikkat çeker ya da başka olasılıklar belirtir \*SEÇİMLİK\*. Başka bir deyişle, **VRFY** komutunun meşru yanıtı şunlardan birinin benzeri olabilir:

```
553 User ambiguous // 553 Kullanıcı belirsiz
```

veya

```
553- Ambiguous; Possibilities are // 553- Belirsizlik; Olasılıklar:
553-Joe Smith <jsmith@foo.com>
553-Harry Smith <hsmith@foo.com>
553 Melvin Smith <dweep@foo.com>
```

ya da

```
553-Ambiguous; Possibilities
553- <jsmith@foo.com>
553- <hsmith@foo.com>
553 <dweep@foo.com>
```

Normal şartlar altında, bir 553 yanıtı alan bir istemcinin kullanıcıya sonucu açıklamaması beklenir. Tam olarak belirtilen biçimlerin ve [34]'te açıklandığı gibi ek yanıt kodları tarafından ilave olarak "user ambiguous" veya "ambiguous" anahtar sözcüklerinin olası kullanımı, gerektiğinde diğer dillere özdevinimli çeviriyi kolaylaştıracaktır. Şüphesiz, oldukça özdevinimli hale getirilmiş ya da İngilizce'den farklı bir dilde işlem yapan bir istemci, yanıtın içerdiği metni olduğu gibi kullanıcıya yansıtmak yerine yanıtı tercüme etmeyi veya kullanıcıya durumu raporlamadan önce ek bilgi için bir sözlük hizmetine başvurulması gibi özdevinimli eylemlerden birini yapmayı tercih ederdi.

**EXPN** komutu için dizge bir postalama listesidir ve başarılı (250 gibi) bir çok satırlı yanıt postalama listesindeki posta kutularının listesini içermeli \*ZORUNLU\* iken, bu liste kullanıcılarının ad ve soyadlarını da içerebilir \*SEÇİMLİK\*.

Bazı konaklarda, bir posta kutusu ile tek bir posta kutusunun rumuzu arasındaki fark, her iki girdi türü için ortak bir veri yapısı kullanıldığından, bulanıktır ve sadece tek bir posta kutusu içeren postalama listelerinin varlığı olasıdır. Bir postalama listesine **VRFY** uygulayacak bir istek yapılmışsa, iletinin listedeki herkese teslimi şeklinde adreslenmiş olması durumunda bir olumlu yanıt verilebilir \*SEÇİMLİK\*, aksi takdirde bir hata raporlanırsa iyi olur \*ÖNERİ\* ("550 bu bir postalama listesi adresidir, bir kullanıcı adresi değildir" veya "252 Posta listesi üyelerini doğrulamaya izin verilmiyor" gibi bir hata raporu). Eğer bir kullanıcı ismini açan bir istek yapılmışsa tek bir isim içeren bir listeden oluşan olumlu bir yanıt verilebileceği gibi bir hata da raporlanabilir \*SEÇİMLİK\* ("550 bu bir kullanıcı adresidir, bir postalama listesi adresi değildir" gibi bir hata raporu).

Başarılı bir çok satırlı cevap (**EXPN** için normal olan) durumunda yanıtın her satırında tam olarak bir posta kutusu belirtilir. Belirsiz bir istek yapılması durumundan yukarıda bahsedilmişti.

"Kullanıcı adı" bulanık bir terimdir ve tedbirli kullanılmıştır. **VRFY** veya **EXPN** komutlarının gerçekleşimi en azından "kullanıcı adları" olarak yerel posta kutularını tanımayı içermelidir \*ZORUNLU\*. Şu an ki Genel Ağ uygulaması sıklıkla çok sayıda alanın postasıyla tek bir konağın ilgilenmesi sonucunu doğurduğundan, konaklar, özellikle de bu işlevselliği sağlayan konakların, bir "kullanıcı ismi" olarak "yerel-kısım@alan" biçimini kabul etmeleri iyi olur \*ÖNERİ\*; bu konaklar ek olarak "kullanıcı isimleri" olarak başka dizgeleri tanımayı tercih edebilirler \*SEÇİMLİK\*.

Bir çok satırlı yanıt gerektiren bir posta kutusu listesinin açılımı durumu şöyle örneklenebilir:

```
i: EXPN Numune-Topluluk
S: 250-Jon Postel <Postel@isi.edu>
S: 250-Fred Fonebone <Fonebone@physics.foo-u.edu>
```

```
S: 250 Sam Q. Smith <SQSmith@ozellikle.genel.com>
```

veya

```
I: EXPN imtiyaz-sevenler-listesi
S: 550 Size Erisim Yasak.
```

**VRFY** ve **EXPN** komutlarının karakter dizisi argümanları kullanıcı adı ve posta kutusu listesi kavramlarının gerçeklenimlerinin çeşitliliğine bağlı olarak daha fazla kısıtlanamaz. Bazı sistemlerde **EXPN** komutunun argümanı bir postalama listesi içeren bir dosyanın adı olabilir, ama tekrar belirtelim ki, Genel Ağ'da dosya isimlendirme uzlaşımları çeşitliliği vardır. Bu komutlardaki tarihsel farklılıklar nedeniyle elde edilen sonuçlar çok dikkatli yorumlanmalı \*ÖNERİ\* ve sadece sorun teşhisi için kullanılmalıdır \*ÖNERİ\*.

### 3.5.2. **VRFY** için Normal Yanıt

Bir **VRFY** veya **EXPN** isteğinden normal yanıt (2yz veya 551) döndüğünde, yanıt normal olarak "<yerel-kısım@alan>" gibi bir posta kutusu ismi içerir; burada "alan" tamamen nitelikli alan adı olup sözdizimi içinde görünmelidir \*ZORUNLU\*. Bu belirtimin niyetine karşı çıkmayı haklı gösterecek kadar olağanüstü durumlarda, serbest biçimli metin döndürülebilir \*SEÇİMLİK\*. Hem bilgisayarlar hem de insanlar tarafından çözümlemeyi kolaylaştırmak için adresler "<" ve ">" arasında olmalıdır \*ÖNERİ\*. Serbest biçimli hata ayıklama bilgisi değil de adresler döndürüldüğünde, **EXPN** ve **VRFY** komutları sadece SMTP **RCPT** komutlarında kullanılabilen geçerli alan adreslerini döndürmelidir \*ZORUNLU\*. Bu sebepten, eğer bir adres, teslimatın bir programa veya başka bir sisteme yapılacağı anlamına gelecekse, bu hedefe erişmekte kullanılan posta kutusu ismi belirtilmelidir \*ZORUNLU\*. Yollar (açıkça kaynak rotaları) **EXPN** veya **VRFY** komutundan döndürülmemelidir \*ZORUNLU\*.

Sunucu gerçeklenimleri **VRFY** ve **EXPN** komutlarının ikisine de destek vermelidir \*ÖNERİ\*. Güvenlik kaygılarıyla, gerçeklenimler, yapılandırma seçenekleri veya eşdeğerleri üzerinden bu komutların biri veya her ikisinin de iptal edilebileceği yerel kurulumları sağlayabilirler \*SEÇİMLİK\*. Bu komutlar desteklendiğinde, rôle desteği de varsa, bu komutların rôlelele çalışmaları gerekli değildir. RFC 821'de bunların her ikisi de seçimli olduğundan, eğer destekleniyorsa, bir **EHLO** yanıtında hizmet eklentileri olarak listelenmeleri gerekir \*ZORUNLU\*.

### 3.5.3. **VRFY** veya **EXPN** için Başarılı Yanıtın Anlamı

Bir sunucu, adresi gerçekten doğrulamadıkça, bir **VRFY** veya **EXPN** komutuna yanıt olarak bir 250 kodu döndürmemelidir \*ZORUNLU\*. Bilhassa, sunucunun yaptığı tek iş verilen sözdiziminin geçerliliğini doğrulamaksa bir 250 kodu döndürmemelidir \*ZORUNLU\*. Bu durumda, 502 (Komut gerçekleşmedi) veya 500 kodu (Sözdizimi hatası, komut anlaşılamadı) döndürmelidir \*ÖNERİ\*. Başka bir yerde de belirtildiği gibi, **VRFY** ve **EXPN** gerçeklenimi (adreslerin gerçekten doğrulanması ve bilgi döndürülmesi anlamında) hararetle önerilmektedir. Bu sebepten, **VRFY** için 500 veya 502 döndüren gerçeklenimler bu belirtimle tam uyumlu değildir.

Özellikle bir sunucunun, bir alan ya da başka bir sunucu için posta aktarımcı olarak çalıştığı durumda bir adresin doğru gibi görüldüğü ama gerçekte sebepsizce doğrulanmadığı durumlar olabilir. Bu durumdaki "Görünen Doğruluk" normalde en azınan sözdizimi denetimi özelliğini ve kimi zaman, belirtilen alanların postayı röleleleyebileceği umulan konaklar olduklarını doğrulayabilme özelliğini ihtiva eder. Bu durumlarda, 252 yanıt kodu döndürülmelidir \*ÖNERİ\*. Bu durumlar *Temel Yapı* (sayfa: 6) bölümünde bahsedilen **RCPT** doğrulama konusuyla paraleldir. Benzer olarak, *Adres Düzeltmek veya Güncellemek için Yönlendirme* (sayfa: 16) bölümünde bahsedilen uygulama, adreslerin tanındığını ama onlar için alınan postanın sevkedildiğini veya geri gönderildiğini belirten **VRFY** (ve **EXPN**) komutlu 251 ve 551 yanıt kodlarına uygulanır. Gerçeklenimler genelde biraz daha uzun sürecek olsa bile **VRFY** durumunda adres doğrulama ile ilgili olarak **RCPT** durumuna oranla daha fazla girişken olmalıdırlar \*ÖNERİ\*.

### 3.5.4. **EXPN** Uygulamaları ve Anlamsallık

**EXPN** komutu çoğunlukla postalama listeleri ve çok sayıda hedef adresi belirten rumuzlarla ilgili sorunların anlaşılması ve hatalarının ayıklanması için çok yararlıdır. Bazı sistemler yinelenenleri ayıklamak için posta listelerinin kaynak yorumlamasını kullanmayı denediler. Rumuzlama sistemlerinin Genel Ağ'da posta ile etkileşimi, bu stratejilerin konaklar (genelde **MX** ve **CNAME** DNS kayıtları), posta kutuları (yerel konak rumuzlarının çeşitli türleri) ve çeşitli vekil düzenlemeleri açısından tutarlı çalışmasını neredeyse imkansız hale getirmiştir ve posta sistemleri bunlara yeltenmemelidir \*ÖNERİ\*.

### 3.6. Alanlar

Alan isimleri SMTP'de kullanılacaksa sadece çözümlenebilir ve tamamen nitelenmiş alan isimlerine (FQDN'ler) izin verilir. Başka bir deyişle, sonuçta **MX** veya **A** kayıtları olarak çözümlenebilen **CNAME** kayıtlarında olduğu gibi, **MX** veya **A** kaydına çözümlenebilen isimlere (*Adres Çözümleme ve Posta Yönetimi* (sayfa: 44) bölümünde açıklandığı gibi) izin verilir. Yerel takma adlar ve niteliksiz isimler kullanılmamalıdır \*ZORUNLU\*. FQDN gerekliliği kuralının iki istisnası vardır:

- **EHLO** komutunda verilen alan ismi ya bir birincil konak ismi (bir **A** kaydı olarak çözümlenen alan ismi) ya da konak isimsizse *Ayrıntılı Selamlama (EHLO) veya Sade Selamlama (HELO)* (sayfa: 23) bölümünde belirtildiği gibi bir adres sabiti olmalıdır \*ZORUNLU\*.
- Bir **RCPT** komutunda alan belirtmeksizin ayrılmış posta kutusu isimlerinden "postmaster" kullanılabilir ve böyle kullanılırsa kabul edilmek zorundadır \*ZORUNLU\*.

### 3.7. Röleleme

Genelde, alan adı sistemindeki [22, 27] posta aktarımcı (**MX**) kayıtlarının varlığı, Genel Ağ posta sisteminde doğrudan kaynak rotası kullanımını gereksiz kılar. Geçmişte yorumlanmalarıyla ilgili yaşanan bir çok sorun kullanımlarının istenmemesine yol açtı. Olağanüstü durumlar müstesna, SMTP istemcileri doğrudan kaynak rotaları üretmemelidir \*ÖNERİ\*. SMTP sunucuları kaynak rotası belirten adresleri kabul etmeyi veya posta rölesi olarak davranmayı reddedebilirler \*SEÇİMLİK\*. Rota bilgisinin mevcudiyeti saptandığında SMTP sunucuların rota bilgisini yoksayma hakkı vardır ve basitçe, postayı rotada son eleman olarak belirtilmiş son varış noktasına gönderebilirler ve böyle de yapmalıdırlar \*ÖNERİ\*. Kaynak rotada ara konaklar olarak belirtilmiş konaklardaki kullanıcıların sorunlarını çözmekle ilgili olarak, DNS'lerde varış noktası olarak görünmeyen isim kullanımı ile ilgili geçersiz bir uygulama olmuştur. Kaynak rotalardaki ara konaklar yoksayıldığında bu uygulama hatalara yolaçar. Bu, SMTP istemcilerinin neden geçersiz kaynak rotaları veya seriye çözünür isimler üretmemeleri gerektiğinin \*ZORUNLU\* sebeplerinden biridir.

Kaynak rotaları kullanılmadığında, RFC 821'de açıklanan, sevk yolundan bir dönüş yolu oluşturmaya yarayan işlem uygulanabilir değildir ve dönüş yolu, teslim anında basitçe **MAIL** komutunda görünen adrestir.

Bir röle SMTP sunucusu genelde son teslim sisteminden ziyade kendisini işaret eden DNS **MX** kaydının hedefidir. Röle SMTP sunucusu röleleme işini yerel bir kullanıcının postasını kabul veya red ettiği şekilde kabul veya red edebilir. Rölelemeyi kabul ederse bir SMTP istemcisi haline gelir, DNS'de belirtilen sıradaki SMTP sunucuya bir aktarım kanalı oluşturur (*Adres Çözümleme ve Posta Yönetimi* (sayfa: 44) bölümündeki kurallar dahilinde) ve postayı ona yollar. Kurallar gereği belli bir adrese postayı rölelemeyi redderse, geriye bir 550 yanıtı göndermelidir \*ÖNERİ\*.

Birçok posta gönderme istemcisi vardır ve bunlar genellikle POP3 veya IMAP üzerinden posta da alabilmekte olup bu belirtimdeki gereksinimlerin bazılarını (peşpeşe teslimat gerektiğinde iletileri kuyruğa almak gibi) sınırlı olarak desteklemektedirler. Bu istemciler için bilinen uygulama, işleme sokulmak veya ardışık olarak dağıtılmak üzere tüm iletileri tek bir sunucuya gönderecek düzenlemeleri yapmaktır. Burada belirtildiği gibi SMTP bu role uygun değildir ve bu iş mevcut uygulamalar için standart hale gelmiş posta teslim etme protokolleri ile fevkalade

yoluna girmiş durumdadır. Her halükarda, bu düzenlemeler bu uygulamalara özeldir ve bu belirtimin kapsamına girmediklerinden burada açıklanmayacaklardır.

Bir konu önemlidir: **MX** kayıtları, sadece SMTP rölelerini ve son teslimat sistemlerini değil, başka ortamlara ağgeçidi rolü oynayan SMTP sunucularını da işaret edebilir; *Postanın Ağgeçitlerinden Geçirilmesi* (sayfa: 20) ve *Adres Çözümleme ve Posta Yönetimi* (sayfa: 44) bölümlerine bakınız.

Bir SMTP sunucusu posta röleleme görevini kabul eder ve daha sonra hedefin yanlış olduğunu veya herhangi bir sebepten dolayı posta teslimatının yapılamadığını görürse, bir "teslimatı yapılamayan posta" uyarısı iletisi oluşturmalı ve bunu o postayı oluşturana (geri dönüş yolunda belirtilene) göndermelidir. Teslimatı yapılamayan postalarla ilgili raporlar için başka standartlar (örn, [24, 25]) tarafından belirtilmiş biçimler mümkün olduğunca kullanılmalıdır **\*ÖNERİ\***.

Bu uyarı iletisi röle konağındaki veya teslimatın gerçekleşmediğinin ilk olarak saptandığı konaktaki SMTP sunucusundan gelmelidir. Şüphesiz, SMTP sunucuları bir de uyarı iletilerinin teslimat sorunlarıyla ilgili uyarı iletileri göndermemelidirler **\*ZORUNLU\***. Hata raporlarken kısır döngüleri engellemenin bir yolu, bir uyarı iletilisinin **MAIL** komutunda boş geri dönüş yolu belirtmektir. Böyle bir ileti aktarılırken, dönüş yolu boş bırakılmalıdır **\*ZORUNLU\*** (ek bilgi için bkz, *Dönüş yolu boş olan iletiler* (sayfa: 44)). Boş geri dönüş yolu içeren bir **MAIL** komutu:

**MAIL FROM:** <>

*Düzensizliklerin Giderilmesi* (sayfa: 46)<sup>(1)</sup> bölümünde bahsedildiği gibi, bir röle SMTP kendi "Received:" başlığını eklemek dışında, ileti gövdesini veya başlıklarını inceleme veya işlemi sokma gereği duymamalıdır **\*ZORUNLU\*** ve posta sistemindeki kısır döngüyü saptamaya çalışmamalıdır **\*SEÇİMLİK\*** (bkz, *Döngü Algılama* (sayfa: 46)).

### 3.8. Postanın Ağgeçitlerinden Geçirilmesi

Yukarıda bahsedilen röleleme işlevi Genel Ağ SMTP aktarım hizmeti ortamında işlemlerini yaparken, **MX** kayıtları ve doğrudan yönlendirmenin çeşitli şekillerinin varlığı bir aktarım hizmetinden diğerine bir dönüşüm işlevi yapacak bir ara SMTP sunucusu gerektirebilir. *Oluşturucu, Teslimatçı, Röle ve Ağgeçidi Sistemler* (sayfa: 11) bölümünde açıklandığı gibi, böyle bir sistem iki aktarım hizmeti ortamına sınır olduğunda, bu sistemi bir "ağgeçidi" veya bir "ağgeçidi SMTP" olarak niteleriz.

Farklı posta biçimleri ve protokolleri gibi farklı posta ortamları arasındaki ağgeçitlerinden posta aktarımı karmaşık bir işlemdir ve kolayca standartlaşmaz. Yine de, Genel Ağ ile diğer posta ortamları arasındaki ağgeçitleri için bazı genel gereksinimler belirtilebilir.

#### 3.8.1. Ağgeçitlerinden Geçişte Başlık Alanları

İletilerin posta ortamının sınırlarından geçirilmesi gerektiğinde posta başlıkları yeniden yazılabilir **\*SEÇİMLİK\***. Buna, *Düzensizliklerin Giderilmesi* (sayfa: 46)<sup>(1)</sup> bölümündeki yasaklamalara karşın, varış adresinin yerel-kısım'ının yorumlanması veya ileti gövdesinin incelenmesi de dahil edilebilir.

Genel Ağ'a ağgeçitliği yapan diğer posta sistemleri çoğunlukla, bir kısım RFC 822 başlığını veya benzer işlevselliği farklı bir sözdizimiyle sağlayan başlıkları kullanırlar, fakat bu posta sistemlerinin bazıları SMTP zarfına eşdeğerliği tutturamazlar. Onun için, bir ileti Genel Ağ ortamını terkettiğinde SMTP zarf bilgisini ileti başlığına sarmak gerekli olabilir. Olası çözüm, zarf bilgisini taşıyacak yeni başlık alanları ("**X-SMTP-MAIL:**" ve "**X-SMTP-RCPT:**" gibi) oluşturmak olurdu; ancak bu, yabancı ortamlarda posta programlarında değişikliği gerektirebilir ve özel bilgilerin ifşa edilmesi riski ortaya çıkabilir (bkz, *"Gizli" Kopyalar* (sayfa: 48)).

#### 3.8.2. Ağgeçitlerinden Geçişte Alınan Satırlar

Bir ileti Genel Ağ ortamının içine veya dışına sevk edilirken bir ağgeçidi bir **Received:** satırı hazırlamalı **\*ZORUNLU\***, fakat başlıkta zaten mevcut olan bir **Received:** satırında değişiklik yapmamalıdır **\*ZORUNLU\***.

Başka ortamlarda oluşturulan iletilerin **Received:** alanları bu belirtme tam olarak uyumlu olmayabilir. Bununla birlikte, **Received:** satırlarının en önemli kullanım alanı posta hataları ayıklamakla ilgilidir ve bu ayıklama bir **Received:** satırını "düzeltmeye" çalışan iyi niyetli ağgeçitleri tarafından ciddiye güçleştirilebilir. İzleme alanlarının SMTP dışı ortamlarda baş göstermesinin diğer bir sonucu olarak, alıcı sistemler postayı bir izleme alanının biçimine bağlı olarak reddetmemeli **\*ZORUNLU\*** ve bu alanların beklenmedik biçimleri ve bilgileri (ışığı) altında (bile) oldukça sağlam durmalıdır **\*ÖNERİ\***.

Bir ağgeçidi, **Received:** alanlarında kaynaklandığı ortamı ve protokolü "via" sözcüğü ile işaret etmelidir **\*ÖNERİ\***.

### 3.8.3. Ağgeçitlerinden Geçişte Adresler

Genel Ağ tarafından bakıldığında, bir ağgeçidi, SMTP komutlarındaki ve RFC 822 başlıklarındaki tüm geçerli adresleri ve tüm geçerli RFC 822 iletilerini kabul etmelidir **\*ÖNERİ\***. Ağgeçitleri tarafından üretilen adresler ve başlıklar uygulanabilir Genel Ağ standartlarına (bu ve RFC 822 dahil) uygun olmalıdır **\*ZORUNLU\***. Şüphesiz ağgeçitleri ayrıca, *Posta Aktarım Harekâtı* (sayfa: 14) bölümünde diğer SMTP sistemleri için açıklandığı gibi kaynak rotalarına uygulanan kuralların da konusu olur.

### 3.8.4. Ağgeçitlerinden Geçişte Diğer Başlık Alanları

Bir ağgeçidi, Genel Ağ posta ortamına sevkettiği bir iletinin tüm başlık alanlarının Genel Ağ postasının gereksinimlerini karşılamalıdır **\*ZORUNLU\***. Özellikle "From:", "To:", "Cc:", vb. alanlarındaki tüm adresler (gerekliyse) RFC 822 sözdizimine uyacak şekilde dönüştürülmeli **\*ZORUNLU\***, sadece tamamen nitelenmiş alan adlarına atıf yapmalı **\*ZORUNLU\*** ve yanıtların gönderimi için etkin ve kullanışlı olmalıdır **\*ZORUNLU\***. Postayı, Genel Ağ protokollerinden diğer ortamların protokollerine dönüştürmekte kullanılacak çeviri algoritması, yabancı posta ortamından gelen hata iletilerinin, bir RFC 822 iletilisinin **From:** alanında (veya diğer alanlarda) görülen göndericiye değil, SMTP zarfındaki dönüş yoluna teslimini sağlamalıdır **\*ÖNERİ\***.

### 3.8.5. Ağgeçitlerinden Geçişte Zarflar

Aynı şekilde, bir iletiyi başka bir ortamdan Genel Ağ ortamına sevk ederken, bir ağgeçidi, bir hata iletilisinin dönüş adresi ile ilgili zarf dönüş yolunu (eğer yabancı ortam bunu sağlamışsa) ayarlamalıdır **\*ÖNERİ\***. Eğer yabancı ortam için böyle bir şey söz konusu değilse, ağgeçidi iletinin oluşturucusunun adresi için son çare olarak en uygun olan seçip bunu kullanmalıdır.

## 3.9. Oturumların ve Bağlantıların Sonlandırılması

Bir SMTP bağlantısı, istemci bir **QUIT** komutu gönderdiğinde sonlandırılır. Sunucu bir olumlu yanıt kodu gönderdikten sonra bağlantıyı kapatır.

Şu durumlar dışında bir SMTP sunucusu bağlantıyı kasten kapatmamalıdır **\*ZORUNLU\***:

- Bir **QUIT** komutu aldıktan sonra bir 221 koduyla yanıtlayarak.
- SMTP hizmetinin kapatılmasını gereksinimi ortaya çıktığında bir 421 kodu döndürerek. Bu yanıt kodu sunucunun aldığı herhangi bir komuttan sonra ya da gerekliyse komutun alınış anından bağımsız olarak (istemcinin yanıtı sıradaki komutu gönderdikten sonra alacağı varsayımıyla) gönderilebilir.

Özellikle, anlamadığı komutlara yanıt olarak bağlantılarını kapatan bir sunucu bu belirtimle çelişkiye düşüyor demektir. Sunucuların bilinmeyen komutlara hoşgörülü davranması, istemciye 500 yanıtı gönderip istemciden talimatları beklemesi umulur.

Dış zorlamalarla kapatılmaya çalışılan bir SMTP sunucusu çıkmadan önce SMTP istemcisine bir 421 yanıt kodu içeren bir satırı göndermeye çalışmalıdır \*ÖNERİ\*. SMTP istemcisi ise, normalde 421 yanıt kodunu sıradaki komutu gönderdikten sonra okuyacaktır.

Bir bağlantı kapanması, sıfırlama veya denetimleri dışında gerçekleşen bağlantı hatalarıyla karşılaşan SMTP istemcileri, posta aktarımını bir 451 yanıtı almış da ona uygun davranıyormuş gibi ele alarak, posta sisteminin sağlam kalmasını sağlamalıdır \*ÖNERİ\*.

### 3.10. Postalama Listeleri ve Rumuzlar

SMTP yapabilen bir konak hem takma adları hem de çoklu teslimat için adres listesi modellerini yorumlamayı desteklemelidir \*ÖNERİ\*. Bir ileti liste şeklinde genişletilmiş adreslere sevk veya teslim edilirken, zarftaki dönüş adresi ("**MAIL FROM:**" adresi) listeyi yöneten kişinin ya da her neyse onun adresi olacak şekilde değiştirilmelidir \*ZORUNLU\*. Bu durumda yine de ileti başlığı [32] değişmeden kalmalı, özellikle de ileti başlığının "**From**" alanı etkilenmemelidir \*ZORUNLU\*.

Önemli posta oluşumlarından biri tek bir iletinin çok sayıda posta kutusuna teslim edilmesi mekanizmasıdır. Bu mekanizma, bir sözde posta kutusu adresini hedef posta kutusu adresleri listesine dönüştürerek (veya "yıkarak" ya da "genişleterek") çalışır. Bir ileti böyle bir sözde posta kutusuna (buna bazan "exploder" \_yıkıcı\_ da denirmiş) gönderildiğinde, iletinin kopyaları genişletilen listedeki posta kutularına sevk edilir veya yeniden dağıtılır. Sunucuların listedeki adreslerden basitçe yararlanmaları gerekir \*ÖNERİ\*; iletinin oluşturucusu gibi bazı adresleri eleyecek eşleştirme kurallarına veya ampirik uygulamalara kesinlikle engel olunmalıdır. Nasıl yorumlandıklarına bağlı olarak bu sözde posta kutularını "takma adar" ve "listeler" şeklinde sınıflandırıyoruz.

#### 3.10.1. Takma Adlar

Bir takma adın yorumlanmasında sonuç olarak, iletiyi alan postacı zarftaki sözde posta kutusu adresini basitçe tek tek adreslerle değiştirerek genişletir; zarfın ve ileti gövdesinin kalanı değişmeden kalır. Bundan sonra ileti bu adreslere sevk edilir veya teslim edilir.

#### 3.10.2. Listeler

Bir postalama listesinin sevk etmekten çok tekrar dağıtma işi yaptığı söylenebilir. Bir listeye genişletmek için iletiyi alan postacı zarftaki sözde posta kutusu adresini liste üyelerinin adreslerine değiştirir. Son teslimatlarla ilgili dönecek hata iletileri için zarftaki dönüş adresi ise, genelde liste içeriğiyle, yönetimiyle ve hata iletileriyle zerre kadar ilgisi olmayan ileti oluşturucusu değil liste yöneticisi olarak belirtilir.

## 4. SMTP Belirtimi

### 4.1. SMTP Komutları

#### 4.1.1. Komut Sözdizimi ve Anlamlandırma

Posta aktarımı veya kullanıcı tarafından talep edilen posta sistemi işlevi SMTP komutlarından, SMTP komutları, `<CRLF>` ile sonlandırılmış karakter dizilerinden oluşur. Komutların kendileri ise ardından parametreler geliyorsa `<BOŞKRK>` ile yoksa `<CRLF>` ile sonlandırılmış alfabetik karakterlerden oluşur. (Birlikte çalışabilirlik uğruna, SMTP alıcıları sonlandırıcı `<CRLF>` öncesinde boşluk karakterliğinin varlığına müsamaha göstermişlerdir.) Bir posta kutusunun yerel kısmının sözdizimi alıcı site uzlaşımlarına ve *Komut Argümanlarının Sözdizimi* (sayfa: 27) bölümünde belirtilen sözdizimine uygun olmalıdır. SMTP komutlarından aşağıda bahsedilmiştir. SMTP yanıtlarından ise *SMTP Yanıtları* (sayfa: 30) bölümünde bahsedilmiştir.



Bir posta hareketi farklı komutların argümanları olarak iletişimi sağlayan çeşitli veri nesnelerinden oluşur. Dönüş yolu **MAIL** komutunun argümanı, sevk yolu **RCPT** komutunun, posta verisi ise **DATA** komutunun argümanıdır. Bu argümanlar veya veri nesneleri, hareketi sonlandıran posta verisi sonu belirteci ile anlaşılan onayı aktarmalı ve saklamalıdır. Bunun için model, veri nesnelerinin her türü için ayrı birer tampon bulundurmaktır. Yani, dönüş yolu için bir tampon, sevk yolu için bir tampon ve posta verisi için bir tampon vardır. Belli tamponlara bilgi eklenmesine veya bir veya daha fazla tamponun temizlenmesine sebep olan belli komutlar vardır.

Bazı komutlar (**RSET**, **DATA**, **QUIT**) parametre almayacak şekilde belirtilmiştir. Sunucu tarafından sunulup istemci tarafından kabul edilen belli eklentilerin yokluğunda, istemcilerin böyle parametreler göndermemesi gerekir **\*ZORUNLU\*** ve sunucuların da geçersiz sözdizimine sahip oldukları gerekçesiyle bu komutları reddetmesi gerekir **\*ÖNERİ\***.

#### 4.1.1.1. Ayrıntılı Selamlama (**EHLO**) veya Sade Selamlama (**HELO**)

Bu komutlar, SMTP sunucusuna SMTP istemcisini tanıtmak için kullanılırlar. Argüman alanı, SMTP istemcisinin varsa tamamen nitelenmiş alan adından oluşur. SMTP istemci sisteminin anlamlı bir alan adına sahip olmadığı durumlarda (örn, adres özdevimli ayrılmıştır ve ters eşleme kaydı (rDNS) yoktur), istemci adresin IP kodlu adını (bkz, *IP Kodlu Adlar* (sayfa: 29)) göndermelidir **\*ÖNERİ\***; ek olarak istenirse istemciyi tanıtmaya yardımcı olacak bilgiler de verilebilir. SMTP sunucusu ise, SMTP istemcisine kendisini tanıtmak için, bağlantı üzerinden bu komuta yanıt olarak bir karşılama iletisi gönderir.

Bir istemci SMTP bir SMTP oturumunu **EHLO** komutu göndererek başlatmalıdır **\*ÖNERİ\***. Eğer SMTP sunucusu, SMTP hizmet eklentilerini destekliyorsa karşılık olarak bir başarı, başarısızlık ya da hata belirtebilir. Eğer bir SMTP sunucusu, bu belirtimi ihlal ederek, SMTP hizmet eklentilerinin hiçbirini desteklemiyorsa bir hata yanıtı üretecektir. Eski istemci SMTP sistemleri, evvelce bahsedildiği gibi, **EHLO** yerine (RFC 821'de belirtildiği gibi) **HELO** komutunu kullanabilir **\*SEÇİMLİK\***; (bu bakımdan) sunucuların **HELO** komutunu desteklemesi ve komutu gerektiği gibi yanıtlaması gerekir **\*ZORUNLU\***. Her halükarda, bir istemci bir posta aktarımına başlamadan önce bir **HELO** veya **EHLO** komutu göndermelidir **\*ZORUNLU\***.

Bu komutlar ve bunlara verilen, hem SMTP istemcisini hem de sunucusunu onaylayan "250 OK" yanıtı, başlangıç aşamasıdır, yani, henüz bir aktarım yoktur ve tüm aşamaların tabloları ve tamponları temizdir.

Sözdizimi:

```
ehlo      = "EHLO" BOŞKRK alan CRLF
helo      = "HELO" BOŞKRK alan CRLF
```

Normalde **EHLO** komutunun yanıtı çok satırlı bir yanıt olacaktır. Yanıtın her satırı bir anahtar sözcük ve isteğe bağlı olarak bir veya daha fazla parametre içerir. Çok satırlı yanıtların normal sözdiziminde, bu anahtar sözcükler yanıt kodundan (250) sonra gelir ve son satır haricinde koddan sonra bir tire işareti konur; son satırda ise bir boşluk konur. Olumlu bir yanıtın sözdizimi, ABNF gösterimi ve [8]'deki uçbirim sembolleri kullanılarak şöyledir:

```
ehlo-tamam-yanıtı = ( "250" alan [ BOŞKRK ehlo-karşılama ] CRLF )
                  / ( "250-" alan [ BOŞKRK ehlo-karşılama ] CRLF
                    * ( "250-" ehlo-satırı CRLF )
                    "250" BOŞKRK ehlo-satırı CRLF )
```

```
ehlo-karşılama = 1*(%d0-9 / %d11-12 / %d14-127)
                ; CR veya LF içermeyen bir dizge
```

```
ehlo-satırı = ehlo-anahtar-sözcüğü * ( BOŞKRK ehlo-parametresi )
```

```
ehlo-anahtar-sözcüğü = (HARF / RAKAM) *(HARF / RAKAM / "-")
                    ; ehlo-anahtar-sözcüğü'ne bağlı olarak ehlo-parametresi
```

```

; için ilave sözdizimi

ehlo-parametresi = 1*(%d33-127)
; <BOŞKRK> hariç herhangi bir karakter ve
; tüm denetim karakterleri (US-ASCII 0-31 dahil)

```

**EHLO** anahtar sözcükleri büyük, küçük ve bunların karışımı harflerle belirtilebildiğinden, bunlar daima harf büyüklüğüne duyarsız olarak ele alınmalı ve işleme sokulmalıdır **\*ZORUNLU\***. Bu, RFC 821 ve [Sözdizimsel Genel Prensipler ve Harekât Modeli](#) (sayfa: 12)<sup>(2)</sup> bölümünde belirtilen uygulamanın basit bir uzantısıdır.

#### 4.1.1.2. Posta' (MAIL komutu)

Postanın bir veya daha fazla posta kutusuna teslimi veya başka bir sisteme aktarılması (büyük olasılıkla SMTP kullanarak) için posta verisinin bir SMTP sunucusuna teslimi başlatılırken bu komut kullanılır. Argüman alanı bir dönüş yolunu içermekten başka isteğe bağlı parametreler de içerebilir. Genelde **MAIL** komutu hiçbir posta aktarımı yokken gönderilebilir; [Komutların Sırası](#) (sayfa: 29) bölümüne bakınız.

Dönüş yolu göndericinin posta kutusundan oluşur. Tarihsel olarak, bu posta kutusu bir konak listesi ile de başlayabilirdi, fakat bu davranış artık önerilmemektedir (bkz, [Kaynak Rotalar](#) (sayfa: 53)). Postalama kısır döngülerine yolaçan bir yanıt ile ilgili raporlama iletilerinin bazı türlerinde (posta teslimatı uyarıları veya teslim edememe uyarıları gibi), dönüş yolu boş olabilir (bkz, [Röleleme](#) (sayfa: 19)).

Bu komut, dönüş yolu, sevk yolu ve posta verisi tamponlarını temizledikten sonra bu komuttaki dönüş yolu bilgisini dönüş yolu tamponuna yerleştirir.

Hizmet eklentileri için karşılıklı uzlaşmışsa, **MAIL** komutu ayrıca, bu hizmet eklentileri ile ilgili parametreleri de taşıyabilir.

Sözdizimi:

```

"MAIL FROM:" ("<" / Dönüş-yolu)
[BOŞKRK Mail-Parametreler] CRLF

```

#### 4.1.1.3. Alıcının Belirtilmesi (RCPT komutu)

Bu komut posta verisinin alıcılarını tek tek belirtmek için kullanılır; çok sayıda alıcı belirtilecekse, komut sayısı alıcı sayısı kadar olur. Argüman alanı bir sevk yolunu içermekten başka isteğe bağlı parametreler de içerebilir.

Sevk yolu gerekli olan varış posta kutusundan oluşur. Gönderen sistemlerin, bir kaynak rota olarak bilinen konakların seçimlik listesini üretmeleri gerekir **\*ÖNERİ\***. Alıcı sistemler kaynak rota sözdizimini bilmek zorundadırlar **\*ZORUNLU\***, fakat kaynak rota belirtimini ayırmalı ve kaynak rota sağlanmamış gibi posta kutusu ile ilişkili alan adını kullanmalıdırlar **\*ÖNERİ\***.

Benzer şekilde, röleleme konakları kaynak rotaları ayırmalı ya da yoksaymalı ve isimleri geri dönüş yoluna kopyalamamalıdırlar **\*ZORUNLU\***. Posta nihai hedefine ulaştığında (sevk yolu sadece varış posta kutusunu içerir), SMTP sunucusu onu, kendi konak posta uzlaşımları gereğince, hedef posta kutusuna yerleştirir.

Örneğin,

```

MAIL FROM:<userx@y.foo.org>
RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org>

```

zarf komutları ile röleleme konağı xyz.com'dan alınan posta normal olarak,

```

MAIL FROM:<userx@y.foo.org>
RCPT TO:<userc@d.bar.org>

```



zarf komutları ile doğrudan d.bar.org konağına gönderilmiş olacaktır. [Kaynak Rotalar](#) (sayfa: 53) ekinde belirtildiği gibi, xyz.com ayrıca iletiyi hosta.int'e de rölelemeyi seçebilir \*SEÇİMLİK\*:

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<@hosta.int,@jkl.org:userc@d.bar.org>
```

zarf komutları ile hosta.int'e de veya,

```
MAIL FROM:<userx@y.foo.org>
RCPT TO:<@jkl.org:userc@d.bar.org>
```

zarf komutları ile jkl.org'a da röleleyebilir.

Hizmet eklentileri karşılıklı uzlaşmışsa, **RCPT** komutu ek olarak sunucu tarafından sunulan belli bir hizmet eklentisi ile ilgili parametreleri de taşıyabilir. İstemcinin, **EHLO** yanıtında, sunucu tarafından sunulan bir hizmet eklentisi ile ilgili olanlar dışında parametre iletmemesi gerekir \*ZORUNLU\*.

Sözdizimi:

```
"RCPT TO:" ("<Postmaster@" alan ">" / "<Postmaster>" / sevk-yolu)
[BOŞKRK Rcpt-parametreleri] CRLF
```

#### 4.1.1.4. Posta Verisi (**DATA** komutu)

Alıcı **DATA** komutuna normalde bir 354 yanıtı gönderir ve komuttan sonrasını göndericiden yollanan veri olarak, ([Satırlar](#) (sayfa: 11) bölümünde bahsedildiği gibi, CRLF ile biten) satırlar halinde ele alır. Bu komut, posta verisinin posta verisi tamponuna eklenmesini sağlar. Deneyimlerin BOŞKRK (boşluk), YSEK (yatay sekme), CR (satırbaşı), ve LF (satırsonu) dışında kontrol karakteri kullanımının sorunlara yol açacağını ve mümkün oldukça bundan kaçınılması gerektiğini \*ÖNERİ\* göstermesine rağmen, posta verisi 128 ASCII karakterin her birini içerebilir.

Posta verisi tek bir nokta içeren bir satırla, yani "<CRLF>.<CRLF>" karakter dizisiyle sonlanır (bkz, [Şeffaflık](#) (sayfa: 40)). Bu posta verisi varlığının sona erdiğini gösterir. Bu sonlandırma dizgesindeki ilk <CRLF>'in ayrıca verinin son satırının sonunu, hatta eğer veri yoksa, **DATA** komutunun sonunu belirttiğine dikkat ediniz. İletinin sonuna boş bir satır eklenmesine yolaçacak ek bir <CRLF> kullanılmamalıdır \*ZORUNLU\*. Bu kuralın tek istisnası, ilk çıkış SMTP göndericisine aktarılan ileti gövdesinin <CRLF> ile bitmeyen bir sonuncu satır içermesi durumudur; bu durumda ilk çıkış SMTP sistemi ya geçersiz sayarak iletiyi reddetmeli \*ZORUNLU\* ya da alan SMTP sunucusu "veri sonu" durumunu arayacağından iletiye eksik <CRLF>'i kendi eklemelidir \*ZORUNLU\* (ikisinden biri zorunlu).

Bazı UNIX sistemlerinde uyumsuz davranışa bir taviz olarak, çözümlediğinden fazla birlikte çalışabilirlik sorunlarına sebep olduğu kanıtlanmış sadece <LF> ile biten satırların kabul edilmesi özelinde, dayanıklılığı arttırmak/mükemmelleştirmek adına yapılıyor olarak sunulsa bile, SMTP sunucu sistemleri bunu yapmamalıdır \*ZORUNLU\*. Özellikle, "<LF>.<LF>" dizgesi (çıplak, satırbaşı karakterleri olmaksızın satırsonu karakterleri arasında nokta) posta verisinin sonunu belirten <CRLF>.<CRLF> dizgesinin eşdeğeri olarak ele alınmamalıdır \*ZORUNLU\*.

Posta verisi sonu belirtecinin alınması sunucunun saklanan posta aktarım bilgisini işleme koymasını gerektirir. Bu işlem, dönüş yolu, sevk yolu ve posta verisi tamponlarındaki bilgilerin toplanmasını da kapsar ve komutun işi bittiğinde bu tamponlar temizlenir. İşlem başarıyla tamamlanmışsa, alıcı bir tamam yanıtı göndermelidir \*ZORUNLU\*. Aksi takdirde, alıcı bir başarısızlık yanıtı göndermelidir \*ZORUNLU\*. SMTP modeli bu noktada kısmi başarısızlıklara izin vermez: ya ileti teslim edilmek üzere sunucu tarafından kabul edilip bir olumlu yanıt verilir ya da kabul edilmez ve bir başarısızlık yanıtı gönderilir. Posta verisi sonu alındıktan sonra bir olumlu tamamdır yanıtı gönderilmesiyle, alıcı iletinin tüm sorumluluğunu almış olur (bkz, [Güvenilir Teslimat ve Eposta Yanıtları](#) (sayfa: 45)). Bundan sonra tespit edilen hatalar, [İzleme Bilgisi](#) (sayfa: 37) bölümünde açıklandığı gibi, bir posta iletisinde raporlanmalıdır \*ZORUNLU\*.

SMTP sunucusu rölemek veya yerine teslim etmek için kabul ettiğinde, posta verisinin üst kısmına bir izleme kaydı ekler (ayrıca, "Received" –alındı– satırı veya "zaman damgası satırı" olarak da bilinir). Bu izleme kaydında, iletiyi gönderen ve alan konakların kimliği ile iletinin alındığı tarih ve saat belirtilir. Rölelenen iletilerin birden fazla zaman damgası satırı olur. Bu satırların oluşturulması sözdizimleriyle birlikte [İzleme Bilgisi](#) (sayfa: 37) bölümünde ayrıntılı olarak belirtilmiştir.

**DATA** komutunun işlemlerinden ayrıca [Posta Aktarım Harekâtı](#) (sayfa: 14) bölümünde de bahsedilmiştir.

Sözdizimi:

**"DATA"** CRLF

#### 4.1.1.5. Sıfırlama (**RSET** komutu)

Bu komut o an ki posta hareketinin ister istemez duracağını belirtir. Saklanmış olan gönderici, alıcılar ve posta verisi iptal edilip tüm tamponlar ve durum tabloları temizlenmelidir \*ZORUNLU\*. Alıcı argümansız bir **RSET** komutuna bir "250 OK" yanıtı göndermelidir \*ZORUNLU\*. Sıfırlama komutu istemci tarafından herhangi bir anda gönderilebilir. Oturumda **EHLO** komutundan hemen önce veya sonra ve posta verisi sonu belirtecinden sonra veya bir **QUIT** komutundan hemen önce gönderilmesi halinde etki bakımından bir **NOOP** komutuna eşdeğerdir (etkisizlik anlamında). Bir SMTP sunucusu aldığı bir **RSET** komutunun sonucu olarak bağlantıyı kapatmamalıdır \*ZORUNLU\*; Bu eylem **QUIT** komutuna ayrılmıştır (bkz, [Çıkış \(QUIT komutu\)](#) (sayfa: 27)).

**EHLO** komutu sunucu tarafından yerine getirilecek bazı ek işlemler ve yanıtlar gerektirdiğinden, normal olarak **RSET** komutu, biçimsel anlamsallığı aynı olmasına rağmen bile, **EHLO** komutunu yeniden göndermekten daha verimli olacaktır.

Bu belirtimin amacının aksine, bir SMTP sunucusunun, temel TCP bağlantısının kapanması veya sıfırlanmasının belirtilerini aldığı bazı durumlar vardır. Posta sisteminin dayanıklılığını korumak için SMTP sunucuları bu duruma hazır olmalı \*ÖNERİ\* ve bağlantı kaybolmadan önce bir **QUIT** komutu almış gibi davranmalıdırlar \*ÖNERİ\*.

Sözdizimi:

**"RSET"** CRLF

#### 4.1.1.6. Posta Kutusu Doğrulama (**VRFY** komutu)

Bu komut, argümanında belirtilen bir kullanıcı veya posta kutusunu alıcının doğrulamasını ister. Eğer argüman bir kullanıcı ismi ise bilgi, [Adres Hatalarını Ayıklama Komutları](#) (sayfa: 16) bölümünde belirtilen şekilde döndürülür.

Bu komutun dönüş yolu, sevk yolu veya posta verisi tamponu üzerinde bir etkisi yoktur.

Sözdizimi:

**"VRFY"** BOŞKRK *dizge* CRLF

#### 4.1.1.7. Liste ve Üyelik Doğrulama (**EXPN** komutu)

Bu komut argümanında belirtilen bir posta listesinin doğrulanmasını ister ve eğer böyleyse, liste üyeliğinin döndürülmesini talep eder. Eğer komut başarılıysa, [Adres Hatalarını Ayıklama Komutları](#) (sayfa: 16) bölümünde açıklanan bilgiyi içeren bir yanıt döndürülür. Bu yanıt bir (listenin tek bir üyesi olması durumu) veya daha fazla satır içerecektir.

Bu komutun dönüş yolu, sevk yolu veya posta verisi tamponu üzerinde bir etkisi yoktur ve her zaman gönderilebilir.

Sözdizimi:

**"EXPN"** BOŞKRK *dizge* CRLF

#### 4.1.1.8. Yardım (**HELP** komutu)

Bu komut, sunucunun istemciye yardım bilgisi göndermesini sağlar. Bu komut bir argüman alabilir (örn, bir komut ismi) ve yanıt olarak argümana özgü bilgi döndürebilir \*SEÇİMLİK\*.

Bu komutun dönüş yolu, sevk yolu veya posta verisi tamponu üzerinde bir etkisi yoktur ve her zaman gönderilebilir.

SMTP sunucuları **HELP** komutunu argümansız desteklemelidirler \*ÖNERİ\*, ancak argümanlarla birlikte de destekleyebilirler \*SEÇİMLİK\*.

Sözdizimi:

```
"HELP" [ BOŞKRK dizge ] CRLF
```

#### 4.1.1.9. Eylemsizlik (**NOOP** komutu)

Bu komut, hiçbir parametreyi ya da daha önce girilmiş hiçbir komutu etkilemez. Alıcının OK yanıtı göndermesi dışında hiçbir faaliyet belirtmez.

Bu komutun dönüş yolu, sevk yolu veya posta verisi tamponu üzerinde bir etkisi yoktur ve her zaman gönderilebilir. Bir parametre dizgesi belirtilmişse sunucu bunu yoksaymalıdır \*ÖNERİ\*.

Sözdizimi:

```
"NOOP" [ BOŞKRK dizge ] CRLF
```

#### 4.1.1.10. Çıkış (**QUIT** komutu)

Bu komut, alıcının OK yanıtını göndermesi ve ardından da aktarım kanalını kapatması \*ZORUNLU\* gerektiğini belirtir.

Alıcı aktarım kanalını, **QUIT** komutu alınana ve yanıtlanana kadar kasten kapatmamalıdır (bir hata oluşmuş olsa bile) \*ZORUNLU\*. Gönderen ise **QUIT** komutunu gönderip yanıtı almadan aktarım kanalını kasten kapatmamalıdır (daha önceki bir komuta bir hata yanıtı olsa bile) \*ZORUNLU\*. Eğer bağlantı, daha önce bahsedilmiş olan bozukluklar ya da sistem veya ağ hataları yüzünden vaktinden önce kapatılmışsa, sunucu askıda bekleyen herhangi bir hareketi iptal etmeli \*ZORUNLU\*, fakat daha önce tamamlanmış olan bir hareketi geri almamalı \*ZORUNLU\* ve genellikle komut ya da hareket işlemdeymiş de o sırada geçici bir hata alınmış gibi davranmalıdır \*ZORUNLU\* (örneğin, bir 4yz yanıtı).

**QUIT** komutu her zaman gönderilebilir.

Sözdizimi:

```
"QUIT" CRLF
```

### 4.1.2. Komut Argümanlarının Sözdizimi

Yukarıda sözü edilen komutların argüman alanlarının sözdizimleri (uygulanabildiği yerlerde [8]'de belirtilen sözdizimleri kullanılarak) aşağıda verilmiştir. Aşağıda verilen bazı gösterimler, sadece *Kaynak Rotalar* (sayfa: 53) bölümünde anlatılan kaynak rotaları ile birarada kullanılır. **HARF**, **RAKAM**, **BOŞKRK**, **CR**, **LF**, **CRLF** gibi karakterlerden bu belgede söz edilmemiştir; bunlar, "çekirdek" sözdizimi olarak [8 (6. bölüm)]'de ve ileti biçimi sözdizimi olarak [32]'de tanımlanmıştır.

```
Dönüş-Yolu = Yol
Sevk-Yolu   = Yol
Yol = "<" [ A-d-l ":" ] Posta-kutusu ">"
A-d-l = Alan-da *( " " A-d-l )
        ; Bu biçime dikkat, "kaynak rota" da denir ve
```

```

; kabul edilmesi *ZORUNLU*, üretilmemesi *ÖNERİ*
; ve yoksayılması *SEÇİMLİK* gerekir.
Alan-da = "@" alan
Mail-parametreleri = esmtp-param *(BOŞKRK esmtp-param)
Rcpt-parametreleri = esmtp-param *(BOŞKRK esmtp-param)

esmtp-param      = esmtp-anah-klm ["=" esmtp-değeri]
esmtp-anah-klm   = (HARF / RAKAM) *(HARF / RAKAM / "-")
esmtp-değeri     = 1*(%d33-60 / %d62-127)
; "=" hariç herhangi bir KARAKTER, BOŞKRK (boşluk)
; ve denetim karakterleri
Anah-klm = Hrt-dizge
Argüman  = Atom
Alan     = (alt-alan 1*("." alt-alan)) / IP-kodlu-ad
Alt-alan = Harf-rakam [Hrt-dizge]

IP-kodlu-ad = "[" IPv4-kodlu-ad /
               IPv6-kodlu-ad /
               Genel-kodlu-ad "]"
; bkz, IP Kodlu Adlar (sayfa: 29)

Posta-kutusu = Yerel-kısım "@" Alan

Yerel-kısım  = Noktalı-dizge / Tırnaklı-dizge
; harf büyüklüğüne duyarlılık *SEÇİMLİK*

Noktalı-dizge = Atom *("." Atom)

Atom = 1*birmetin

Tırnaklı-dizge = ÇTIRNAK *tdizge ÇTIRNAK

Dizge = Atom / Tırnaklı-dizge

```

Yerel-kısım için yukarıdaki tanım, birlikte çalışabilirliğin en yüksek derecede olabilmesi için görece serbest olduğu sürece posta almayı uman bir konak Yerel-kısım'ları Tırnaklı-dizge biçimini gerektiren veya harf büyüklüğüne duyarlı olmayı gerektiren posta kutuları tanımlamaktan kaçınmalıdır \*ÖNERİ\*. Yerel-kısımların üretilmesini ve karşılaştırılmasını gerektiren her amaç (posta kutularının isimlerine özgü olmak gibi) için, tırnaklı tüm biçimler eşdeğer olarak ele alınmalı \*ZORUNLU\* ve gönderen sistem olası en az tırnaklama kullanan biçimde aktarmalıdır \*ÖNERİ\*.

Sistemler, posta kutularını, ASCII olmayan karakterlerin (yüksek bitleri 1 olan sekizliler) veya ASCII "denetim karakterleri"nin (onluk değerleri 0–31 ve 127 olan karakterler) SMTP'de kullanılmasını gerektirecek şekilde tanımlamamalıdır \*ZORUNLU\*. Bu karakterler **MAIL** ve **RCPT** komutları ile posta kutusu ismi gerektiren diğer komutlarda kullanılmamalıdır \*ZORUNLU\*.

Tersbölü "\" karakterinin, kendinden sonra gelen karakterin harfiyen yorumlanmasını (normal yorumu yerine) belirtmek üzere kullanılması bakımından bir önceleme karakteri oluşuna dikkat ediniz. Örneğin, "Joe\,Smith", dördüncü karakteri virgül olan dokuz karakterlik bir kullanıcı alanı belirtir.

Uygulamalarda ve isimlendirmede DNS'nin (örn, temel DNS belgesi RFC 1035'in [22] 2.3.1. bölümüne bakınız) uzun süredir devam eden tutucu kullanımıyla tutarlılığı ve birlikte çalışabilirliği yükseltmek için, harfler, rakamlar

ve tire işareti dışındaki karakterler SMTP istemcileri ve sunucularının alan adı yaftalarında görünmemelidir \*ZORUNLU\*. Özellikle, altçizgi karakterine izin verilmemiştir. Geçersiz karakterlerden oluşan bir komut alan her SMTP sunucusu, reddi için başka bir sebep yoksa, bu komutu bir 501 yanıtı ile reddetmelidir \*ZORUNLU\*.

### 4.1.3. IP Kodlu Adlar

Bazan, bir konak, alan adı sistemi tarafından bilinmez ve iletişim engellenir (özellikle, bir hatayı bildirme ve giderme iletişimde). Bu engeli aşmak için, bir alan isminin yerine kullanılmak üzere adresin özel kodlanmış bir biçimine izin verilir. IPv4 adresler için bu biçim, bir Genel Ağ adresini (IPv4) [123.255.37.2] örneğindeki gibi, köşeli ayraç içine alınmış, birbirlerinden noktalarla ayrılmış, sıralı, dört küçük, sekiz bitlik bayta sığabilen onluk tamsayılar biçiminde kullanılır. En sonunda standartlaşabilen IPv6 ve diğer adres biçimleri için biçim, IPv6 standartlarının [17] bir parçası olarak belirtilen biçimde, bir ikinokta üstüste ve adresin kendisi olarak adres sözdizimini tanımlayan standartlaşmış bir "yafta"dan oluşur.

Özellikle:

```
IPv4-kodlu-ad  = Snum 3("." Snum)
IPv6-kodlu-ad  = "IPv6:" IPv6-adrs
Genel-kodlu-ad = Standardize-yafta ":" 1*tdizge
Standardize-yafta = Hrt-dizge
                  ; Standartlaşma aşamalarındaki bir RFC'de belirtilmiş *ZORUNLU*
                  ; ve IANA ile kayıt altına alınmış olmalıdır *ZORUNLU*.

Snum = 1*3RAKAM ; 0 ile 255 arasındaki onluk bir tamsayı gösterimi
Harf-rakam = HARF / RAKAM
Hrt-dizge  = *( HARF / RAKAM / "-" ) Harf-rakam

IPv6-adrs   = IPv6-tam / IPv6-kısmi / IPv6v4-tam / IPv6v4-kısmi
IPv6-onaltı = 1*4ONALTILIKRAKAM
IPv6-tam    = IPv6-onaltı 7(":" IPv6-onaltı)
IPv6-kısmi  = [IPv6-onaltı *5(":" IPv6-onaltı)] "::" [IPv6-onaltı *5(":"
                  IPv6-onaltı)]
                  ; "::" ile en az 2 tane 16 bitlik sıfır grubu belirtilir.
                  ; "::"ye ek olarak 6 gruptan fazlası yoktur.
IPv6v4-tam  = IPv6-onaltı 5(":" IPv6-onaltı) ":" IPv4-kodlu-ad
IPv6v4-kısmi = [IPv6-onaltı *3(":" IPv6-onaltı)] "::"
                  [IPv6-onaltı *3(":" IPv6-onaltı) ":"] IPv4-kodlu-ad
                  ; "::" ile en az 2 tane 16 bitlik sıfır grubu belirtilir.
                  ; "::"ye ek olarak 4 gruptan fazlası yoktur ve
                  ; IPv4-kodlu-ad bulunabilir.
```

### 4.1.4. Komutların Sırası

Hangi komutun hangi sırada kullanılacağına ilişkin sınırlamalar vardır.

Posta aktarımını içerecek bir oturum önce **EHLO** komutu kullanarak ilklendirilmelidir \*ZORUNLU\*. Posta aktarımı yapılmayacaksa bir SMTP sunucusu bu ilklendirme olmaksızın komut kabul edebilmelidir \*ÖNERİ\* (**VERFY** veya **EXPN** gibi).

İstemci tarafından oturum sırasında bir **EHLO** komutu gönderilebilir. Oturum başlangıcından sonra gönderilmişse, SMTP sunucusu tüm tamponları temizlemeli ve bir **RSET** komutu alınmışçasına aşamayı sıfırlamalıdır. Başka bir deyişle, **RSET**'in hemen ardından **EHLO** kullanımı gereksizdir ama lüzumsuz komutların çalıştırılmasının başarıma maliyeti yanında zararsızdır.

Eğer **EHLO** komutu SMTP sunucusu tarafından kabul edilebilir değilse, 501, 500 veya 502 başarısızlık yanıtlarından hangisi uygunsa o gönderilmelidir \*ZORUNLU\*. SMTP sunucusu bu yanıtlar aktarıncaya kadar **EHLO** alınmadan önceki durumunda kalmalıdır \*ZORUNLU\*.

SMTP istemcisi, eğer mümkünse, **EHLO** komutundaki alan parametresinin kendi konağı için geçerli bir asıl konak adı (bir **CNAME** veya **MX** ismi değil) içerdiğinden emin olmalıdır \*ZORUNLU\*. Bu mümkün değilse (örneğin, istemcinin adresi özdevimli atanmıştır ve istemci belirgin bir isme sahip değildir), alan ismini bir IP kodlu adla ikame etmeli \*ÖNERİ\* ve istemciyi tanıtmaya yardımcı olacak ek bilgileri de sağlamış olmalıdır.

SMTP sunucusu, **EHLO** komutundaki alan adı parametresinin istemcinin IP adresine tekabül edip etmediğini doğrulatabilir \*SEÇİMLİK\*. Ancak, doğrulama başarısız olursa, sunucu bu sebeple bir iletiyi reddetmemelidir \*ZORUNLU\*; doğrulama bilgisi başarısızlığı sadece oturum açma ve izleme gecikmelerinden kaynaklanmış olabilir.

**NOOP**, **HELP**, **EXPN**, **VRFY** ve **RSET** komutları oturum sırasında veya önceden oturumu iklendirmeksizin herhangi bir anda kullanılabilir. SMTP sunucuları bunları evvelce bir **EHLO** komutu alınmamış olsa bile normal olarak (yani, bir 503 kodu döndürmeksizin) işleme almalı \*ÖNERİ\*; istemciler ise bu komutları göndermeden önce **EHLO** ile bir oturum açmalıdır \*ÖNERİ\*.

Eğer bu kurallara uyulursa, RFC 821'deki bir örnekteki, bir **EXPN** komutuna "550 erişiminize izin verilmedi" yanıtının verilmesi, **EXPN** komutunun öncesinde bir **EHLO** olmadıkça veya erişim yasağı istemcinin IP adresine veya diğer kimlik kanıtlama/saptama mekanizmalarından kaynaklanmadıkça yanlış olacaktır.

**MAIL** komutu (veya artık atıl olan **SEND**, **SOML** ve **SAML** komutları) bir posta aktarımı başlatır. Başlatıldığında, bir posta aktarımı, sırasıyla, bir aktarım başlatma komutu, bir veya daha fazla **RCPT** komutu ve bir **DATA** komutundan oluşur. Bir posta aktarımı **RSET** (veya yeni bir **EHLO**) komutu ile terkedilebilir. Bir oturumda birden fazla posta aktarımı yapılabildiği gibi hiç posta aktarımı da yapılmayabilir. **MAIL** komutu (veya artık atıl olan **SEND**, **SOML** ve **SAML** komutları) zaten açık olan bir posta aktarımında gönderilmemelidir \*ZORUNLU\*, yani, sadece şu durumlarda gönderilebilir: başlatılmış bir posta aktarımı yoksa veya aktarım başarılı bir **DATA** komutuyla önceden tamamlanmışsa ya da evvelce bir **RSET** ile oturum terkedilmişse.

Eğer aktarım başlatma komutunun argümanı kabul edilebilir değilse, bir 501 başarısızlık yanıtı döndürülmeli \*ZORUNLU\* ve SMTP sunucusu aynı durumda kalmalıdır \*ZORUNLU\*. Bir aktarımdaki komutlar sunucu tarafından işlenemeyecek derecede sırasızsa, bir 503 başarısızlık yanıtı döndürülmeli \*ZORUNLU\* ve SMTP sunucusu aynı durumda kalmalıdır \*ZORUNLU\*.

Bir oturumdaki son komut **QUIT** komutu olmalıdır \*ZORUNLU\*. **QUIT** komutu oturum sırasında herhangi bir başka zaman kullanılamaz, fakat bir oturum açma komutu gönderilmiş veya alınmış olmasa bile, SMTP istemcisi tarafından bağlatının kapatılmasını istemek için kullanılması gerekir \*ÖNERİ\*.

#### 4.1.5. Özel Kullanımlı Komutlar

*Eklentilerin Tanımlanması ve Kayda Geçirilmesi* (sayfa: 8) bölümünde belirtildiği gibi, "X" ile başlayan komutlar istemci (gönderen) ve sunucu (alan) SMTP sistemleri arasında karşılıklı uzlaşarak kullanılabilir. Böyle bir komutu tanımayan bir SMTP sunucusunun komutu, "500 Komut tanınmıyor" ile yanıtlaması beklenir. Eklentili bir SMTP sunucusu **EHLO** komutunun yanıtında bu özel komutlarla ilgili özellik isimlerini listeleyebilir \*SEÇİMLİK\*.

SMTP sistemlerince gönderilip kabul edilen "X" ile başlamayan komutlar *Eklentilerin Tanımlanması ve Kayda Geçirilmesi* (sayfa: 8) bölümündeki gereksinimlere uymalıdır \*ZORUNLU\*.

## 4.2. SMTP Yanıtları

SMTP komutlarının yanıtları, posta aktarım işlemindeki isteklerin ve eylemlerin eşzamanlanmasının temini ve SMTP istemcisinin SMTP sunucusunun durumunu daima bilmesini garantilemek için kullanılırlar. Her komutun sadece ve sadece bir yanıt üretmesi gerekir \*ZORUNLU\*.



Komut-yanıt dizilimlerinin ayrıntıları *Komutların ve Yanıtların Sıralanışı* (sayfa: 35) bölümünde açıklanmıştır.

Bir SMTP yanıtı bu belgede aksi belirtilmiş olmadıkça, üç rakamlı bir sayıyı (üç tane sayısal karakter olarak aktarılır) izleyen bir metinden oluşur. Sayı bilgisayar tarafından geçilecek durumu saptamak için, metin ise insan kullanıcılar içindir. 3 rakam, SMTP istemcisinin metni incelemeksizin kullanıcıya mı aktaracağı yoksa iptal mi edeceğine karar verebilmesine yetecek kadar kodlanmış bilgiyi içerir. İstisnalara bu belgenin çeşitli yerlerinde dikkat çekilmiştir. Kısım, 220, 221, 251, 421 ve 551 yanıt kodları, makineler tarafından çözümlenip yorumlanması gereken ileti metinleriyle ilgilidir. Genel durumda ise, metin alıcıya bağımlı ve bağlama bağımlı olabilir, bu yüzden her yanıt kodu için metnin değişmesi sözkonusu olabilir. Yanıt kodları teorisinin açıklaması *Yanıt Kodlarının Önemleri ve Kuram* (sayfa: 31) bölümünde verilmiştir. Biçimsel olarak bir yanıt bir dizilim olarak tanımlanmıştır: üç rakamlık bir kod, <BOŞKRK>, metnin bir satırı ve <CRLF> ya da çok satırlı bir yanıt (*Yanıt Kodlarının Önemleri ve Kuram* (sayfa: 31) bölümünde tanımlandığı gibi). Bu belirtimle çelişerek metin bazan gönderilmediğinden, metni almayan istemciler kodu tek başına (bir boşluk karakteri içersin içermesin) işlemeye hazırlıklı olmalıdırlar \*ÖNERİ\*. Sadece **EHLO**, **EXPN** ve **HELP** komutlarının normal koşullarda çok satırlı yanıtlarla sonuçlanması beklenirse de, çok satırlı yanıtlara her komutta izin verilmektedir.

ABNF gösterimiyle sunucunun yanıtları:

```
Karşılama = "220 " Alan [ BOŞKRK metin ] CRLF
Yanıt-satırı = Yanıt-kodu [ BOŞKRK metin ] CRLF
```

sadece 220 yanıtının görüldüğü "Karşılama" iletisi ile sunucu, bağlantının kendine düşen parçasını açtığını duyurmuş olur.

Bir SMTP sunucusu sadece bu belgede listelenen yanıt kodlarını göndermeli \*ÖNERİ\* ve uygun düştükçe örneklerde gösterilen metinleri kullanmalıdır \*ÖNERİ\*.

Bir SMTP istemcisi eylemini metne bakarak değil sadece yanıt koduna bakarak saptamalıdır \*ZORUNLU\* ("adres değişikliği" için olan 251 ve 551 ile gerekliyse 220, 221 ve 421 yanıtları hariç); genel durumda, hiç metin bulunmaması halini de içererek her metin kabul edilebilmelidir \*ZORUNLU\*(göndericiler çıplak kodlar göndermemelidir \*ÖNERİ\* dense de). Yanıt kodundan sonra gelen boşluk metnin parçası olarak kabul edilir. Mümkün olduğunca, bir alıcı SMTP sistemi yanıt kodunun ilk rakamını (önem belirteci) sinamalıdır \*ÖNERİ\*.

Aşağıda bulunan kodların listesi kalıcıymış gibi yorumlanmamalıdır \*ZORUNLU\*. Yanıtın metinsel kısmındaki tamamlayıcı bilginin tercih edilmesiyle birlikte yeni kodların eklenmesi nadir ve önemli bir etkinlik olduğu sürece, yeni standartların ya da standartlaşma aşamalarındaki belirtilerin sonucu olarak yeni kodlar eklenebilir. Sonuç olarak, bir gönderici SMTP sistemi bu belgede belirtilmemiş kodlarla çalışmaya hazırlıklı olmalı \*ZORUNLU\* ve sadece ilk rakamı yorumlayarak gereğini yapmalıdır \*ZORUNLU\*.

#### 4.2.1. Yanıt Kodlarının Önemleri ve Kuram

Yanıtın üç rakamının her birinin özel bir önemi vardır. İlk rakam yanıtın iyi mi, kötü mü yoksa eksik mi olduğunu belli eder. Aşırı karmaşılaşmamış veya beklenmedik bir kod alan bir SMTP istemcisi bu ilk rakamı inceleyerek yapacağı eylemi (planlı işlem, yeniden yapma, kısıntı, vb. gibi) saptayabilecektir. Ne çeşit hata oluştuğunu (posta sistemi hatası, komut sözdizimi hatası, vb. gibi) yaklaşık olarak bilmek isteyen bir SMTP istemcisi, ikinci rakamı inceleyebilir. Üçüncü rakam ve mevcut olabilecek bütünleyici her bilgi, bilginin eniyi derecelenmesi için ayrılmıştır.

Yanıt kodunun ilk rakamı için beş değer vardır:

##### 1yz Ön Hazırlık Olumlu yanıtı

Komutun kabul edilmiş olduğunu ama istenen eylemin askıda tutulduğunu, bu yanıtta bilginin doğrulanmasının bekletildiğini belirtir. SMTP istemcisi eylemin sürdürüleceğini mi yoksa bırakılacağını mı belirten başka bir komut göndermelidir. Bilgi: Eklentisiz SMTP'nin yanıtın bu türüne izin veren komutları yoktur ve dolayısıyla devam veya terk komutlarına da sahip değildir.

##### 2yz Tamamlama Olumlu yanıtı

İstenen eylem başarıyla tamamlanmıştır. Yeni bir istek başlatılabilir.

### 3yz Araşlem Olumlu yanıtı

Komut kabul edilmiştir, fakat istenen eylem askıya alınmış olup bu bilginin alındısı bekletilmektedir. SMTP istemcisi bu bilgiyi belirten başka bir komut göndermelidir. Bu yanıt sıralı komut gruplarında (örn, **DATA**) kullanılır.

### 4yz Geçici Tamamlama Olumsuz yanıtı

Komut kabul edilmemiş ve istenen eylem gerçekleşmemiştir. Ancak, hata durumu geçicidir ve eylem yeniden talep edilebilir. Gönderici (varsa) komut sırasının başına dönmelidir. "Geçici" için bir anlam atamak, her iki tarafın da (alıcı ve gönderici SMTP sistemleri) yorumda hemfikir olması gerektiğinde zordur. Bu kapsamdaki her yanıt farklı bir zaman değerine sahip olabilir, fakat SMTP sunucusu tekrar denemesi için teşvik edilir. Bir yanıtın 4yz ya da 5yz (aşağıya bakınız) sınıfına girip girmediğini saptamanın ana kuralı, gönderici veya alıcının özelliklerinde veya komut biçiminde değişiklik yapmaksızın yinelenenirse başarılı olma şansı varsa (yani, komut aynen yinelenir ve alıcı yeni bir gerçeklenim ortaya koymaz), bu yanıtlar 4yz yanıtlarıdır, şeklindedir.

### 5yz Kalıcı Tamamlama Olumsuz yanıtı

Komut kabul edilmemiş ve istenen eylem gerçekleşmemiştir. SMTP istemcisi aynı isteği (aynı sırayla) yinelemekten vazgeçirilir. Hatta bazı "kalıcı" hata durumları doğrulanabilir, böylece insan kullanıcı, SMTP istemcisinden, gelecekteki bir anda doğrudan bir eylemin sonucu olarak komut sırasını yeniden başlatmasını isteyebilir (örneğin, yazılışta veya kullanıcının hesap bilgilerinde değişiklik olduğunda).

İkinci rakam yanıtları belli sınıflara kodlar:

#### x0y Sözdizimi:

Bu yanıtlar, başka bir işlevsel sınıfla örtüşmeyen sözdizimsel olarak yanlış komutlar, gerçekleşmemiş ya da gereksiz komutlar ve sözdizimi hataları ile ilgilidir.

#### x1y Bilgi:

Bunlar yardım veya durum bilgisi isteği gibi bilgi isteklerine yanıtlardır.

#### x2y Bağlantılar:

Bunlar aktarım kanalına atıfta bulunan yanıtlardır.

#### x3y Belirsiz.

#### x4y Belirsiz.

#### x5y Posta sistemi:

Bu yanıtlar alıcı posta sisteminin istenen aktarımla veya başka bir posta sistemi eylemiyle karşı karşıya kaldığı durumu belirtir.

Üçüncü rakam, ikincisi tarafından belirtilen sınıflamalara daha hassas dereceleme sağlar. Yanıtların listesi bunu en iyi gösteren yerdir. Her yanıt metni zorunludan ziyade önerileni belirtir ve hatta ilişkilendirildiği komuta göre değişebilir. Diğer taraftan, yanıt kodları kesinlikle bu bölümdeki belirtilmeleri takip etmelidir. Alıcı gerçeklenimleri, burada açıklanandan azıcık farklı durumlarda zaten tanımlanmış olanlara uyum sağlamaktansa yeni kodlar uydurmamalıdır.

Örneğin, başarılı çalışması SMTP istemcisine yeni bir bilgi sunmayan **NOOP** gibi bir komut bir 250 yanıtı döndürecektir. Bir komut siteye özgü olmayan gerçekleşmemiş bir eylemi talep ettiğinde yanıt 502 olur. Gerçeklenmiş bir komuttan gerçekleşmemiş bir parametre ile istekte bulunmanın cezası ise 504 yanıtıdır.

Yanıt metni tek bir satırdan daha uzun olabilir; bu gibi durumlarda, SMTP istemcisinin metnin tamamın elde etmek için nereye kadar okuyacağını belirtecek şekilde ileti metni imlenmelidir. Bu, çok satırlı bir yanıt belirten özel bir biçimi gerektirir.



Çok satırlı yanıt biçimi, son satır dışında bütün satırlar yanıt koduyla başlar, ardına bir tireden (eksi işareti diye de bilinir) sonra satır metni eklenir. Son satırda ise tire işaretinin yerini `<BOŞKRK>` (boşluk) alır ve metin isteğe bağlıdır. Satırların tamamı `<CRLF>` ile biter. Yukarıda da dikkat çekildiği gibi, sunucular, ardında bir metin bulunmasa bile `<BOŞKRK>` göndermelidir \*ÖNERİ\*, fakat istemcilerin bunun yokluğuna karşı hazırlıklı olması gerekir \*ZORUNLU\*.

Örneğin:

```
123-ilk satır
123-ikinci satır
123-234 metin sayıyla basliyor
123 son satır
```

Çoğu durumda SMTP istemcisi basitçe yanıt kodundan sonra `<BOŞKRK>` veya `<CRLF>` gelen satırı aramaya ihtiyaç duyar ve öncesindeki tüm satırları yoksayar. Sadece birkaç durumda, yanıt metninde istemci için önemli bilgi vardır. İstemci bu durumları o anki bağlamdan tespit etme konusunda yetkin olmalıdır.

#### 4.2.2. İşlev Gruplarına göre Yanıt Kodları

```
500 Sözdizimi hatası, komut tanınmıyor
    (Komut satırı çok uzun gibi hataları içerebilir)
501 Parametre ya da argümanlarda sözdizimi hatası
502 Komut gerçekleşmedi (bkz, 502 Yanıt Kodu (sayfa: 34))
503 Komutların sırası hatalı
504 Komut parametresi gerçekleşmedi
211 Sistem durumu veya sistem yardımı yanıtı
214 Yardım iletisi
    (Kullanım bilgisi veya standart dışı bir komutun anlamı;
    bu yanıt sadece insan kullanıcılar için yararlıdır.)
220 <alan> Hizmete hazır
221 <alan> Hizmet, aktarım kanalını kapatıyor
421 <alan> Hizmete uygun değil, aktarım kanalı kapanıyor
    (Hizmet kapatılmakta olduğunu biliyorsa bu yanıt herhangi bir
    komuta verilebilir.)
250 İstenen posta eylemi başarıyla tamamlanmıştır
251 Kullanıcı yerel kullanıcı değil; <sevk-yolu> adresine sevkedilecek
    (bkz, Adres Düzeltmek veya Güncellemek için Yönlendirme (sayfa: 16))
252 VRFY için kullanıcı doğrulanamıyor, ama ileti kabul edilecek ve
    teslim edilmeye çalışılacaktır
    (bkz, VRFY veya EXPN için Başarılı Yanıtın Anlamı (sayfa: 18))
450 İstenen posta eylemi yerine getirilemedi: posta kutusu elverişli değil
    (örn, posta kutusu meşgul)
550 İstenen eylem yerine getirilemedi: posta kutusu elverişli değil
    (örn, posta kutusu bulunamadı, erişilemedi veya
    kurallar gereği komut reddedildi)
451 İstenen eylem tamamlanmadı: işlem sırasında hata
551 Kullanıcı yerel kullanıcı değil; lütfen <sevk-yolu> adresini deneyin
    (bkz, Adres Düzeltmek veya Güncellemek için Yönlendirme (sayfa: 16))
452 İstenen eylem yerine getirilemedi: sistem kaynakları yetersiz
552 İstenen posta eylemi yerine getirilemedi: saklama alanı yetmiyor
553 İstenen eylem yerine getirilemedi: posta kutusu ismine izin yok
```

(örn, posta kutusu isminde sözdizimi hatası)  
 354 Posta girdisini başlat ve <CRLF>.<CRLF> ile bitir  
 554 Aktarım başarısız oldu (Veya, bir bağlantı açılış yanıtında:  
 "Burada öyle bir SMTP hizmeti verilmiyor")

### 4.2.3. Numara Sırasıyla Yanıt Kodları

211 Sistem durumu veya sistem yardımı yanıtı  
 214 Yardım iletisi  
 (Kullanım bilgisi veya standart dışı bir komutun anlamı;  
 bu yanıt sadece insan kullanıcılar için yararlıdır.)  
 220 <alan> Hizmete hazır  
 221 <alan> Hizmet, aktarım kanalını kapatıyor  
 250 İstenen posta eylemi başarıyla tamamlanmıştır  
 251 Kullanıcı yerel kullanıcı değil; <sevk-yolu> adresine sevk edilecek  
 (bkz, [Adres Düzeltmek veya Güncellemek için Yönlendirme](#) (sayfa: 16))  
 252 VRFY için kullanıcı doğrulanamıyor, ama ileti kabul edilecek ve  
 teslim edilmeye çalışılacaktır  
 (bkz, [VRFY veya EXPN için Başarılı Yanıtın Anlamı](#) (sayfa: 18))  
 354 Posta girdisini başlat ve <CRLF>.<CRLF> ile bitir  
 421 <alan> Hizmete uygun değil, aktarım kanalı kapanıyor  
 (Hizmet kapatılmakta olduğunu biliyorsa bu yanıt herhangi bir  
 komuta verilebilir.)  
 450 İstenen posta eylemi yerine getirilemedi: posta kutusu elverişli değil  
 (örn, posta kutusu meşgul)  
 451 İstenen eylem tamamlanmadı: işlem sırasında hata  
 452 Talep edilen faaliyet alınamadı: yetersiz bellek alanı  
 500 Sözdizimi hatası, komut tanınmıyor  
 (Komut satırı çok uzun gibi hataları içerebilir)  
 501 Parametre ya da argümanlarda sözdizimi hatası  
 502 Komut gerçekleştirilmedi (bkz, [502 Yanıt Kodu](#) (sayfa: 34))  
 503 Komutların sırası hatalı  
 504 Komut parametresi gerçekleştirilmedi  
 550 İstenen eylem yerine getirilemedi: posta kutusu elverişli değil  
 (örn, posta kutusu bulunamadı, erişilemedi veya  
 kurallar gereği komut reddedildi)  
 551 Kullanıcı yerel kullanıcı değil; lütfen <sevk-yolu> adresini deneyin  
 (bkz, [Adres Düzeltmek veya Güncellemek için Yönlendirme](#) (sayfa: 16))  
 552 İstenen posta eylemi yerine getirilemedi: saklama alanı yetmiyor  
 553 İstenen eylem yerine getirilemedi: posta kutusu ismine izin yok  
 (örn, posta kutusu isminde sözdizimi hatası)  
 554 Aktarım başarısız oldu (Veya, bir bağlantı açılış yanıtında:  
 "Burada öyle bir SMTP hizmeti verilmiyor")

### 4.2.4. 502 Yanıt Kodu

502 yanıt kodu (Komut gerçekleştirilmedi) diğer kodlara tercih edildiğinde \*ÖNERİ\*, sorular yükselir. 502 yanıt kodu, komutun aslında SMTP sunucusu tarafından tanındığı ama gerçekleştirilmediği durumda kullanılmalıdır \*ÖNERİ\*. Eğer komut tanınmıyorsa 500 yanıt kodu döndürülmelidir \*ÖNERİ\*. Eklentili SMTP sistemleri **EHLO** yanıtında yeteneklerini listelerken 502 (veya 500) döndürecekleri yetenekleri belirtmemelidirler \*ZORUNLU\*.

#### 4.2.5. <CRLF> .<CRLF>'in Ardından DATA Komutuna Yanıt

Bir SMTP sunucusu **DATA** komutu <CRLF> .<CRLF> ile tamamlandıktan sonra bir 2yz Tamamlama Olumlu yanıtı geri döndürdüğünde şu sorumlulukları almış olur:

- iletinin teslimatı (alıcı posta kutusu mevcutsa) veya
- eğer geçici durumlar yüzünden (gecikerek) ileti teslim etmeye çalışacaksa, *Yanıt Stratejileri* (sayfa: 43) bölümünde belirtilen zaman aralıklarıyla makul sayıda yineleyerek iletinin teslimatı
- iletinin teslimat çalışması kalıcı durumlar yüzünden başarısız olursa veya geçici durumlar yüzünden yinelenen teslimat çabası başarısız olursa, özgün ileti göndericisine uygun bir uyarı iletisinin gönderilmesi (SMTP **MAIL** komutundaki adresi kullanarak).

Bir SMTP sunucusu **DATA** komutu <CRLF> .<CRLF> ile tamamlandıktan sonra bir kalıcı hata durumu (5yz) kodu geri döndürdüğünde, iletiyi teslim etmek için bir daha teşebbüste bulunmamalıdır \*ZORUNLU\*. İletinin teslimatı SMTP istemcisinin sorumluluğundadır ve bunu ya kullanıcıya geri döndürür ya da teslim etmeye çalışmak üzere yeniden kuyruğa alır (bkz, *Gönderme Stratejisi* (sayfa: 43)).

İletinin kaynaklandığı kullanıcı, geçici hata durumundan dolayı bir dönüşü (posta iletisi veya başka bir şekilde) tıpkı kalıcı başarısızlıkta olduğu gibi teslimatın yapılamayışının bir belirtisi olarak yorumlayabilmelidir \*ÖNERİ\*. Yani, istemci SMTP sistemi bu durumları başarıyla ele alabiliyorsa, kullanıcı böyle bir yanıt almayacaktır.

Bir SMTP sunucusu **DATA** komutu <CRLF> .<CRLF> ile tamamlandıktan sonra bir kalıcı hata durumu (5yz) kodu geri döndürdüğünde, iletiyi teslim etmek için bir daha teşebbüste bulunmamalıdır \*ZORUNLU\*. Geçici hata durumu kodlarındaki gibi iletinin teslimatı yine SMTP istemcisinin sorumluluğundadır, fakat kullanıcı iletiyi inceleyip müdahale etmeden teslimatı tekrar aynı sunucuya yapmaya çalışmamalıdır \*ÖNERİ\*.

### 4.3. Komutların ve Yanıtların Sıralanışı

#### 4.3.1. Sıralanışa Genel Bakış

Alıcı ile gönderici arasındaki iletişim gönderici tarafından denetim altında tutulan değişken bir diyalogdur. Aslında, gönderici bir komut verir ve alıcı da yanıtını. Başka türlü düzenlenmedikçe, hizmet eklentileri üzerinden görüşülür. Gönderici bir komut yollamadan önce önceki komutun yanıtını beklemelidir \*ZORUNLU\*.

Önemli tek yanıt bağlantı karşılama yanıtıdır. Normal olarak, bağlantı kurulduğunda alıcı bir 220 "Hizmete hazırım" yanıtı gönderir. Göndericinin herhangi bir komut göndermeden önce bu karşılama iletisini beklemesi gerekir \*ÖNERİ\*.



#### Bilgi

Tüm karşılama türü yanıtlarda yanıt kodundan sonraki ilk sözcük sunucu konağın resmi adı (tamamen nitelenmiş birincil alan adı) olur. Bazan konak anlamlı bir isme sahip olmayabilir. Bu gibi durumlarla ilgili olasılıkların açıklamaları için *IP Kodlu Adlar* (sayfa: 29) bölümüne bakınız.

Örneğin,

```
220 ISIF.USC.EDU Service ready
```

veya

```
220 mail.foo.com SuperSMTP v 6.1.2 Service ready
```

ya da

```
220 [10.0.0.1] Clueless host service ready
```

Aşağıdaki tablo, her komut için olası başarı ya da başarısızlık yanıtlarını listeler. Bunlar şuna kesinlikle bağlı kalmalıdır \*ÖNERİ\*: alıcı yanıtlardaki metinlerde değişiklik yapabilir, fakat kod numaralarına ve komuta özgü yanıt sırasına göre uygulanan eylem ve anlam değiştirilemez.

#### 4.3.2. Komut–Yanıt Sıralanışı

Her komut kendi olası yanıtlarıyla birlikte listelenmiştir. Kullanılan örneklerle olası yanıtlar belirtilmiştir: Ara yanıtlar için "A", hatalar için "H", başarı yanıtları için "B" örnekleri kullanılmıştır. Özel bazı durumlar ve gelecek eklentilere izin vermek için bazı sunucular özel yanıtlar üretebildiklerinden, SMTP istemcilerinin, mümkün olduğu anda, yanıtın sadece ilk rakamını yorumlamaları \*ÖNERİ\* ve sadece ilk rakamı yorumlayarak, tanımadıkları yanıt kodları ile çalışmaya hazırlıklı olmaları gerekir \*ZORUNLU\*. *Eklenti Modeli* (sayfa: 7) bölümünde açıklanan mekanizmaları kullanarak genişletilmiş olmadıkça, SMTP sunucularının üç rakamdan farklı veya 2,3,4,5 ile başlamayan yanıt kodları aktarmamaları gerekir \*ZORUNLU\*.

Bu sıralama kuralları ve presipte kodların kendileri, sunucularda sunulmak ve istemcilerce kabul edilmek (istenmek) üzere, SMTP eklentileri tarafından değiştirilebilir ve genişletilebilir.

Aşağıda listelenen kodlara ilaveten, her SMTP komutu, ilgili yararsız durumlar saptanırsa aşağıdaki kodlardan herhangi birini döndürebilir:

500

"komut satırı çok uzun" durumunda veya komut isminin tanınmadığı durumlarda. Bu komutların gerekli alt kümesine yanıtta bir "komut tanınmıyor" hatası üretilmesinin bu belirtimle çelişildiğini göstereceğine dikkat ediniz.

501

Komut veya argümanlarda sözdizimi hatası. Gelecekteki genişletmeler için sağlanması durumunda, bu belgede argüman kabul etmeyen komutlar olarak geçen komutlar (**DATA**, **RSET**, **QUIT** komutları), argümanlar **EHLO** için ilan edilmiş eklentilerin yokluğunda sağlanmışsa, bir 501 yanıtı döndürmelidir \*ÖNERİ\*.

421

Hizmet kapanıyor ve aktarım kanalını kapatıyor.

Belli başlı sıralamalar:

BAĞLANTI TESİSİ

B: 220

H: 554

EHLO veya HELO

B: 250

H: 504, 550

MAIL

B: 250

H: 552, 451, 452, 550, 553, 503

RCPT

B: 250, 251 (ama 251 ve 551 açıklaması için

bkz, *Adres Düzeltmek veya Güncellemek için Yönlendirme* (sayfa: 16))

H: 550, 551, 552, 553, 450, 451, 452, 503, 550

DATA

A: 354 -> veri -> B: 250

H: 552, 554, 451, 452

```

      H:  451, 554, 503
RSET
      B:  250
VRFY
      B:  250, 251, 252
      H:  550, 551, 553, 502, 504
EXPN
      B:  250, 252
      H:  550, 500, 502, 504
HELP
      B:  211, 214
      H:  502, 504
NOOP
      B:  250
QUIT
      B:  221

```

#### 4.4. İzleme Bilgisi

Bir SMTP sunucusu teslim etmek veya işleme koymak için bir ileti aldığı anda, *Posta Verisi (DATA komutu)* (sayfa: 25) bölümünde açıklandığı gibi ileti içeriğinin başlangıcına bir izleme bilgisi ("zaman damgası" veya "Received" satırı) yerleştirmelidir.

Bu satır şöyle yapılandırılmalıdır **\*ZORUNLU\***:

- Bir SMTP ortamından kaynaklanması gereken **FROM** alanı **\*ZORUNLU\***, şunların ikisini birden içermelidir **\*ÖNERİ\***: (1) **EHLO** komutunda sunulduğu gibi kaynak konağın ismi ve (2) TCP bağlantısından saptanan, kaynak IP adresiyle kodlanmış adres.
- RFC 822'de tavsiye edildiği gibi **ID** alanı "@" içerebilir **\*SEÇİMLİK\***, fakat bu gerekli değildir.
- Çok sayıda **RCPT** komutu verildiğinde **FOR** alanı < yol > girdilerinden oluşmuş bir liste içerebilir **\*SEÇİMLİK\***. Bu bazı güvenlik sorunlarını arttırabilir ve genellikle de istenen bir şey değildir; bkz, *"Gizli" Kopyalar* (sayfa: 48).

Bir Genel Ağ posta programı, evvelce ileti başlığına eklenmiş bir "Received:" satırını değiştirmemelidir **\*ZORUNLU\***. SMTP sunucuları "Received:" satırlarını iletilerin başlarına eklemeli **\*ZORUNLU\***; mevcut satırların sırasını değiştirmemeli **\*ZORUNLU\*** veya "Received:" satırlarını başka bir yere yerleştirmemelidirler **\*ZORUNLU\***.

Genel Ağ'ın büyümesiyle, *Received* alanlarının karşılaştırılabilirliği, sorunları, özellikle de yavaş röle sorunlarını saptamada önem kazanmaktadır. *Received* alanlarını oluşturan SMTP sunucuları zaman dilimi isimlerinden ziyade doğrudan doğruya saat farklarını (−0800 gibi) kullanmalıdırlar **\*ÖNERİ\***. Uygulanabilir olduğunda, yerel zamanı evrensel zamana (UT) göre saat farkıyla belirtmek tercih edilmelidir. Bu yöntem, belirtilecek yerel durumlar hakkında biraz daha fazla bilgiyi mümkün kılar. Evrensel zaman (UT) gerekliyse, alıcının değer dönüşümü için sadece basit işlemler yapmaya ihtiyacı olur. Evrensel zaman (UT) kullanımı, sunucunun yeri–zaman dilimi hakkındaki bilgiyi kaybeder. Bir zaman dilimi ismi sağlanması isteniyorsa, ismin bir açıklamanın içinde bulunması gerekir **\*ÖNERİ\***.

Teslimatçı SMTP sunucusu bir iletinin "son teslimat"ını yaparken, posta verisinin başına bir "Return-Path" (Dönüş Yolu) satırı yerleştirir. Bu "Return-Path" satırı kullanımı gereklidir ve posta sistemleri bunu desteklemelidir **\*ZORUNLU\***. "Return-Path" satırı **MAIL** komutundaki <dönüş-yolu> bilgisinin korunmasını sağlar. Burada, "son teslimat" ile iletinin SMTP ortamında kaldığı anlatılmak istenmektedir. Normalde, bu, postanın

hedef kullanıcıya veya posta ile ilişkili bir yere teslim edileceği, ancak bazı durumlarda başka bir posta sistemine aktarılabilirliği ve orada işleme sokulacağı anlamına gelirdi.

Dönüş yolundaki posta kutusunun asıl göndericinininkinden farklı olması olasıdır, örneğin, hata yanıtlarının ileti göndericisinden ziyade özel bir hata iletileri alıcısı posta kutusuna teslimi gerekiyorsa, bu yararlıdır. Olaya postalama listeleri karıştığında bu düzenleme sıradandır ve hataların iletiyi yazana değil de listeyi yönetene yönlendirilmesi anlamında yararlıdır.

Yukarıdaki metinde ima edilen, son posta verisinin dönüş yolu satırı ile başladığı, bir ya da daha fazla zaman damgası satırı ile devam ettiğidir. Bu satırları posta verisi başlıkları ve gövdesi izler [32].

Sevk ve diğer işlemler ileti teslimat için kabul edildikten sonra yapıldığından teslimatın ne amaçla yapıldığının tespiti bir SMTP sunucusu için bazan zor olur. Sonuç olarak, ilgili (sevk, ağgeçidi, röle) sistemler dönüş yolunu söylebilir \*SEÇİMLİK\* ve **MAIL** komutunu, teslim edilen iletide tam olarak böyle tek bir satırın görünmesini temin edecek şekilde yeniden kurgulayabilirler.

İletinin kaynaklandığı SMTP sistemi, iletiyi, başlığında bir "Return-Path" satırı mevcut olarak göndermemelidir \*ÖNERİ\*. Bir röleme işlemi uygulayan SMTP sunucuları ileti verisini incelememeli \*ZORUNLU\* ve özellikle de bir "Return-Path" satırı mevcut mu, diye bakmamalıdır. Son teslimatı yapan SMTP sunucuları ise, kendilerininkini eklemekten önce "Return-Path" satırlarını söylebilirler \*SEÇİMLİK\*.

Dönüş yolunun birincil amacı, yapılmayan teslimatı belirten iletinin veya gönderilecek başka bir posta sistemi başarısızlık bildiriminin adresini tayin etmektir. Bir belirsizlik oluşturmaması için, iletinin teslimatı sırasında sadece ve sadece bir dönüş yolu mevcut olmalıdır \*ÖNERİ\*. SMTP dışı aktarımlarda RFC 822 sözdizimini kullanan sistemler hataların (örn, teslim edilmeyen iletiler) raporlanması gerektiğinde, aktarım zarfıyla ilişkili ve belirsizlik oluşturmayan bir adres tayin etmelidirler \*ÖNERİ\*.



### Tarihsel Bilgi

Hata iletileri için hedef olarak "Return-Path" başlığının (veya **MAIL** komutundaki zarf dönüş yolu adresinin) kullanımını yalanlar görünen RFC 822'deki metin Genel Ağ'da uygulanabilir değildir. Dönüş yolu adresi (Return-path içine kopyalanmış olanı), teslimat hatalarını içeren hata iletilerinin hedefi olarak kullanılmalıdır \*ZORUNLU\*.

Özellikle:

- SMTP'den bir "başka yere" ağgeçidi olan bir konağın, bu "başka yer" aktarımının Genel Ağ alan adreslerini kullanıp zarf göndericisi adresini de ayrıca sağladığı bilinmedikçe bir dönüş yolu başlığı yerleştirmesi gerekir \*ÖNERİ\*.
- bir "başka yerden" SMTP'ye ağgeçidi olan bir konak, iletide mevcut bir dönüş yolu başlığı varsa silmeli ve bilgiyi ya SMTP zarfına kopyalamalı ya da SMTP zarfındaki **MAIL** komutunun dönüş yolu argümanını oluşturacak diğer aktarım sisteminin zarfındaki mevcut bilgiyle biraraya getirmelidir \*ÖNERİ\*.

Sunucu, posta verisi sonu belirtecini izleyen işlemlerin sadece kısmen başarılı olduğu durumlarda özel muamele yapmalıdır. Bu, bir miktar alıcı ve posta verisi kabul edildikten sonra SMTP sunucunun posta verisini alıcıların tamamına olmasa bile, bir kısmına başarıyla teslim edebileceğini saptarsa olur. Bu durumlarda, **DATA** komutuna OK yanıtı verilmelidir \*ZORUNLU\*. Bununla birlikte, SMTP sunucusu iletinin oluşturucusuna bir "teslim edilemeyen posta" uyarı iletisi oluşturup göndermesi gerekir \*ZORUNLU\*.

Başarısız olunmuş her alıcı için ya ayrı ayrı uyarı iletileri ya da bunları listeleyen tek bir uyarı iletisi gönderilmelidir \*ZORUNLU\*. İşlemin gönderici açısından ekonomik olması için mümkün olduğunca ikincisi tercih edilir. Tüm teslim edilemeyen posta uyarı iletileri **Röleme** (sayfa: 19) bölümünde açıklandığı gibi boş dönüş yollu **MAIL** komutu kullanılarak gönderilir (artık kullanılmayan **SEND**, **SOML** veya **SAML** komutlarının işleme sokulmasının sonucu olsalar bile).

Zaman damgası ve dönüş yolu satırları biçimsel olarak şöyle tanımlanır:

Dönüş-yolu-satırı = "Return-Path:" KBOŞ Dönüş-yolu <CRLF>

```
Zaman-damgası-satırı = "Received:" KBOŞ Damga <CRLF>
```

Damga = Kimden-alanı Tarafından-alanı İstemlik-bilgi ";" KBOŞ tarih-saat

```
; buradaki "tarih-saat" [32]'de açıklandığı gibidir.  
; fakat "atıl-" biçimler, özellikle iki haneli yıllar  
; SMTP'de yasaklanmıştır ve kullanılmamalıdır *ZORUNLU*.
```

Kimden- alanı = "FROM" KBOŞ Genişletilmiş- alan AKBOŞ

Tarafından-alanı = "BY" KBOŞ Genişletilmiş-alan AKBOŞ

```
Genişletilmiş-alan = Alan /
                    ( Alan KBOŞ "(" TCP-bilgisi ")" ) /
                    ( IP-kodlu-ad KBOŞ "(" TCP-bilgisi ")" )
```

```
TCP-bilgisi = IP-kodlu-ad / ( Alan KBOŞ IP-kodlu-adı )
; Bilgi sunucu tarafından TCP bağlantısından üretilir,
; istemci EHLO komutundan değil.
```

İstemlik-bilgi = [Üzerinden] [İle] [Kimlik] [İçin]

Üzerinden = "VIA" KBOŞ Bağ AKBOŞ

```
ile = "WITH" KBOŞ Protokol AKBOŞ
```

Kimlik = "ID" KBOŞ Dizge / İleti-kimliği AKBOŞ

İçin = "FOR" KBOŞ 1\*( Yol / Posta-kutusu ) AKBOŞ

$\text{Bağ} = \text{"TCP"} / \text{Ek-Bağ}$

$$E_{k-\text{Bağ}} = A_{\text{tom}}$$

```
; Bařlarla ilgili ek standart isimler Genel Ađ Atanmıř
; Numaralar Yetkilisi (IANA) tarafından kayıt altına
; alınır. SMTP sunucularının kayıtdıřı isimler kullanmaması
; gerekir *ÖNERİ*. "Üzerinden" deęeri asıl olarak,
; Genel Ađ dıřı aktarımlarla ilgilidir.
```

```
Protokol = "ESMTP" / "SMTP" / Ek-Protokol
```

Ek-Protokol = Atom

```
; Protokollerle ilgili ek standart isimler Genel Ağ Atanmış
; Numaralar Yetkilisi (IANA) tarafından kayıt altına
; alınır. SMTP sunucularının kayıtdışı isimler
; kullanmaması gerekir *ÖNERİ*.
```

#### 4.5. Gerçeklenimle İlgili Ek Hususlar



#### 4.5.1. Asgari Gerçeklenim

SMTP'yi tüm alıcılar için çalışır kılmak için, aşağıdaki asgari gerçeklenim gereklidir. Aşağıdaki komutların bu belirtimle uyumlu olmak için desteklenmesi gerekir **\*ZORUNLU\***.

```
EHLO
HELO
MAIL
RCPT
DATA
RSET
NOOP
QUIT
VRFY
```

Posta röleleme ve teslimatını destekleyen bir SMTP sunucusu içeren her sistemin harf büyüklüğüne duyarsız bir yerel isim olarak "postmaster" adına ayrılmış bir posta kutusunu desteklemesi gerekir **\*ZORUNLU\***. Eğer sunucu bağlantı açılışında (*Oturum İklendirme* (sayfa: 13) bölümünde açıklandığı gibi) daima 554 döndürüyorsa, bu postmaster adresi mutlaka gerekli değildir. Postmaster için posta kabul etme gereksinimi, SMTP sunucusunun posta hizmeti verdiği her alan adı için bir postmaster posta kutusu belirtilen **RCPT** komutları ile "**RCPT**TO:<Postmaster>" şeklindeki (alan belirtilmeksizin) özel durumun desteklenmesi gerektiği **\*ZORUNLU\***, anlamına gelir.

SMTP sistemlerinin, Genel Ağ üzerindeki herhangi bir sistemden postmaster'a doğrudan posta kabul edilmesi için makul her türlü çabayı göstereceği umulur. Bazı uç durumlarda, örneğin, bir hizmet reddi saldırısı veya diğer güvenliği kırma saldırılarının olduğu durumlarda, bir SMTP sunucusu postmaster'a gelen postayı engelleyebilir. Bununla birlikte, bu tür saldırıların bir parçası olmayan iletilerin de engellenmemesi için böyle düzenlemelerin kapsamı oldukça dar tutulmalıdır **\*ÖNERİ\***.

#### 4.5.2. Şeffaflık

Veri şeffaflığı için gerekli bazı önlemleri almaksızın "<CRLF> .<CRLF>" karakter dizisi posta metnini bitirir ve kullanıcı tarafından gönderilemez. Genelde, kullanıcıların bazı "yasaklanmış" dizilimlerden haberleri yoktur. Tüm kullanıcılarca oluşturulan metinlerin şeffaf olarak aktarılabilmesini mümkün kılmak için şu yöntemler kullanılır:

- Posta metninin bir satırını göndermeden önce, SMTP istemcisi satırın ilk karakterine bakar. Bir nokta ise, onun yanına, satırın başına bir nokta daha konur.
- SMTP sunucusu posta metninin bir satırını aldığı anda satıra bakar. Satırın tamamı tek bir noktadan oluşmuşsa, bu satır posta sonu belirtici olarak ele alınır. Eğer ilk karakter bir nokta olduğu halde satırın devamında başka karakterler varsa ilk karakter silinir.

Posta verisi, 128 ASCII karakterinin herhangi birini içerebilir. Boşluklar, dikey ve yatay sekmeler ile diğer kontrol karakterleri de dahil olmak üzere tüm karakterler alıcının posta kutusuna (bir yoruma konu edilmeksizin) teslim edilmek içindir. Eğer aktarım kanalı veri akımını 8 bitlik baytlarla (sekizli) sağlıyorsa, 7 bitlik ASCII kodları sekizlilerde sağa yanaştırılıp en anlamlı bitleri sıfır yapılarak iletilirler. Bir röleleme işlevi sunan SMTP sistemlerinde bu durumlar *Röleleme* (sayfa: 19) bölümünde özellikle ele alınmıştır.

Bazı sistemlerde veriyi alınıp saklanmış gibi dönüştürmek gerekli olabilir. Yerel karakter kümesi olarak ASCII'den farklı bir karakter kümesi kullanan, veriyi dizgeler halinde değil kayıtlar halinde saklayan veya posta kutularının içinde araç olarak özel karakter dizilimleri kullanan konaklar için bu gerekli olabilir. Eğer böyle dönüşümler gereklyse, bunlar geri alınabilir olmalıdır **\*ZORUNLU\***; özellikle de, rölelenen postaya uygulanmışsa.

#### 4.5.3. Boyutlar ve Zamanaşırımları



#### 4.5.3.1. Boyut sınırları ve asgari değerler

Azami ve/veya asgari boyutları olması gereken bazı nesneler vardır. Her gerçekleşimin nesneleri en azından bu boyutlarda almasının mümkün olması gerekir **\*ZORUNLU\***. Bu boyutlardan daha büyük nesnelerden olabildiğince kaçınılmalıdır **\*ÖNERİ\***. Bununla birlikte, kodlanmış X.400 adresleri [16] gibi sıklıkla daha geniş nesneler gerektiren bazı Genel Ağ posta oluşumları vardır: istemciler bunları aktarmaya çalışabilirler **\*SEÇİMLİK\***, fakat onları işleme alamıyacak bir sunucu tarafından reddedilmelerine karşı da hazırlıklı olmalıdırlar **\*ZORUNLU\***. Azami genişleme olasılığı için, bu nesnelerin uzunluğu ile ilgili bir sınır koymayan gerçekleşim teknikleri kullanılmalıdır.

##### yerel-kısım

Bir kullanıcı isminin veya bir yerel-kısım'ın toplam uzunluğu en çok 64 karakter olabilir.

##### alan

Bir alan isminin veya numarasının toplam uzunluğu en çok 255 karakter olabilir.

##### yol

Bir dönüş veya sevk yolunun toplam uzunluğu en çok 256 karakter olabilir (noktalama imlerini ve bileşen ayrıçalarını içererek).

##### komut satırı

Komut sözcüğünü ve `<CRLF>`'yi içererek bir komut satırının toplam uzunluğu en çok 512 karakter olabilir. Bu sınırı arttırmak için SMTP eklentileri kullanılabilir.

##### yanıt satırı

Yanıt kodunu ve `<CRLF>`'yi içererek bir yanıt satırının toplam uzunluğu en çok 512 karakter olabilir. Daha fazla bilgi çok satırlı yanıtlarla taşınabilir.

##### metin satırı

`<CRLF>`'yi içererek bir metin satırının toplam uzunluğu en çok 1000 karakter olabilir (şeffaflık açısından uçlardaki nokta tekrarları sayılmaz). Bu miktar SMTP Hizmet Eklentileri kullanarak artırılabilir.

##### ileti içeriği

Bir ileti içeriğinin (ileti başlıklarını da içererek ileti gövdesinin) toplam uzunluğu hiç olmazsa (bari, en azından) [at least] 64K sekizli olmalıdır **\*ZORUNLU\***. Çoklu ortam postası Genel Ağ standartlarına [12] girdiğinden beri, Genel Ağ'da ileti uzunlukları çarpıcı biçimde büyümektedir. Bu bakımdan ileti boyu sınırlamalarından mümkün olduğunca kaçınılmalıdır. Sınırlamaları zorlamak isteyen SMTP sunucu sistemleri "BOYUT" hizmet eklentisini [18] gerçeklemedir **\*ÖNERİ\***.

##### alıcılar tamponu

Tamponlanması gereken alıcıların toplam sayısı en az 100 olabilir. 100 **RCPT** komutundan daha azından sonraki alıcılar için iletilerin reddedilmesi bu belirtim uylmadığı anlamına gelir. Genelde prensip olarak, röleleyen SMTP sunucuları için zorunlu olarak **\*ZORUNLU\*** ve teslimat SMTP sunucuları için öneri olarak **\*ÖNERİ\***, bir iletinin alıcılarının toplam sayısına bağlı olarak reddildiğini ima eden ileti başlıkları üzerinde doğrulama denemeleri yapılmaması gerekir. Alıcı sayısına bir sınır koyan bir sunucu alıcıları sıralı bir tarzda ele almalı, örneğin, sınırı aşan adresleri reddetmeli ama evvelce kabul edilmiş adresleri sonraya kalmış gibi reddetme yoluna gitmemelidir **\*ZORUNLU\***. Eğer sunucu tek bir iletide 100 alıcıdan fazlasını kabul etmeyi tavsatiyorsa, istemci, 100'den fazla **RCPT** komutu gerektiren bir iletinin teslimatını 100 alıcılık iletiler halinde yapmak için hazırlıklı olmalıdır.

Bu sınırların aşılmasından dolayı oluşan hatalar yanıt kodları kullanılarak raporlanabilir. Bazı yanıt kodu örnekleri:

```
500 Satır çok uzun.
```

veya

501 Yol çok uzun

veya

452 Alıcılar çok fazla (aşağıya bakınız)

ya da

552 Posta verisi çok fazla.

RFC 821 [30] bir hatayı yanlış listelemiştir: **RCPT** komutlarının miktarıyla ilgili gerçeklenim sınırından dolayı yetersiz kalan bir SMTP sunucusunun hatayı ("Alıcılar çok fazla") '552 yanıt koduyla' bildireceği belirtilmiştir. Doğrusu '452 yanıt koduyla' olacaktır. İstemciler bu durumda bir 552 yanıt kodunu kalıcı değil geçici bir hata durumu olarak ele almalıdırlar \*ÖNERİ\*, başarısızlık durumunda aşağıdaki mantık yürütülür.

Belirtimle uyumlu bir SMTP sunucusu bu durumu saptadığında, alıcılar tamponunda en azından 100 başarılı **RCPT** komutu var demektir. Sunucu iletiyi kabul edebilecekse, en azından 100 adres SMTP istemcisinin kuyruğundan silinmiş olacaktır. 452 yanıtı almış adresleri istemci yeniden aktarmaya çalışırsa, bunların en azından 100 tanesi SMTP sunucusunun alıcılar tamponuna sığabilecektir. Teslim edilecek ne varsa yeniden her aktarma çabasında bu alıcıların en azından 100 tanesinden kurtulmak mümkün olacaktır.

Bir SMTP sunucusunun **RCPT** komutlarının sayısına bağlı bir gerçeklenim sınırı varsa ve bu sınıra ulaşılmışsa, sunucu 452 yanıt kodunu kullanmalıdır \*ZORUNLU\* (fakat, istemci yukarıda belirtildiği gibi bir 552 yanıtına karşı da hazırlıklı olmalıdır \*ÖNERİ\*). Eğer sunucu **RCPT** komutlarının sayısı ile ilgili kural olarak konmuş bir sınırlamaya (gerçeklenimin desteklediğinden az) göre hareket ediyorsa bir 5XX yanıt kodu da kullanabilir \*SEÇİMLİK\*. Eğer belli bir ileti gövdesi çok sayıda posta aktarımı ile gönderilmiş olsa bile o ileti için bir toplam alıcı sayısı sınırı uygulanabiliyorsa, böyle bir sınırlama en iyisi olurdu.

#### 4.5.3.2. Zamanaşimleri

Her SMTP istemcisi bir zamanaşımı mekanizması sağlamalıdır \*ZORUNLU\*. Bu mekanizma posta aktarımının tamamına bir şekilde uygulanabilen bir zamanaşımı değil her komut için ayrı ayrı uygulanabilen zamanaşimleri kullanmalıdır \*ZORUNLU\*. Zamanaşimleri, tercihan SMTP kodunu yeniden derlemek gerekmeksizin, yeniden yapılandırılabilir olmalıdır \*ÖNERİ\*. Bunu gerçeklemek için, her SMTP komutu ve her veri aktarım tamponu için bir zamanlayıcı tahsis edilir. Sonuncusu, aktarımın bütününe kapsayan zamanaşımının ister istemez iletinin boyutuyla orantılı olduğu anlamına gelir.

Meşgul posta röleme konakları ile gerçekleştirilen kapsamlı deneyimlere dayanarak, komut başına asgari zamanaşımı değerleri şöyle olmalıdır \*ÖNERİ\*:

İlk 220 İletisi: 5 dakika

Bir SMTP istemci sürecinin, başarısız bir TCP bağlantısı ile ilk 220 karşılama iletisinin gecikmesi arasındaki farkı ayırmaya ihtiyacı vardır. Çoğu SMTP sunucusu bir TCP bağlantısını kabul eder ama sistem yükü başka postaları da işleme almayı mümkün kılana kadar 220 iletisinin teslimatını geciktirir.

**MAIL** Komutu: 5 dakika

**RCPT** Komutu: 5 dakika

Postalama listelerinin ve takma adların işlenmesi iletinin kabulü sonrasında ertelenmiyorsa, daha uzun bir zamanaşımı gerekir.

**DATA** ilklendirme: 2 dakika

Bu, **DATA** komutuna "354 Girdiyi Başlat" yanıtı beklenirken geçen süredir.

Veri Bloku: 3 dakika

Veri kısım kısım aktarılırken her TCP GÖNDER çağrısının tamamlanması için geçmesi beklenecek süredir.

**DATA** sonlandırma: 10 dakika.

Bu, "250 OK" yanıtı beklenirken geçen süredir. Alıcı ileti verisini sonlandıran son noktayı aldığı anda, genellikle iletinin kullanıcının posta kutusuna teslimini gerçekleştirir. Bu noktada taklit bir zamanaşımı, ileti gönderilmiş ve sunucu teslimatın sorumluluğunu zaten kabul etmiş olduğundan çok yıkıcı olurdu ve genelde aynı iletinin çok sayıda kopyasının teslimi ile sonuçlanırdı. Bu konu ile ilgili olarak [Güvenilir Teslimat ve Eposta Yanıtları](#) (sayfa: 45) bölümüne de bakınız.

Bir SMTP sunucusu göndericiden gelecek bir sonraki komutu en az 5 dakika beklemelidir \*ÖNERİ\*.

#### 4.5.4. Yanıt Stratejileri

Bir konak SMTP gerçekleniminin bilinen yapısı kullanıcı posta kutuları, gelip geçen iletileri kuyruğa almak için bir veya daha fazla alan ile posta alımı ve gönderimi için çalışan bir veya daha fazla artalan sürecinden oluşur. Kesin yapı konak üzerindeki kullanıcıların ihtiyaçları ile konak tarafından desteklenen posta listelerinin boyutlarına ve sayısına bağlı olarak değişir. Özellikle yüksek trafik seviyelerini destekleyen postacılar için yardımcı olduğu kanıtlanmış çeşitli eniyilemeleri açıklayacağız.

Her kuyruklama stratejisi her türlü etkinliğin zamanaşımını her komuta özel olarak ele almalıdır \*ZORUNLU\*. Bir kuyruklama stratejisi ne olursa olsun hata iletilerine yanıt olarak hata iletileri göndermemelidir \*ZORUNLU\*.

##### 4.5.4.1. Gönderme Stratejisi

Bir SMTP istemcisinin genel modeli giden postayı aktarmaya çalışan bir veya daha fazla süreçten oluşur. Ortalama bir sistemde, bir iletiyi oluşturan program, hemen aktarılamayıp kuyruğa alınıp belirli aralıklarla tekrar gönderilmeye çalışılmıyken \*ZORUNLU\*, giden postanın yeni bir parçasının hemen dikkate alınmasını talep eden bir yönteme sahiptir. Bir posta kuyruğu girdisi iletinin kendisinden başka zarf bilgisini de içerecektir.

Belli bir hedef için bir çaba başarısız olduktan sonra çabayı yinelemek için bir süre beklenmelidir \*ZORUNLU\*. Genelde, yineleme aralığı en azından 30 dakika olmalıdır \*ÖNERİ\*; bununla birlikte, SMTP istemcisi teslimat yapılmaması için sebep saptayabildiği zaman, daha karmaşık ve değişken stratejilerin yararı olacaktır.

İleti aktarılan veya gönderici vazgeçene kadar yineleme devam eder; vazgeçme süresinin genelde en azından 4–5 gün olması gerekir. Yineleme algoritmasının parametreleri yapılandırılabilir olmalıdır \*ZORUNLU\*.

Bir istemci kuyruklu posta öğelerini salt tekrar göndermeye çalışmaktan çok, ulaşamadığı konakların ve ilgili bağlantı zamanaşımının bir listesini tutması gerekir \*ÖNERİ\*.

Deneyimler bu başarısızlıkların genellikle geçici olduğunu (hedef sistem ya da bağlantı çökmüştür), kuyruktaki iletiyi göndermek için ilk saatte iki, daha sonra ise iki veya üç saatte bir bağlantı kurmaya çalışmak şeklinde bir kuralın lehte olacağını göstermiştir.

SMTP istemcisi, SMTP sunucusu ile anlaşarak kuyruklama gecikmesini kısaltabilir. Örneğin, posta belli bir adresten alınmışsa, posta onu hemen gönderebilecek konak için kuyruğa alınmış gibi ele alınabilir. Bu prensibin uygulaması, çoğu durumda, ETRN [9] gibi apaçık bir "kuyruktakileri hemen gönder" işlevi için gereksinimi ortadan kaldırabilir.

Strateji, çok sayıda adresin her konak başına özkaynak kullanımını (teslimat zamanı gibi) eniyileme gereğinin bir sonucu olarak böyle değiştirilmiş olabilir.

Bir SMTP istemcisinin erişilemeyen hedef konakların her biri için dev bir ileti kuyruğu olabilir. Bu iletilerin tümü her yineleme döngüsünde yineleniyorsa, Genel Ağ'a haddinden fazla yük bindirebilir ve gönderen sistem uzun bir süre boyunca engellenebilir. Bir SMTP istemcisinin, bir teslimat çabasının başarısız olacağını, aynı konak için kuyruklanmış iletilerin düzinelerce hatta yüzlercesinin tekrar tekrar yinelenmesi halinde bağlantı başına

bırakın bir kaç dakikalık sadece tek bir dakikalık zamanaşımının bile çok büyük bir gecikmeyle sonuçlanacağını saptayabileceğine dikkat ediniz.

Aynı zamanda, SMTP istemcileri sunuculardan gelen olumsuz yanıtları arabelleğe alırken büyük dikkat sarfetmelidirler \*ÖNERİ\*. Çok uç bir durumda, aynı SMTP bağlantısı sırasında **EHLO** komutu defalarca kullanılmışsa, sunucudan farklı yanıtlar dönebilir. Daha manidar olarak, **MAIL** komutuna verilen **5yz** yanıtları arabelleğe alınmamalıdır \*ZORUNLU\*.

Bir posta iletisi çok sayıda alıcıya teslim edilecekse ve bunlardan bir kısmı tek bir SMTP sunucusundaysa, bu sunucuya iletinin sadece tek bir kopyası aktarılmalıdır \*ÖNERİ\*. Yani, SMTP istemcisi böyle bir komut dizisi yerine:

**MAIL, RCPT, DATA, ..., MAIL, RCPT, DATA**

böyle bir komut dizisini kullanmalıdır:

**MAIL, RCPT, RCPT,... RCPT, DATA.**

Yine de, çok fazla adres varsa, **MAIL** komutu başına **RCPT** komutu sayısına bir sınırlama getirilebilir \*SEÇİMLİK\*. Bu verimli özelliğin gerçekleşmesi kesinlikle önerilmektedir.

Benzer şekilde, teslimatlarda tam zamanlılığın sağlanması için, SMTP istemcisi aynı anda çok sayıda giden posta aktarımını destekleyebilir \*SEÇİMLİK\*. Bununla birlikte, bütün kaynakların postaya tahsis edilmesinden korunmayı sağlayacak bir sınırlama uygun olabilir.

#### 4.5.4.2. Alım Stratejisi

SMTP sunucusu her zaman SMTP portunu dinlemeyi sürdürmeye çalışmalıdır \*ÖNERİ\*. Bu, SMTP için gelen çok sayıda TCP bağlantısının desteklenmesini gerektirir. Bazı sınırlar konulabilir \*SEÇİMLİK\*, fakat aynı anda birden fazla SMTP aktarımını kabul edemeyen sunucular bu belirtimin amacıyla uyumlu değildirler.

Yukarıda bahsedildiği gibi SMTP sunucu postayı belli bir konak adresinden almaktayken bu konak adresi için bekleyen bir postayı yineleyebilmek için kendi SMTP kuyruklama mekanizmasını etkinleştirebilir.

#### 4.5.5. Dönüş yolu boş olan iletiler

Mevcut standartlardan başka standart adayı belirtilmelerin de gerektirdiği boş dönüş yolu ile gönderilecek çeşitli uyarı türleri vardır. Bunlar arasında [Röleleme](#) (sayfa: 19) bölümünde açıklanan "teslimatı yapılamayan posta" uyarısı iletisi, Teslimat Durum Bildirimleri (Delivery Status Notifications – DSN'ler) [24] ve İleti Elverişlilik Bildirimleri (Message Disposition Notifications – MDN'ler) [10] başlıcalarıdır. Tüm bu ileti çeşitleri önceki bir posta iletisi hakkında birer bildirimdirler ve önceki posta iletisinin dönüş yoluna gönderilirler. (Eğer böyle bir bildirim iletisi teslim edilemezse, bu, bildirim iletisinin adreslendiği konağın posta sistemi ile ilgili bir sorunun olduğunu gösterir. Bu sebeple bazı konaklarda MTA, böyle başarısız bildirim iletilerinin sevkedileceği, posta sistemi ile ilgili sorunları giderebilen birilerine, örneğin, **postmaster** takma adı kullanılarak, yönlendirilmiş bir posta kutusuna sahiptir. )

Tüm diğer ileti türleri (yani, boş bir dönüş yoluna sahip olması standartlaşma aşamalarındaki bir RFC tarafından gerekli görülmemiş her ileti), boş olmayan geçerli bir dönüş yolu ile gönderilmelidir \*ÖNERİ\*.

Özdevinimleştirilmiş eposta işlemcilerinin gerçeklenimcileri boş dönüş yolu içeren ileti çeşitlerini işleme sokarken dikkatli olmalı, özellikle de böyle sistemler boş dönüş yolu içeren iletileri yanıtlamamalıdır \*ÖNERİ\*.

## 5. Adres Çözümleme ve Posta Yönetimi

Bir SMTP istemcisi işlenmek üzere ([Alanlar](#) (sayfa: 19) ve [Röleleme](#) (sayfa: 19) bölümünde açıklandığı gibi) posta gönderebileceği bir alanı sözdizimsel olarak tanımladığında, alan adını çözümlemek için bir DNS sorgusu

yapmalıdır \*ZORUNLU\* [22]. İsimlerin tam nitelikli alan adları (FQDN) olması beklenir: kısmi isimlerden veya yerel takma adlardan tam nitelikli alan adlarını elde etme mekanizmaları bu belirtimin kapsamı dışında olup, sorunlarla dolu bir geçmişten dolayı genellikle tavsiye edilmez. Sorgu öncelikle isimle ilişkili bir **MX** kaydı bulmak için yapılır. Eğer bunun yerine bir **CNAME** kaydı bulunursa, sonuçlanan isim bir ilk isimmiş gibi işleme sokulur. Eğer hiç **MX** kaydı bulunmaz da bir **A** kaydı bulunursa, **A** kaydı 0 tercihli örtük bir **MX** kaydı ile ilişkililmiş gibi ele alınır. Belirtilen isim için bir veya daha fazla **MX** kaydı bulunursa, **MX** kayıtlarında aynı isim belirtilmiş olmadıkça, SMTP sistemlerinin bu alan adıyla bir **A** kaydını ilişkilendirmemeleri gerekir \*ZORUNLU\*; yukarıdaki "örtük **MX**" kuralı sadece mevcut bir **MX** kaydının bulunmaması durumunda uygulanır. Eğer **MX** kayıtları varsa, fakat hiçbirini kullanışlı değilse, bu durum bir hata olarak raporlanmalıdır \*ZORUNLU\*.

Sorgu başarılı olabilir ve çok sayıda **MX** kaydı, çok evlilik veya her ikisinin de varlığından dolayı tek bir adres yerine birbirlerinin yerlerine kullanılabilecek birden fazla adres içeren bir liste ile eşleşme sağlanabilir. Güvenilir posta aktarımı sağlamak için SMTP istemcisi, başarılı bir teslimat gerçekleştirene kadar bu listedeki her adresi deneyebilmelidir (hatta tekrar tekrar) \*ZORUNLU\*. Yine de, denenebilecek adres sayısı ile ilgili yapılandırılabilir bir sınır konulabilir \*SEÇİMLİK\*. Ancak ne olursa olsun, SMTP istemcisinin en azından iki adresi denemesi gerekir \*ÖNERİ\*.

Konak adreslerinin sıralanmasında iki tür bilgi kullanılır: çoklu **MX** kaydı ve çok evli konaklar.

Çoklu **MX** kaydı, sıralı erişilme gereğini \*ZORUNLU\* belirten bir tercih gösterimi içerir (aşağıya bakınız). Küçük sayılar büyüklere göre öncelik belirtir. Aynı tercihe sahip birden fazla hedef varsa ve birinin tercih edilmesi için aleni bir sebep (örneğin, kolay erişilen bir adresin saptanması) yoksa, gönderici SMTP sisteminin yükü çok sayıda posta aktarımcısı arasında onlara özel bir örgütlenime göre dağıtması gerekir \*ZORUNLU\*.

Hedef konak (şüphesiz, tercihli bir **MX** kaydından alınmış olarak) çok evli olabilir, yani, alan adı çözümleyici aynı konak için hepsi birbirinin yerine kullanılabilen birden fazla IP adresi döndürebilir. Gerektiğinde listenin azalan tercihli sıralamaya tabi tutulması alan adı çözümleme arayüzünün sorumluluğundadır. SMTP listeyi sunulduğu sıraya göre denemelidir \*ZORUNLU\*.

Birbirlerinin yerine kullanılabilen çok sayıda adresi deneyebilme yeterliliğinin gerekliliğinden dolayı, bazı kurulumlar bu tür adres kullanımını sınırlamak hatta tamamen iptal etmek isteyebilirler. Bir gönderici çok evli bir konağın farklı adreslerini kullanarak gönderiyi yinelemeli midir sorusu tartışmalıdır. Çok sayıda adres kullanımını savunanların ana argümanı zamanında teslimat olasılığını ve hatta bazan da herhangi bir teslimat olasılığını azamileştirmesidir; karşıtların argümanı ise, gereğinden fazla özkaynak kullanımına yolaçmasıdır. *Gönderme Stratejisi* (sayfa: 43) bölümünde açıklanan gönderi stratejisi kullanılarak ek olarak özkaynak kullanımının da kesin olarak saptanabileceğini dikkatinize sunarız.

Bir SMTP sunucusu, hedefi, tasarlanmış bir posta aktarımcısı (**MX**) olan bir ileti alırsa, iletiyi röleleyebilir \*SEÇİMLİK\* (mumtemelen **MAIL FROM** ve/veya **RCPT TO** adreslerini yeniden yazdıktan sonra), iletinin son teslimatını yapabilir \*SEÇİMLİK\* ya da SMTP dışı bir aktarım mekanizmasını kullanarak elden çıkarabilir \*SEÇİMLİK\*. Tabii ki, sonuncuya dahil olanların hiçbir **MX** kayıtları listesinin bir şekilde incelenmesini gerektirmez.

Eğer iletinin, adresler yeniden yazılmaksızın rölelenmesi gerektiği saptanırsa, teslimat adaylarını saptamak için **MX** kayıtlarının sıralanması gerekir \*ZORUNLU\*. En küçük numaralı kayıt en tercihli kayıt olmak üzere kayıtlar önce tercih sırasına sokulur. Röleleme konağı daha sonra bu listeyi posta aktarımı yapılabilecek isim ve adresleri saptamak için inceler. Bir eşleşen kayıt bulunursa, tercih seviyesindeki ve daha yüksek numaralı tercihlere sahip tüm kayıtlar gözden çıkarılmalıdır \*ZORUNLU\*. Bu noktada hiçbir kayıt kalmazsa, bu bir hata durumudur ve ileti teslim edilemediği gerekçesiyle geri gönderilmelidir \*ZORUNLU\*. Eğer elde kayıt kalırsa, bunlar yukarıda açıklandığı gibi en tercihlisinden başlanarak denenmelidir \*ÖNERİ\*.

## 6. Sorun Saptama ve Giderme

## 6.1. Güvenilir Teslimat ve Eposta Yanıtları

Alıcı SMTP bir posta parçasını kabul etmekle (**DATA** komutuna yanıt olarak bir "250 OK" iletisi göndererek), iletinin teslimat veya röleme sorumluluğunu kabul etmiş olur. Bu sorumluluğu ciddiye alması gerekir. İletiyi konağın sonradan bozulması veya önceden kestirilebilir kaynak kıtlığı gibi sudan sebeplerle kaybetmemelidir \*ZORUNLU\*.

Bir iletinin kabulü sonrası bir teslimat başarısızlığı olursa, alıcı SMTP'nin bir bildirim iletisi oluşturup postalaması gerekir \*ZORUNLU\*. Bu bildirim zarfta boş ("**<>**") dönüş yolu kullanılarak gönderilmelidir \*ZORUNLU\*. Bu bildirimin alıcısının adresi zarf dönüş yolundan (veya **Return-Path**: satırından) elde edilmelidir \*ZORUNLU\*. Ancak, bu adres boşsa ("**<>**"), alıcı SMTP bir bildirim göndermemelidir \*ZORUNLU\*. Açıkça, bu bölümdeki hiçbir şey günlük tutma ile ilgili yerel kararları (alıcı SMTP ile aynı sistem ortamının parçası olarak) yasaklayamaz, yasaklamamalıdır da, aksi takdirde boş adres olayları hakkında bilgi yerel olarak aktarılır, eğer istenen buysa. Eğer adres açık bir kaynak rotası ise, son sekmesine indirgenmelidir \*ZORUNLU\*.

Örneğin,

```
MAIL FROM:<@a,@b:kullanıcı@d>
```

ile gelen bir ileti için bir hata bildirimi gönderilmesi gerektiğini varsayalım. Bildirim iletisinin

```
RCPT TO:<kullanıcı@d>
```

kullanılarak gönderilmesi gerekir \*ZORUNLU\*. İleti SMTP tarafından kabul edildikten sonraki bazı teslimat başarısızlıkları kaçınılmaz olacaktır. Örneğin, **RCPT** komutlarındaki tüm teslimat adreslerinin doğrulanması alan SMTP sunucusu için imkansız olabilir; bunun sebebi, bir "yazılımsal" alan adı sistemi hatası olabileceği gibi hedefin bir posta listesi olması (**RCPT** ilk açıklamalarına bakınız) veya sunucunun bir röle olarak davranmasından dolayı teslimat sistemine doğrudan erişilememesi olabilir.

Zamanaşımının bir sonucu olarak yinelenmiş iletilerin alınmasından kaçınmak için alıcı SMTP, son **<CRLF> . <CRLF>** veri sonu belirtecine yanıt için gereken süreyi en aza indirecek çalışmayı yapmalıdır \*ZORUNLU\*. Bu sorunun daha ayrıntılı bir açıklaması için RFC 1047'ye [28] bakınız.

## 6.2. Döngü Algılama

Bir iletideki "Received:" başlıklarının basitçe sayılması her zaman en iyisi olmasa da posta sistemlerinde döngülerin saptanması için etkin bir yoldur. Bu tekniği kullanan SMTP sunucuları en azından 100 "Received:" girdilik büyükçe bir red eşiği kullanmalıdırlar \*ÖNERİ\*. Hangi mekanizma kullanılırsa kullanılsın, sunucular gereksiz döngüleri algılamak ve durdurmak için hazırlıklı olmalıdırlar \*ZORUNLU\*.

## 6.3. Düzensizliklerin Giderilmesi

Şanssızlık eseri, Genel Ağ posta protokolleri ile ilgili çeşitlenmeler, yaratıcı yorumlar ve açıkça ihlaller ortaya çıkar; bazıları bunların o kadar sık görülmediğini söyler. İyi bir SMTP alıcısı veya rölesi, bozuk bir iletiyi red mi etmeli, hiçbir değişiklik yapmadan geçirmeye mi çalışmalı yoksa başarılı bir teslimat veya yanıt şansını arttırmak için onarmaya mı çalışmalı tartışmaları yapısal ağ postasının ortaya çıkışı ile başladı ve bitecek gibi de görünmemektedir. Red yanlıları onarmaya çalışmanın her zaman yeterli olmadığını ve hatalı iletilerin reddedilmesinin yazılımın tamirinde tek çözüm olduğunu iddia ederler. "Tamir et" veya "ne olursa olsun teslim et" yanlıları ise kullanıcıların postanın eğer olabilirse iletilmesi gerektiğini düşündüklerini ve bu yönde önemli piyasa baskısı olduğunu söyleyip karşı çıkarlar. Uygulamada, bu piyasa baskıları belirli satıcılar için asıl geliştiricilerin tercihlerine bakmaksızın, standartlara kesinlikle uymaya çalışmaktan daha önemli olabilir.

Hatalı biçimlenmiş iletilerle ilgili sorunlar ayrıık posta okuma protokollerinin [3, 26, 5, 21] ortaya çıkışı ile iyice arttı. Bu protokoller SMTP'yi postalama protokolü olarak ve SMTP sunucularını da bu istemci konaklar (sıkça



ama aralıklarla Genel Ağ'a bağlanan konaklar) için röleleme sistemleri olarak kullanmayı teşvik etti. Geçmişte baktığımızda, bu istemci makinelerin çoğunun SMTP tarafından varsayılan bazı bilgilere ve mekanizmalara (ve tabii, posta biçimleme protokolüne [7]) ihtiyaç duyduklarını görürüz. Bazıları zamanı yeterince takip edemedi; bazıları zaman dilimleri kavramından habersizdi; bazıları hala isim ve adreslerini tanımlayamıyor; ve, tabii ki hiçbir RFC 822'nin kimlik kanıtlamalı adresler kavramının dayandığı öngereklilikleri sağlayamadı.

Bu zayıf SMTP istemcilerine yanıt olarak, artık bir çok SMTP sistemi kendilerine eksik veya yanlış biçimlenmiş olarak teslim edilen iletileri tamamlamaktalar. Bu strateji, sunucu istemciyi tanıdığı anda veya kimliğini kanıtlamasını istediğinde ve aralarında ön anlaşmalar olduğunda genellikle doğru sayılır. Karşıt olarak, en büyük endişe, kullanıcı veya istemci makinesi hakkında çok az bilgisi olan veya hiç bilgisi olmayan bir röle veya teslimat SMTP sunucusu tarafından uygulanan düzeltmelerle ilgilidir.

Aşağıdaki değişiklikler işlenmekte olan bir iletiye, gerek oluşturucu gerekse SMTP'nin ilk postalama protokolü hedefi olarak kullanıldığı SMTP sunucusu tarafından uygulanabilir \*SEÇİMLİK\*.

- `message-id` alanının yokluğu halinde eklenmesi
- tarih, saat ve zaman dilimi bilgilerinin yokluğu halinde eklenmesi
- adreslerin doğru FQDN biçimine getirilmesi

Sunucunun istemci hakkında ne kadar az bilgisi olursa, bu değişiklikler o kadar az doğru olur ve düzeltmelerin yapılıp yapılmaması veya nasıl yapılması gerektiği ele alınırken daha fazla dikkat ve tutarlılık gösterilmesi gerekir. Bu değişiklikler ara röleleme işlemi yapan SMTP sunucuları tarafından uygulanmamalıdır \*ZORUNLU\*.

Her durumda, doğru bilgi sağlayarak düzgün işleyen istemciler, SMTP sunucuları tarafından düzeltmeler bakımından tercih edilirler. Tüm durumlarda, sunucular tarafından yapılan hareketlerin mutlaka belgelenmesi (izleme alanları ve/veya başlık yorumlarında) önerilir.

## 7. Güvenlik Kaygıları

### 7.1. Posta Güvenliği ve Yanıltma

SMTP postası doğal olarak güvensizdir, öyle ki ilgisiz kullanıcılar bile alıcı ve röle SMTP sunucuları ile doğrudan haşır neşir olabilirler ve saf/toy/taze bir alıcıyı başka bir yerden gelmiş gibi görünen iletiler gönderip kandırabilirler. Böyle bir iletinin "yanıltıcı" davranışının bir uzman tarafından tespit edilemeyecek şekilde oluşturulması biraz zordur, ama bilgili ve kararlı birini caydıracak kadar değil. Sonuçta, Genel Ağ posta bilgisinin artışına bağlı olarak, SMTP postasının aktarım seviyesinde doğal olarak kimlik kanıtlamalı olamayacağı veya bütünlük sınamalarının yapılamayacağı ortaya çıktı. Gerçek posta güvenliği sadece uç noktalarda ileti gövdesinin incelenmesiyle (örn, sayısal imzalar) sağlanabilir (bkz, PGP [4], S/MIME [31]).

Aktarım seviyesinde (yani, SMTP istemcisinden SMTP sunucusuna aktarımda) kimlik kanıtlaması sağlayan çeşitli protokol eklentileri ve yapılandırma seçenekleri yukarıda açıklanan geleneksel durumu biraz düzeltebilir. Yine de, dikkatle tasarlanmış bir güvenlik ortamının sorumluluğu bunlara aynı dikkatle eşlik etmedikçe, aktarım sisteminin bütünlüğüne bağlı kalmaktansa sayısal imzalı iletileri kullanan uçtan uca mekanizmalardan doğal olarak daha zayıf kalacaklardır.

Zarf dönüş yolunu ve başlık "From" alanlarını kendilerinininkinden farklı olarak doğru bir adresi gösterecek şekilde ayarlamayı kullanıcılar için daha zor hale getirme çabaları amacından epeyce saptırılmıştır: bir kullanıcı tarafından bir başkası yararına posta gönderimi veya özel bir adrese yönlendirilmesi gereken hata (veya normal) yanıtların gönderimi şeklindeki meşru uygulamaları boşa çıkarmışlardır. (Her iletiye özel olmak üzere kullanıcılarına bu alanları değiştirebilme imkanı sunan sistemler, ileti verisi içindeki gönderici alanlarının hassas bir şekilde üretilmesi için kullanıcıya bir birincil ve kalıcı posta kutusu adresi sağlamaya çalışmalıdırlar.)

Bu belirtim, sahte posta göndermeye çalışan görgüsüz bir kullanıcıya karşı küçük bir koruma sağlayacağını umarak bu faydalı işlevselliğin iptal edilmemesini savunmak dışında, SMTP ile ilgili kimlik kanıtlama konularının adresi değildir.

## 7.2. "Gizli" Kopyalar

İleti başlıklarında görünmeyen adresler bir SMTP sunucusunda **RCPT** komutlarında şu veya bu sebeple görünebilir. En çok karşılaşılan ikisi bir posta adresinin bir "liste patlatıcısı" olarak kullanımı (tek bir adres çok sayıda adres olarak çözümlenir) ile "gizli kopya" varlığıdır. Özellikle birden fazla **RCPT** komutunun varlığında ve bu mekanizmaların bazı amaçlarını da yok etmemek için, ister izleme başlıklarının parçası olarak ister bilgilendirici ya da özel eklenti başlıkları olarak, SMTP istemcileri ve sunucuları **RCPT** komutlarının argümanlarının tamamını başlıklara kopyalamamalıdır *\*ÖNERİ\**. Bu kural uygulamada sıkça ihlal edildiğinden, "bcc" kullanmayı bilen gönderici SMTP sistemleri her gizli kopyayı tek bir **RCPT** komutu içeren ayrı bir ileti aktarımında göndermeleri daha yararlıdır *\*SEÇİMLİK\**.

SMTP aktarımındaki ("zarf") ve başlıklardaki ne "dönüş" adresleri (**MAIL**, **SAML**, vs. komutlarındaki) ne de "sevk" adresleri (**RCPT** komutlarındaki) arasında doğal bir ilişki vardır. Alıcı sistemler böyle ilişkileri ortaya çıkarmaya ve teslimat için onları ileti başlıklarını değiştirmekte kullanmaya çalışmamalıdır *\*ÖNERİ\**. Güncel olan "Apparently-to" başlığı bir kasıtsız bilgi ifşasının genel kaynağı olarak bu prensibin ihlalidir ve kullanılmamalıdır *\*ÖNERİ\**.

## 7.3. **VRFY**, **EXPN** ve Güvenlik

*Adres Hatalarını Ayıklama Komutları* (sayfa: 16) bölümünde bahsedildiği gibi bağımsız bazı siteler güvenlik kaygılarıyla **VRFY** veya **EXPN** komutunu veya her ikisini de iptal etmek isteyebilirler. Yukarıda bahsedilenin doğal sonucu olarak, buna izin veren gerçeklemler aslında doğrulamadıkları halde adresleri doğrulamış gibi görünmemelidirler *\*ZORUNLU\**. Eğer bir site bu komutları güvenlik nedenleriyle iptal ederse, SMTP sunucu başarılı veya başarısız doğrulama ile karıştırılabilecek bir yanıt kodu kullanmak yerine bir 252 yanıtı döndürmelidir *\*ZORUNLU\**.

Sadece sözdizimsel olarak kontrol ettikten sonra **VRFY** komutundaki adresi içeren bir 250 yanıtı döndürmek bu kuralı ihlal eder. Şüphesiz, **VRFY** komutunu, adres geçerli olsun olmasın daima 550 yanıtı döndürerek destekleyen bir gerçeklemler de aynı uyumlulukta değildir.

Son bir kaç yıldır, posta listelerinin içeriği "spamcılar" denen kitle için bir adres bilgi kaynağı haline geldi. Liste yöneticileri listelerin kendilerini uygunsuz kullanımına karşı korumak üzere önlemler aldıkça "adres hasadı"nda **EXPN** kullanımı arttı. Gerçeklemler **EXPN** desteğini yine de sağlamalı *\*ÖNERİ\**, fakat siteler karşılıklı tavizleri dikkatle değerlendirmelidirler *\*ÖNERİ\**. Kimlik kanıtlama mekanizmaları SMTP'ye tanıtıldıkça, bazı siteler **EXPN**'yi sadece kimliğini kanıtlayan istekçilere kullanılabilir kılmayı seçebilir.

## 7.4. Duyurularda Bilgi İfşası

Karşılama yanıtlarında ya da **HELP** komutunun yanıtında sunucu türünü ve sürümünü (hatta bazan alan adını) duyurmanın hata ayıklamaya getirileri ile olası bir düşmanca saldırı için kullanışlı olabilecek bilgiyi açığa çıkarmasının götürüleri arasındaki ödünleşimler hakkında süregiden bir tartışma yaşanmıştı. Hata ayıklama bilgisinin faydası şüphe götürmez. Bu bilginin duyurulmasını isteyen kişiler bir SMTP sunucusunu gerçekten güvenli kılmamanın, sunucunun kimliğini saklayarak bilinen savunmasızlıkların gizleneceğini ummaktan daha iyi olduğu noktasına dikkat çekerler. Sitelerin bu durumu akılda bulundurarak ödünleşime değer biçmeleri (neye taviz vereceklerine karar vermeleri) tavsiye edilir; gerçeklemlerinin diğer ağ konaklarına tür ve sürüm bilgilerini asgari düzeyde bile olsa bir şekilde erişilebilir kılmaya çalışmaları kesinlikle tavsiye edilmektedir.

## 7.5. İzleme Alanlarında Bilginin İfşası

Postanın konakları doğrudan Genel Ağ'a bağlı olmayan bir yerel ağdan kaynaklanması gibi durumlarda, bu belirtimle uyumlu olarak üretilmiş izleme ("Received") alanları, konak isimlerinin ve normalde erişilir olmayan benzeri bilgilerin ifşasına sebep olabilir. Bu sıradan bir durum olarak bir sorun teşkil etmese de isim ifşası ile özel ilgisi olan sitelerin bundan haberleri olması gerekir. Ayrıca, birden fazla alıcı olduğu durumda **FOR** cümlecigi dikkatli kullanılmalıdır, aksi taktirde "gizli kopya" alıcılarının diğerlerine görünür hale gelmesine yol açılabilir.

## 7.6. İleti Yönlendirmede Bilginin İfşası

*Adres Düzeltmek veya Güncellemek için Yönlendirme* (sayfa: 16) bölümünde açıklandığı gibi, bir posta kususyla ilişkilendirilmiş sevk yolu adresini tanımlamak için 251 veya 551 yanıt kodlarının kullanımı hassas bilgilerin açığa çıkmasına yol açabilir. Bu gibi durumlardan endişe duyan siteler, sunucuları buna uygun seçip yapılandırdıklarından emin olmalıdırlar.

## 7.7. SMTP Sunucularının Harekat Alanı

Sunucuyu sağlayan siteye mantıklı gelen herhangi bir işlemsel veya teknik sebep yüzünden bir SMTP sunucunun posta alımını reddetmesi iyice oturmuş bir prensiptir. Bununla birlikte, Genel Ağ, siteler ve tesisler arasındaki işbirliği ile mümkün olur. Siteler trafiği reddetmenin yararlarından aşırı yararlanmaya kalkarlarsa, epostanın yaygın olarak kullanılabilirliği (Genel Ağ'ın güçlü yanlarından biri) giderek azalmaya başlayacaktır; eğer bir site kabul edip işleyeceği trafikte seçici olmaya karar verirse çok dikkatli olunmalı ve denge sağlanmalıdır.

Son yıllarda, postanın kaynaklandığı yeri gizlemek için röleleme işlevi düşmanca bir çababanın bir parçası olarak rasgele sitelerde kullanıldı. Bazı siteler kaynakları tanımlayabilmek ve bilmek için röleleme işlevinin kısıtlanmasına ve gerçeklenimlerin bu tür filtreleme yapabilme kabiliyetinde olması gerektiğine **\*ÖNERİ\*** karar verdiler. Posta bu veya başka bir kural sebebiyle reddedildiğinde, **EHLO**, **MAIL** veya uygunsa **RCPT**'e yanıt olarak bir 550 kodu kullanılmalıdır **\*ÖNERİ\***.

## 8. IANA Değerlendirmeleri

IANA bu belirtimi desteklemek için üç kayıt alanı sağlar. İlki anahtar kelimeler ve gerektiğinde, parametreler ve fiiller ile ilişkili SMTP hizmet eklentilerinden oluşur. *Eklentilerin Tanımlanması ve Kayda Geçirilmesi* (sayfa: 8) bölümünde belirtildiği gibi bu kayıt alanında "X" ile başlayan hiçbir girdi yapılmaz. Girdiler sadece IESG tarafından özellikle bu amaç için onaylanmış deneysel RFC'ler veya standartlaşma aşamalarındaki RFC'lerde tanımlanan hizmet eklentileri (ve ilişkili anahtar kelimeler, parametreler veya fiiller) için yapılabilir.

İkinci yazmaç, IPv4 (RFC 821'de ve bu belgede belirtildi) ve IPv6 (bu belgede belirtildi) adresler için olanlar hariç, alan sabitlerinin biçimlerini tanımlayan "yaftalardan" oluşur. Ek sabit türleri kullanım öncesi standartlaşım gerektirir; şimdilik böyle birşey yoktur.

RFC 821 tarafından kurgulanan ve bu belirtimle yenilenen üçüncüsü, *İzleme Bilgisi* (sayfa: 37) bölümünde bahsedilen zaman damgasının ("Received:" başlığı) "via" ve "with" alt cümlecikleri ile kullanılacak bağ ve protokol betimleyicilerin bir kayıdır. Bu belgede belirtilenlere ek olarak bağ ve protokol betimleyiciler sadece standartlaşarak veya bir RFC'de belgelenmiş IESG onaylı bir deneysel protokol eklentisi yoluyla kayıt altına alınabilir.

## 9. Kaynakça

### 1. [X3.4]

(Bilgi değişimi için ABD kodu) ANSI X3.4-1968 arasına yapılan değişikliklerle yeni sürümleriyle

- değiştirilmiştir ama 1968 sürümü Genel Ağ için tanımlayıcı olarak kalmıştır. — **X3.4, 1968, USA Code for Information Interchange — V. Cerf ve R. Kahn** — Amerikan Ulusal Standartları Enstitüsü (eski adıyla, Amerika Birleşik Devletleri Standartları Enstitüsü) — Mayıs 1974
2. [RFC1123]  
Genel Ağ konakları için gereksinimler – uygulama ve destek — **STD 3, Requirements for Internet hosts – application and support — R. Braden** — Ekim 1989
  3. [RFC937]  
Postane Protokolü –2. sürüm (POP2) — **Posta Office Protocol – version 2 — M. Butler, D. Goldberg, J. Postel ve J. Reynolds** — Şubat 1985
  4. [RFC2440]  
OpenPGP İleti Biçimi — **OpenPGP Message Format — J. Callas, L. Donnerhacke, L. Finney, H. ve R. Thayer** — Kasım 1998
  5. [RFC1176]  
Etkileşimli Posta Erişim Protokolü – 2. sürüm — **Interactive Mail Access Protocol – Version 2 — M. Crispin** — Ağustos 1990
  6. [RFC2060]  
Genel Ağ İleti Erişim Protokolü – 4. sürüm (IMAP4) — **Internet Message Access Protocol – Version 4 — M. Crispin** — Aralık 1996
  7. [RFC822]  
ARPA Genel Ağ Metin İletilerinin Biçimi için Standart — **Standard for the Format of ARPA Internet Text Messages — D. Crocker** — Ağustos 1982
  8. [RFC2234<sup>(B174)</sup>]  
Sözdizimi Belirtilimleri için Arttırımlı BNF: ABNF — **Augmented BNF for Syntax Specifications: ABNF — D. Crocker ve P. Overell** — Kasım 1997
  9. [RFC1985]  
Uzaktan İleti Kuyruklamaya Başlamak için SMTP Hizmet Eklentisi — **SMTP Service Extension for Remote Message Queue Starting — J. De Winter** — Ağustos 1996
  10. [RFC2298]  
İleti Elverişlilik Bildirimleri için Geliştirilebilir İleti Biçimi — **An Extensible Message Format for Message Disposition Notifications — R. Fajman** — Mart 1998
  11. [RFC2979]  
Genel Ağ Güvenlik Duvarları için Davranışlar ve Gereksinimler — **Behavior of and Requirements for Internet Firewalls — N. Freed** — Ekim 2000
  12. [RFC2045]  
Çok Amaçlı Genel Ağ Posta Eklentileri (MIME) Birinci Kısım: Genel Ağ İleti Gövdeleri — **Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies — N. Freed ve Borenstein** — Aralık 1996
  13. [RFC2920]  
Komut Borulama için SMTP Hizmet Eklentisi — **SMTP Service Extension for Command Pipelining — N. Freed** — Eylül 2000

14. [RFC1847]  
MIMH için Çok Parçalı Güvenliği: Çok Parçalı/İmzalı ve Çok Parçalı/Şifreli — **Security Multiparts for MIMH: Multipart/Signed and Multipart/Encrypted** — J. Galvin, S. Murphy, S. Crocker, S. ve N. Freed — Ekim 1995
15. [RFC2476]  
İleti Teslimatı — **Message Submission** — R. Gellens ve J. Klensin — Aralık 1998
16. [RFC2156]  
X.400 ve RFC822/MIME arasındaki Uyum — **Mapping between X.400 and RFC822/MIME** — S. Kille — Ocak 1998
17. [RFC2373]  
IPv6 Adreleme Mimarisi — **IP Version 6 Addressing Architecture** — R. Hinden ve S. Deering — Temmuz 1998
18. [RFC1870]  
İleti Boyu Bildirimi için SMTP Hizmet Eklentisi — **STD 10, SMTP Service Extension for Message Size Declaration** — J. Klensin, N. Freed ve K. Moore — Kasım 1995
19. [RFC1869]  
SMTP Hizmet Eklentileri Standardı — **STD 10, SMTP Service Extensions** — J. Klensin, N. Rose, M. Stefferud, E. ve K. Crocker — Kasım 1995
20. [RFC1652]  
8bitlik MIME aktarımı için SMTP Hizmet Eklentisi — **SMTP Service Extension for 8bit-MIMEtransport** — J. Klensin, N. Rose, M. Stefferud, E. ve K. Crocker — July 1994
21. [RFC1056]  
PCMAIL: Kişisel Bilgisayarlar için Dağıtık Posta Sistemi — **PCMAIL: A distributed mail system for personal computers** — M. Lambert — Temmuz 1988
22. [RFC1035]  
Alan adları – gerçekleştirim ve belirtim — **STD 13, Domain names – implementation and specification** — P. Mockapetris — November 1987
- [RFC1034]  
Alan adları – kavramlar ve oluşumlar — **STD 13, Domain names – concepts and facilities** — P. Mockapetris — Kasım 1987
23. [RFC2047]  
Çok Amaçlı Genel Ağ Posta Eklentileri (MIME) Üçüncü Kısım: ASCII olmayan Metinler için Posta Başlığı Eklentileri — **MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text** — K. Moore — Aralık 1996
24. [RFC1891]  
Teslimat Durum Bildirimleri için SMTP Hizmet Eklentisi — **SMTP Service Extension for Delivery Status Notifications** — K. Moore — Ocak 1996
25. [RFC1894]  
Teslimat Durum Bildirimleri için Geliştirilebilir Bir İleti Biçimi — **An Extensible Message Format for Delivery Status Notifications** — K. Moore ve G. Vaudreuil — Ocak 1996

26. [RFC1939]  
POstane Protokolü – 3. sürüm (POP3) — **STD 53, Post Office Protocol – Version 3** — J. Myers ve M. Rose — May 1996
27. [RFC974]  
Posta yönlendirme ve alanadı sistemi — **Mail routing and the domain system** — C. Partridge — Ocak 1986
28. [RFC1047]  
Yinelenmiş İletiler ve SMTP — **Duplicate messages and SMTP** — C. Partridge — Şubat 1988
29. [RFC793<sup>(B196)</sup>]  
Aktarım Denetim Protokolü (TCP) – DARPA Genel ağ Programı Protokol Belirtimi — **STD 7, Transmission Control Protocol – DARPA Internet Program Protocol Specification** — J. Postel — Eylül 1981
30. [RFC821]  
Basit Posta Aktarım Protokolü (SMTP) — **Simple Mail Transfer Protocol** — J. Postel — Ağustos 1982
31. [RFC2633]  
S/MIME 3. sürüm İleti Belirtimi — **S/MIME Version 3 Message Specification** — B. Ramsdell — Haziran 1999
32. [RFC2822<sup>(B199)</sup>]  
Genel Ağ İleti Biçimi — **Internet Message Format** — B. Ramsdell — Nisan 2001
33. [RFC1830]  
Büyük ve İkili MIME İletilerinin Aktarımı için SMTP Hizmet Eklentisi — **SMTP Service Extensions for Transmission of Large and Binary MIME Messages** — G. Vaudreuil — Ağustos 1995
34. [RFC1893]  
Gelişkin Posta Sistemi Durum Kodları — **Enhanced Mail System Status Codes** — G. Vaudreuil — Ocak 1996

## 10. Yazarın Adresi

John C. Klensin  
AT&T Laboratories  
99 Bedford St  
Boston, MA 02111 USA

Telefon: 617-574-3076

Eposta: <klensin (at) research.att.com>

## 11. Teşekkür

Bu belgenin çoğu yenilemesinde bir çok insan uzun ve zorlu bir çalışma yaptı. IETF DRUMS Çalışma grubunda, hem grubun posta listesinde hem yüz yüze yapılan tartışmalarda bir çok teknik husus ve Genel Ağ posta aktarımında gözden geçirilmiş standardın rolü çok geniş çapta tartışıldı ve katkıda bulunan bir çok kişi bu belirtimin anlatım biçiminin oluşmasına yardım etti. RFC 821 üretilmeden önce yapılan tartışmalardaki yüzlerce katılımcı saymak için çok fazla, ama bu belgenin bu haline gelmesi için hepsinin yardımı oldu.



## A. TCP İletim Hizmeti

TCP bağlantısı 8 bitlik baytların iletimini destekler. SMTP verisi ise 7 bitlik ASCII karakterlerden oluşur. Her karakter yüksek biti sıfırlanarak bir 8 bitlik bayt olarak iletilir. SMTP komutlarında veya yanıtlarında değil, sadece ileti gövdesinin veri parçasının tam 8 bitlik baytlarla aktarımını mümkün kılmak için hizmet eklentileri bu kuralı değiştirebilirler.

## B. SMTP Komutlarının RFC 822 Başlıklarından Üretilmesi

Bazı sistemler posta teslimat protokolünde (sadece) RFC 822 başlıklarını kullanır, kullanamadığında da, örneğin bir ileti bir kullanıcı aracı (MUA) tarafından bir aktarım aracına (MTA) bırakıldığında, SMTP komutlarını RFC 822 başlıklarından üretir. MTA–MUA protokolü özel bir konu olduğundan ve hiçbir Genel Ağ standardınca kapsamadığından, bu yaklaşımla ilgili sorunlar vardır. Örneğin, kavramsal olarak bir posta zarfına ait bir bilgi başlık bilgisinden önceden ayrılmadığında (ve ayrı olarak tutulmadığında) listelerin tekrar dağıtılmasıyla ve gizli ("bcc") kopyaların düzgün ele alınmasıyla ilgili yinelenen sorunlar yaşanmıştır.

Kullanıcı aracının (MUA) ilk aktarım aracına (MTA) postayı bırakırken ileti ve zarfı ayrı ayrı teslim etmesinin sağlanması önerilir. Bununla birlikte, eğer zarf ayrı olarak sağlanmıyorsa, SMTP komutları şöyle üretilmelidir \*ÖNERİ\*:

1. **TO**, **CC** veya **BCC** başlık alanındaki her alıcı adresi **RCPT** komutuna kopyalanmalıdır \*ÖNERİ\* (eğer kuyruklama veya teslimat için gerekliyse çok sayıda ileti kopyası üreterek). BCC alanları varsa başlıklardan kaldırılmalıdır. Bu işlem tamamlandıktan sonra, kalan başlıklar, **To:**, **Cc:** veya **Bcc:** başlıklarından en az birinin kaldığından emin olmak için sınanmalıdır \*ÖNERİ\*. Eğer hiçbir yoksa, [32]'de belirtildiği gibi hiçbir ek bilgi olmaksızın bir **Bcc:** başlığı yerleştirilmelidir \*ÖNERİ\*.
2. **MAIL** komutundaki dönüş adresi, eğer mümkünse, postayı teslim eden (yerel) kullanıcının sistemdeki kimliğinden, mümkün değilse, "**From:**" başlığından türetilmelidir. Kullanılabilir sistem kimliği varsa ve **From:** başlığındaki adresten farklıysa, ayrıca **Sender** başlığına da kopyalanmalıdır \*ÖNERİ\*. (Bir **Sender** alanı zaten varsa silinmelidir \*ÖNERİ\*.) Sistemler zarf dönüş adresini değiştirmek için kullanıcılarına bir yöntem sunabilirler, ama kullanımını ayrıcalıklı kullanıcılar için kısıtlamak isteyebilirler. Bu, posta sahtekarlığını önlemeyecektir, ama görülme sıklığını düşürebilir; bkz, *Posta Güvenliği ve Yanıtlma* (sayfa: 47).

Bir MTA bu yönde kullanıldığında, aktarılan iletinin geçerliliğinden emin olunması sorumluluğunu alır. Geçerliliği sınama ve geldiğinde geçersiz olan iletileri elden geçirme (veya almama) mekanizmaları MUA–MTA arayüzünün bir parçası olup bu belirtimin kapsamında değildir.

Standard RFC 822 bilgisine dayalı bir teslimat protokolü bir iletiyi yabancı (SMTP dışı) bir posta sisteminden SMTP ortamına geçirmek için tek başına kullanılmamalıdır \*ZORUNLU\*. Zarfı oluşturacak ek bilgi, ister ilave başlıklarla ister yabancı sistemin zarfıyla olsun, diğer ortamdaki bir kaynaktan gelmelidir.

İletilerin sadece "**to**" ve "**cc**" alanlarını kullanarak geçitleme çabaları, posta döngülerine ve Genel Ağ posta ortamının düzgün çalışmasını engelleyici başka davranışlara yol açtı. Bu sorunlar çoğunlukla yaygın olarak, ileti bir Genel Ağ posta listesinden kaynaklanıp zarf bilgisi kullanılarak yabancı ortama dağıtıldığında görüldü. Bu iletiler daha sonra bir salt–başlık posta göndericisi tarafından işlendiğinde, Genel Ağ ortamına (ve posta listesine) geri dönüşler nerdeyse kaçınılmazdır.

## C. Kaynak Rotalar

Tarihsel olarak, <dönüş–yolu> konakların ve bir kaynak posta kutusunun tersine kaynak yönlendirme listesi idi. <dönüş–yolu> içindeki ilk konak **MAIL** komutunu gönderen konak olmalıdır \*ÖNERİ\*.

Benzer şekilde, <sevk-yolu> konakların ve bir varış posta kutusunun kaynak yönlendirme listesi olabilir. Yine de, genelde, <sevk-yolu> sadece bir posta kutusu ve gerekiyorsa yönlendirme bilgisini sağlamak için alan adı sistemine güvenerek, alan adını içermelidir \*ÖNERİ\*. Kaynak rota kullanımı önerilmemektedir; sunucuların *Posta Aktarım Harekâtı* (sayfa: 14) ve *Kaynak Yönlendirme* (sayfa: 57) bölümünde bahsedildiği gibi kaynak rotaları almaya ve işleme sokmaya hazırlıklı olmaları gerekiyken \*ZORUNLU\*, istemciler bunları aktarmasalar daha iyi olur \*ÖNERİ\*. Bu bölüm sadece bu bağlamı bulundurmak için eklendi.

Röleleme amacıyla, <sevk-yolu>, *alfa*, *beta* ve *gama* tamamen nitelenmiş alan adları olmaları şartıyla "*@alfa,@beta:biri@gama*" biçiminde bir kaynak rotası olabilir. Bu biçim bir adresle bir rota arasında ayrımı vurgulamak için kullanılır. Posta kutusu bir mutlak adresken, rota bir yere nasıl ulaşılabileceği bilgisini içerir. İki kavram karıştırılmamalıdır.

Kaynak rotalar kullanılıyorsa, sevk ve dönüş yollarını oluşturma ve güncelleme mekanizmaları için RFC 821'e ve aşağıdaki metne başvurulmalıdır.

Sevk yolundan dönüş yolunun başlangıcına kadar kendi tanıtıcısı (kendi alan adı veya posta aktarımcılığını yaptığı alan adı) görünüyorsa, SMTP sunucusu komut argümanlarını kendi tanıtıcısını taşıyarak dönüştürür.

Dönüş ve sevk yollarının SMTP komutlarında ve yanıtlarında görüldüğü halde iletide görünmesinin gerekli olmayışına dikkat ediniz. Yani, bu yolların, özellikle de bu sözdiziminin ileti başlığının "To:", "From:", "CC:", vs. alanlarında görünmesine ihtiyaç yoktur. Ancak, SMTP sunucularının da son ileti teslimat bilgisini iletinin başlık alanlarından elde etmemesi gerekir \*ZORUNLU\*.

Konak listesinin varlığı durumunda, bu bir "tersine" kaynak rotasıdır ve postanın listedeki konaklarda rölelendiğini gösterir (listedeki ilk konak en son röleleyendir). Bu liste göndericiye yapılamayan teslimatların bildirimlerini göndermek için kaynak rotası olarak kullanılır. Bir röleleme konağı olarak bir konak kendisini listenin başına eklerken, isim olarak, postanın geldiği aktarım ortamında değil postasını rölelediği aktarım ortamında bilinen ismini (farklıysa) kullanmalıdır \*ZORUNLU\*.

## D. Senaryolar

Bu bölümde çeşitli SMTP oturum türleri eksiksiz birer senaryo halinde sunulmuştur. Örneklerde "İ:" 'SMTP istemcisi dedi ki' anlamında "S:" ise 'SMTP sunucusu dedi ki' anlamında kullanılmıştır.<sup>(3)</sup>

### D.1. Tipik bir SMTP Aktarım Senaryosu

Bu SMTP örneğinde, bar.com konağındaki Smith tarafından foo.com konağındaki Jones, Green ve Brown'a posta gönderimi gösterilmiştir. Burada bar.com konağının foo.com konağına doğrudan eriştiğini varsayıyoruz. Posta Jones ve Brown için kabul edilmekte, Green için foo.com konağında bir posta kutusu olmadığı belirtilmektedir.

```
S: 220 foo.com Basit Posta Aktarım Hizmetine Hazır
İ: EHLO bar.com
S: 250-foo.com bar.com'a hosgeldiniz der
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
İ: MAIL FROM:<Smith@bar.com>
S: 250 OK
İ: RCPT TO:<Jones@foo.com>
S: 250 OK
İ: RCPT TO:<Green@foo.com>
S: 550 Burada boyle biri yok
İ: RCPT TO:<Brown@foo.com>
```

```
S: 250 OK
İ: DATA
S: 354 Posta girdisini baslat; <CRLF>.<CRLF> ile bitir
İ: Falan filan fesmekan...
İ: ...vesaire vesaire vesaire
İ: .
S: 250 OK
İ: QUIT
S: 221 foo.com aktarım hizmeti bu kanalı kapatıyor
```

## D.2. Sıfırlanan bir SMTP Aktarım Senaryosu

```
S: 220 foo.com Basit Posta Aktarım Hizmetine Hazir
İ: EHLO bar.com
S: 250-foo.com bar.com'a hosgeldiniz der
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
İ: MAIL FROM:<Smith@bar.com>
S: 250 OK
İ: RCPT TO:<Jones@foo.com>
S: 250 OK
İ: RCPT TO:<Green@foo.com>
S: 550 Burada boyle biri yok
İ: RSET
S: 250 OK
İ: QUIT
S: 221 foo.com aktarım hizmeti bu kanali kapatıyor
```

## D.3. Röleli Posta Senaryosu

### 1. Adım — Çıkış Konağından Röleleme Konağına

```
S: 220 foo.com Basit Posta Aktarım Hizmetine Hazir
İ: EHLO bar.com
S: 250-foo.com bar.com'a hosgeldiniz der
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
İ: MAIL FROM:<JQP@bar.com>
S: 250 OK
İ: RCPT TO:<@foo.com:Jones@XYZ.COM>
S: 250 OK
İ: DATA
S: 354 Posta girdisini baslat; <CRLF>.<CRLF> ile bitir
İ: Date: Thu, 21 May 1998 05:33:29 -0700
İ: From: John Q. Public <JQP@bar.com>
İ: Subject: Kurulun gelecek toplantisi
İ: To: Jones@xyz.com
İ:
İ: Bill:
İ: Yonetim kurulunun bir dahaki toplantisi
İ: Cuma gunu olacak.
```

```
İ: John.
İ: .
S: 250 OK
İ: QUIT
S: 221 foo.com aktarım hizmeti bu kanali kapatıyor
```

## 2. Adım — Röleleme Konağından Varış Konağına

```
S: 220 xyz.com Basit Posta Aktarım Hizmetine Hazir
İ: EHLO foo.com
S: 250-xyz.com yayindayiz
İ: MAIL FROM:<@foo.com:JQP@bar.com>
S: 250 OK
İ: RCPT TO:<Jones@XYZ.COM>
S: 250 OK
İ: DATA
S: 354 Posta girdisini baslat; <CRLF>.<CRLF> ile bitir
İ: Received: from bar.com by foo.com ; Thu, 21 May 1998
İ: 05:33:29 -0700
İ: Date: Thu, 21 May 1998 05:33:22 -0700
İ: From: John Q. Public <JQP@bar.com>
İ: Subject: Kurulun gelecek toplantisi
İ: To: Jones@xyz.com
İ:
İ: Bill:
İ: Yonetim kurulunun bir dahaki toplantisi
İ: Cuma gunu olacak.
İ: John.
İ: .
S: 250 OK
İ: QUIT
S: 221 foo.com aktarım hizmeti bu kanali kapatıyor
```

## D.4. Doğrulama ve Gönderme Senaryosu

```
S: 220 foo.com Basit Posta Aktarım Hizmetine Hazir
İ: EHLO bar.com
S: 250-foo.com bar.com'a hosgeldiniz der
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250-VRFY
S: 250 HELP
İ: VRFY Crispin
S: 250 Mark Crispin <Admin.MRC@foo.com>
İ: SEND FROM:<EAK@bar.com>
S: 250 OK
İ: RCPT TO:<Admin.MRC@foo.com>
S: 250 OK
İ: DATA
S: 354 Posta girdisini baslat; <CRLF>.<CRLF> ile bitir
İ: Falan filan fesmekan...
İ: ...vesaire vesaire vesaire
İ: .
S: 250 OK
İ: QUIT
```

S: 221 foo.com aktarım hizmeti bu kanali kapatıyor

## E. Diğer Ağgeçidi Konuları

Genelde, Genel Ağ ile diğer posta sistemleri arasındaki ağgeçitleri iki posta sisteminin sınırları arasında birini diğerine karşı katmanlama anlamında korumaya çalışmalıdır \*ÖNERİ\*. Eşleşmelerle kestirme yollar oluşturmaya çalışan ağgeçitli dönüşüm yaklaşımının (örneğin, ileti başlıklarına veya başka bir ileti gövdesine bir sistemdeki zarf bilgisini eşleme) önemli yollarda genellikle yetersiz kaldığı kanıtlanmıştır. Zarfların ve başlıkların her ikisini de desteklemeyen ortamlar arasında dönüşüm yapan sistemler ve Genel Ağ postası bilgi kaybının neredeyse kaçınılmaz olduğunun bilincinde olarak yazılmalıdır.

## F. RFC 821'in Önerilmeyen Özellikleri

RFC 821'in bir kaç özelliğinin sorunlu olduğu kanıtlanmıştır ve Genel Ağ postasında kullanılmaması gerekir \*ÖNERİ\*.

### TURN Komutu

RFC 821'de açıklanan bu komut, istemci ve sunucunun rol değiştirmesini talep eden konağın kimliğinin kesinlikle kanıtlanması gereği yerine getirilmedikçe bu durum, postayı kolayca doğru hedefinden saptırmak için kullanılabileceğinden önemli güvenlik kaçaklarını arttırır. Kullanımı önerilmez; sunucu tarafından istemci kimliğinin kanıtlanması sağlanmadıkça SMTP sistemlerinin bu komutu kullanmaması gerekir \*ÖNERİ\*.

### Kaynak Yönlendirme

RFC 821, postanın bir konaktan diğerine bir röleleme silsilesinden sonra aktarılması anlamına gelen doğrudan kaynak yönlendirme kavramından yararlanır. Sıradan posta trafiğinde kaynak rotalardan yararlanma gereksinimi, alan adı sistemine "MX" kaydının girişiyle ve bunların son derece önemli bir ayarlaması da, RFC 1123'e, adreslerde "@" imini izleyen kısmın tamamen nitelenmiş alan isimleri içermesi şeklindeki açık gereksinimin girişiyle ortadan kalkmıştır.

Netice olarak, kaynak rota kullanımı için sadece hizalamanın kalması, çok eski SMTP istemcileri ile kullanıcı postalama araçları ve posta sistemi hata ayıklaması için desteklenmektedir. Bunlar yine de, son durumla ilgili olarak ve maksada uygun DNS kayıtları gibi ciddi ama geçici sorunların çevresinden dolanarak posta yönlendirme için hala kullanışlıdır.

Bu belgenin ana gövdesinde ve RFC 1123'te belirtildiği gibi SMTP sunucuları kaynak rota sözdizimini kabul etmeye devam etmelidirler \*ZORUNLU\*. Bunlar gerekirse rotaları yoksayarak sadece adresteki hedef alandan yararlanabilirler \*SEÇİMLİK\*. Eğer kaynak rotadan yararlanırlarsa, iletinin adreste gösterilen ilk alana gönderilmesi gerekir \*ZORUNLU\*. Özellikle bir sunucu kaynak rota içindeki kısayollarda tahmin yapmamalıdır \*ZORUNLU\*.

Posta sistemi yapılandırma hataları veya güvenlik duvarı etrafından dolaşmak için röleleme olasılığı veya hata ayıklama gibi olumsuz durumlar haricinde istemcilerin doğrudan kaynak yönlendirmeden yararlanmamaları gerekir \*ÖNERİ\*.

### HELO Komutu

*Oturum İklendirme* (sayfa: 13) ve *Komut Sözdizimi ve Anlamlandırma* (sayfa: 22) bölümünde bahsedildiği gibi, sunucu **EHLO** komutunu kabul edebilecekse, **EHLO** komutu daima/mutlaka **HELO** komutuna tercih edilir. Sunucu-

ların eski istemcileri desteklemek için **HELO** komutunu kabul etmeye ve işleme sokmaya devam etmesi gerekir.

## # imli sabitler

RFC 821, bir Genel Ağ adresinin, bir "#" imi ile başlayan ve konak numarasını ifade eden bir ondalık tamsayı ile belirtilmesine izin verir. Uygulamada, TCP/IP'ye geçildiğinden beri, bu biçim artık kullanılmamaktadır ve kullanılmamalıdır \*ZORUNLU\*.

## Tarihler ve Yıllar

SMTP istemcileri ve sunucuları tarafından iletilere tarih yerleştirilmek istendiğinde (örn, izleme alanlarına), dört rakamlı yıl gösterimi kullanılmalıdır \*ZORUNLU\*. İki rakamlı yıllar önerilmemektedir; üç rakamlı yıllara ise Genel Ağ posta sisteminde hiçbir zaman izin verilmemiştir.

## Postalamayıp Gönderivermek

İletilerin kullanıcıların posta kutularına teslimatı için bir mekanizma belirtilmesine ek olarak, RFC 821, iletileri doğrudan kullanıcının uçbirim ekranına teslim eden isteğe bağlı ek komutlar sağlamıştır. Bu komutlar (**SEND**, **SAML**, **SOML**) nadiren gerçekleşmiş, iş istasyonu teknolojisindeki değişiklikler ve diğer protokollerin devreye girmesiyle gerçekleştirildikleri yerlerde bile kullanılmayarak atıl olmuştur.

İstemciler hizmet olarak **SEND**, **SAML**, **SOML** komutlarını bulundurmamalıdır \*ÖNERİ\*. Bunlar sunucular tarafından gerçekleştirirse, RFC 821'de belirtilen gerçekleştirim modeli kullanılmalı \*ZORUNLU\* ve komut isimleri **EHLO** komutunun yanıtında yayınlanmalıdır \*ZORUNLU\*.

## G. Tam Telif Hakkı Beyanı

Copyright (C) The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

### Bilgi için

**RFC Editor**<sup>(B210)</sup> işlevinin mali desteği şu an Genel Ağ Derneği (The Internet Society) tarafından sağlanmaktadır.



## Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(B1) <ftp://ftp.rfc-editor.org/in-notes/bcp/bcp78.txt>

(B3) <http://www.ietf.org/>

(1) Ç.N. – Bu bağ özgün metinde 2.4.1 numaralı bölümü göstermektedir. <http://www.mhonarc.org/archive/html/ietf-smtp/2002-07/msg00053.html> adresindeki iletide belgenin yazarı bu atıfların aslında 6.3 numaralı bölümü göstermesi gerektiğini belirtmektedir. Bu bağ ve belgedeki böyle diğer iki bağ bu açıklamaya göre düzeltilmiştir.

(2) Ç.N. – Bu bağ özgün metinde 2.4.1 numaralı bölümü göstermektedir. <http://www.mhonarc.org/archive/html/ietf-smtp/2002-07/msg00053.html> adresindeki iletide belgenin yazarı bu atıfların aslında 6.3 numaralı bölümü göstermesi gerektiğini belirtmektedir. Ancak aynı listeye 3 yıl sonra gönderilen [başka bir iletide](http://www.mhonarc.org/archive/html/ietf-smtp/2005-05/msg00069.html) (<http://www.mhonarc.org/archive/html/ietf-smtp/2005-05/msg00069.html>) özellikle bu bağın 2.4 numaralı bölümü göstermesi gerektiği belirtilmektedir. (6.3 numaralı bölümde harf büyüklüklerinden bahis yoktur.) Buradaki bağ bu saptamaya göre düzeltilmiştir.

(B174) [../rfc/rfc2234.pdf](http://rfc/rfc2234.pdf)

(B196) [../rfc/rfc793.pdf](http://rfc/rfc793.pdf)

(B199) [../rfc/rfc2822.pdf](http://rfc/rfc2822.pdf)

(3) Ç.N. – Senaryolar, gerçekte olmayacak şekilde Türkçeye çevrilmiştir. Gerçekçi senaryolar için bu RFC'nin özgün haline bakınız.

(B210) <http://www.rfc-editor.org/>

Bu dosya (rfc2821.pdf), belgenin XML biçiminin T<sub>E</sub>XLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

17 Ocak 2007