



İSTANBUL AYDIN ÜNİVERSİTESİ
KAMPÜS VERİ MERKEZİ ALIMI
TEKNİK ŞARTNAMESİ

ŞARTNAME NU: 2026-DATACENTER

:

TARİH

:Temmuz 2026

1. Bu onaylı teknik şartname, yayım tarihinden itibaren yürürlüğe girer.
2. Bu onaylı teknik şartnamenin yürürlükten kaldırılma tarihi
31 Aralık 2028
3. Bu onaylı teknik şartname üzerinde değişiklik yapılamaz.
4. Bu onaylı teknik şartname kapak dâhil toplam 21 (yirmibir) sayfadan ibarettir.

İÇİNDEKİLER

1. KONU	2
2. GENEL HUSUSLAR.....	2
3. İSTEK VE ÖZELLİKLER	6
4. DENETİM VE MUAYENE	19
5. EKLER	20



1. KONU

Bu teknik şartname, satın alınacak Bilgi Sistemlerinin; donanımları ve yazılımlarının teknik özelliklerini, denetim ve muayene metotlarını ve ilgili diğer hususları konu alır.

2. GENEL HUSUSLAR

2.1. Tanımlar

2.1.1. Arabirim

2.1.1.1. Bilgisayar sisteminin başka bir bilgisayar sistemi ya da bir yan donanımla (yazıcı, disk, teyp, terminal, optik okuyucu gibi) bağlantısı için gerekli her türlü kart, modem, switch (anahtar) gibi cihazlarla, kablo, konnektör ve buna benzer diğer tüm donanım unsurlarıdır.

2.1.2. Dokümantasyon

2.1.2.1. Bilgisayarın işletim, bakım-onarım, eğitim konularında kullanılmak üzere ilgili üretici tarafından yayımlanmış her türlü kitap, basılı form, not, resim, şekil, plan, prospektüs, broşür, CD ve bunların benzerleridir.

2.1.3. İş Günü

2.1.3.1. Resmi tatil günleri ve hafta sonu (Cumartesi, Pazar) günleri haricindeki diğer günlerin 08.00 ile 17.30 arasındaki saatleridir.

2.1.4. Kurum

2.1.4.1. İstanbul Aydın Üniversitesi'dir

2.1.5. Yan Donanım (Çevre Birimi)

2.1.5.1 Bir bilgisayar sistemine giriş/çıkış cihazları olarak bağlanabilecek disk, teyp, terminal, yazıcı vb. her türlü donanım unsurlarıdır.

2.1.6. Yazılım Lisansı

2.1.6.1. Yazılımı çalıştırmak için verilen yasal haktır.

2.1.7. Yazılım Güvencesi (Software Assurance)

2.1.7.1. Tedarik edilecek yazılım lisanslarının çıkarılacak en son sürümünü, güvencenin geçerli olduğu süre içerisinde ek ücret ödemeden kullanma hakkıdır.

2.1.8. Modül

2.1.8.1. Modüler tipte üretilmiş her türlü bilgi sistem donanımına takılabilen ve belli yetenekler sağlayan parçadır.

2.1.9. Port

2.1.9.1. Bağlantı noktasıdır.

2.1.10. Uplink Portu

2.1.10.1. Üst bağlantı noktasıdır.

2.1.11. Fiber Optik Kablolama

2.1.11.1. Optik lif içeren kablolar ile yapılan kablolamadır.

2.1.12. SC-LC Tipi Konnektör

2.1.12.1. Fiber optik kablolamada sonlandırmada kullanılan küçük tip konnektörlerdir.

2.1.13. Yüklenici

2.1.13.1. Başkası için yapı ve ticaretle ilgili bir işi yapmayı üstüne alan kimse, üstenci.

2.1.14. Yazılım

2.1.14.1 Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelerin tümü.

2.2. Kısaltmalar

ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point (Kablosuz Erişim Noktası)
BGP	Border Gateway Protocol
CAT6	Category 6
CPU	Central Processing Unit
DAC	Direct Attach Cable
Db	Decibel
DDR	Double Data Rate
DNS	Domain Name System
ECC	Error Correction Code
ECMP	Equal-Cost Multi-Path
EN	European Norm
FCC	Federal Communications Commission
GAA	Geniş Alan Ağı
GB	Giga Byte
GHz	Giga Hertz
GUI	Graphical User Interface
HTML	HyperText Markup Language
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol

ISO	International Organization of Standardization
ITU	International Telecommunication Union
KGK	Kesintisiz Güç Kaynağı
KVA	Kilo Volt Amper
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LC	Lucent Connector
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MACsec	Media Access Control Security (IEEE 802.1AE)
MB	Mega Byte
Mbps	Mega bits per second
mGig	Multigigabit Ethernet (IEEE 802.3bz)
MHz	Mega Hertz
mm	Milimetre
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failures
NAS	Network-Attached Storage
NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PBR	Policy-Based Routing
PCI	Peripheral Component Interconnect
PDF	Portable Document Format
PoE	Power over Ethernet (IEEE 802.3af/at/bt)
QoS	Quality Of Service
QSFP28	Quad Small Form-factor Pluggable 28 (100G)
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RJ-45	Registered Jack (Connector 45)
RoHS	Restriction of Certain Hazardous Substances in Electrical and Electronic Equipment
RSTP	Rapid Spanning Tree Protocol
RS-232	Recommended Standard 232
SAN	Storage Area Network
SFP	Small Form Pluggable
SFP28	Small Form-factor Pluggable 28 (25G)
SFP56	Small Form-factor Pluggable 56 (50G)
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSH	Secure Shell

STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access-Control System Plus
TSE	Türk Standartları Enstitüsü
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VA	Volt Amper
VAC	Volt Alternative Current
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
VXLAN	Virtual Extensible LAN
°C	Santigrat derece

Handwritten signature in blue ink, followed by a circular blue ink stamp.Handwritten signature in blue ink.

3. İSTEK VE ÖZELLİKLER

3.1. Genel İstekler

3.1.1. Bu şartname kapsamındaki yazılım ve donanımlar, kurum tarafından talep edildiğinde, kurulumu ve çalıştırılması dâhil olarak satın alınacaktır.

3.1.2. Yüklenici tarafından yürütülecek her türlü kurulum faaliyetleri sırasında; yüklenicinin kusurundan ötürü hasar gören, bozulan, kirlenen veya işlevini yitiren her türlü bina, tesis, açık veya kapalı alanlardaki zemin kaplama malzemeleri, boya, badana, kablo, teçhizat, dekorasyon malzemeleri ve benzeri kullanıcı envanterinde bulunan unsurlar yüklenici tarafından, ücretsiz olarak eski haline gelecek şekilde düzeltilecek ve/veya yenilenecektir.

3.1.3. Yüklenici tarafından, verilecek hiçbir yazılım ve donanım, ürünün üreticisi tarafından satıştan veya destekten kaldırılmamış olacaktır (out of date / out of sale / out of support v.b.)

3.1.4. Sistemleri oluşturan tüm donanım, yan donanım ve ara birimler yeni ve hiç kullanılmamış olacaktır. Bu malzemelerin hiçbir bölümünde kırık, çatlak, deformasyon ve malzeme hataları bulunmayacaktır.

3.1.5. Tüm sistem ve bağlı donanımlar, teknik şartnamede aksi belirtilmediği sürece, 220 (ikiyüzyirmi) Volt AC ($\pm\%10$ (artı eksi yüzde on) tolerans ile), 50 (elli) Hz ve/veya 50 (elli) Hz ($\pm\%1$ (artı eksi yüzde bir) tolerans ile) elektrik özelliklerinde hatasız çalışacak, şebeke gerilimi düşürücü trafo kullanımına ihtiyaç göstermeyecektir.

3.1.6. Teknik şartnamede tanımlı olan donanımlar ile bu donanımların muhteviyatları (alt donanımları, kablo, soket, optik modül, RAM vb.), söz konusu ürünü üreten firmanın orijinal ürünü olacak veya söz konusu donanımı üreten üretici firmanın söz konusu donanıma ait kataloglarında tanımlı ürünler arasında olacaktır.

3.1.7. İstenen dokümanlardan elektronik, manyetik vb. ortamlarda olanlar, bulundukları ortamda (CD/DVD) ayrıca verilecektir.

3.1.8. Teknik Şartname kapsamında satın alınacak, Ethernet Anahtarlar aynı üreticinin ürünü olacaktır.

3.1.9. Satın alınacak ürünler 3 yıl süre ile üretici veya üretici tarafından yetkilendirilmiş bir iş ortağı tarafından yazılım ve donanım garantisi altında olacaktır. Kullanıcı tarafından bildirilecek ve servis kesintisine sebep olan problemlere en geç 4 saat içerisinde uzaktan veya yerinde müdahale edilecektir.

3.2. Teknik İstekler

3.2.1. Sunucu F/O Ethernet Anahtarı

3.2.1.1. Anahtar üzerinde bağlantılar için en az 48 adet 1/10/25 Gbps fiber arayüz ve uplink bağlantıları için de en az 6 adet 40/100Gbps fiber arayüz bulunacaktır.

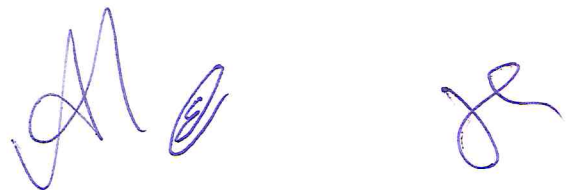
3.2.1.2. 1/10/25 Gbps arayüzlere 1000Base-T, 1GBase SX, 1GBase-LH, 10 Gbps SR, 10 Gbps LR, 25 Gbps LR, 25 Gbps SR ve Direct Attach kablolar takılabilmelidir.

3.2.1.3. 40/100 Gbps arayüzlere de 40Gbps SR, 40Gbps LR, 100Gbps LR, 100Gbps SR arayüzler ve Direct Attach kablolar takılabilmelidir.

- 3.2.1.4. Anahtar üzerinde bir bakır bir de fiber bağlantılar için en az 1 adet Ethernet yönetim arayüzü, 1 adet USB arayüzü ve bir adet konsol arayüzü bulunmalıdır.
- 3.2.1.5. Anahtar tüm portlarında desteklenen en yüksek hızlarda tıkanmasız ve tel hızında çalışacaktır.
- 3.2.1.6. Anahtarın tüm portlarında portlar arası gecikme değeri 1 mikro saniyenin altında olacaktır.
- 3.2.1.7. Anahtar en az 3.6 Tbps bandwidth ve 1.2 bpps değerine sahip olmalıdır.
- 3.2.1.8. Anahtarın en az 4 core bir işlemcisi olmalıdır.
- 3.2.1.9. Anahtar en az 16 GB belleğe, en az 64 GB SSD/eMMC disk'e ve en az 32MB buffer'a sahip olmalıdır. Cihaz üzerinde uygulama barındırma (container/guest shell) desteği bulunması tercih sebebidir.
- 3.2.1.10. İstenmesi halinde 16 GB sistem belleği ilave edilebilmelidir.
- 3.2.1.11. Anahtar en az 400.000 adet route bilgisini (LPM-Longest Prefix Match) tutabilmelidir.
- 3.2.1.12. Anahtar en az 200.000 adet MAC adresi tablolarında tutabilmelidir.
- 3.2.1.13. Anahtar en az 8.000 adet multicast route tutabilmelidir.
- 3.2.1.14. Anahtar en az 8000 adet IGMP snooping grubu desteklemelidir.
- 3.2.1.15. Anahtar en az 64 adet VRF destekleyebilmelidir.
- 3.2.1.16. Anahtar kablo hızında VXLAN destekleyecek bir donanıma sahip olmalıdır. İstenmesi halinde ilerde lisans alınarak bu özellik kullanılabilir olmalıdır.
- 3.2.1.17. Anahtar en az 64 kanal route yedekliliği (ECMP) desteklemelidir.
- 3.2.1.18. Anahtar en az 1000 adet NAT satırı destekleyebilir olmalıdır.
- 3.2.1.19. Anahtarın MTBF değeri en az 200.000 saat olmalıdır.
- 3.2.1.20. İki anahtarı sanal olarak birleştirip bağlı diğer anahtar ve sunucuların bu iki sanallaştırılmış Anahtara aktif aktif bağlanması sağlanabilmelidir. (Multi-Chassis Etherchannel)
- 3.2.1.21. LLDP protokolünü desteklemelidir.
- 3.2.1.22. Anahtar 0. Gün işlemlerini kısaltan ve otomatik hale getiren, otomatik provizyon özelliğine sahip olmalıdır.
- 3.2.1.23. Anahtar bütün CLI fonksiyonlarının karşılığı olarak API URI larına sahip olmalıdır.
- 3.2.1.24. Anahtar üzerinde IEEE 802.1d STP (Spanning-Tree Protocol) protokolü desteklenmelidir ve anahtar üzerinde tanımlanan her bir VLAN için farklı STP kullanılabilmelidir. Bu amaçla anahtar IEEE 802.1s MSTP (Multiple Spanning-Tree Protocol) protokolünü desteklemelidir. Anahtar kullanıcı ve trunk portlarında STP hesaplamalarını hızlandırabilmek amacıyla IEEE 802.1w RSTP (Rapid Spanning-Tree Protocol) protokolünü desteklemelidir.
- 3.2.1.25. Anahtar üzerinde aktif olarak en az 3967 adet vlan kullanılabilmelidir.



- 3.2.1.26. Anahtar üzerinde en az 64 farklı MST örneđi tanımlanabilmelidir.
- 3.2.1.27. Anahtar üzerinde istenmeyen STP paketlerinin durdurulması amacıyla BPDU (Bridge Protocol Data Unit) paketlerinin istenilen arayüzden alınması, gönderilmesi ve filtrelenebilmesi (BPDU Guard, BPDU Filter) desteklenmelidir. STP kök anahtarını koruyacak mekanizmalar (Root Guard, Loop Guard) var olmalıdır.
- 3.2.1.28. Anahtar üzerinde istenmesi halinde STP hesaplamalarını hızlandırmak için gereken mekanizmalar çalıştırılabilmelidir.
- 3.2.1.29. Anahtar üzerinde birden fazla portun bir araya getirilerek tek bir port gibi çalışabilmesini sağlayan 802.3ad LACP protokolü desteklenmelidir. Tek bir Anahtar üzerinde en az 16 adet port aynı grup içine alınabilmelidir.
- 3.2.1.30. Anahtar (ya da anahtar grubu) üzerinde en az 128 adet port channel tanımlanabilmelidir.
- 3.2.1.31. Anahtar fiber bağlantının kontrolü için UDLD ya da benzeri bir mekanizmaya sahip olmalıdır.
- 3.2.1.32. Cihaz 802.3 Flow Control özelliđine sahip olmalıdır.
- 3.2.1.33. Statik yönlendirmenin haricinde lisans artırımı ile dinamik yönlendirme protokollerinden OSPF, BGP veya IS-IS protokollerinden en az ikisini ve IPv6 destekleyebilmelidir; EIGRP desteđi opsiyoneldir. Anahtar static route destekleyecek şekilde teklif edilecektir.
- 3.2.1.34. Anahtarın BFD desteđi olmalıdır.
- 3.2.1.35. Anahtar IPv6 desteđine sahip olabilmelidir.
- 3.2.1.36. Anahtar DHCP paketlerini ađ üzerinde iletmek için DHCP relay özelliđine sahip olmalıdır.
- 3.2.1.37. Anahtar Multicast desteđine sahip olmalıdır ve IGMP v1, v2, v3 protokollerini desteklemelidir.
- 3.2.1.38. Anahtar Netflow, FT, FTE, SSX veya telemetry özelliklerine sahip olmalıdır.
- 3.2.1.39. Anahtar, Protocol-Independent Multicast (PIM) sparse mode (PIM-SM), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) destekleyebilmelidir.
- 3.2.1.40. Anahtardaki her portun en az 4 adet kuyruk desteđi olmalıdır.
- 3.2.1.41. DSCP, CoS deđerlerine göre ya da ACL ile yakalanan trafiđe önceliklendirme yapabilmelidir.
- 3.2.1.42. Anahtar portların çıkış yönünde Strict Priority, Weighted Random Early Detection (WRED) veya Weighted Round-Robin (WRR) kuyruklama özelliklerini desteklemelidir.
- 3.2.1.43. Anahtar gelen ya da giden trafiđin L2, L3 ya da L4 bilgilerine bakarak erişim kontrol listeleri (ACL) uygulayabilmelidir.
- 3.2.1.44. Anahtar broadcast, multicast ya da unknown unicast fırtınalarını engelleyici ya da sınırlayıcı bir mekanizmaya sahip olmalıdır.
- 3.2.1.45. Anahtar üzerinde CPU vb kaynakları korumak için bir control plane koruma mekanizması bulunmalıdır.



- 3.2.1.46. Anahtara farklı yetkilerde yöneticiler atanabilmelidir.
- 3.2.1.47. Anahtar kendi veritabanından, RADIUS ya da TACACS+ protokollerinden en az birisini kullanarak kullanıcı doğrulama yapabilmelidir.
- 3.2.1.48. Anahtar Telnet, SSHv2 ya da harici bir yönetim yazılımı aracılığı ile yönetilebilmelidir.
- 3.2.1.49. Anahtar,EEM (Embedded Event Manager) veya üreticinin eşdeğer olay otomasyon/scripting altyapısını desteklemelidir.
- 3.2.1.50. Anahtarın konfigürasyon geri alma ya da kayıtlı konfigürasyona geri dönme özellikleri olacaktır.
- 3.2.1.51. Anahtar SNMP v1, v2, v3 desteğine sahip olmalıdır.
- 3.2.1.52. Anahtara dosya transferi amacıyla FTP, SFTP ya da TFTP protokolleri desteklenmelidir. Dosya transferi için ayrıca USB arayüzü de kullanılabilir.
- 3.2.1.53. Anahtar ağ üzerindeki tüm anahtarlarla senkron olabilmek için NTP protokolünü desteklemelidir.
- 3.2.1.54. Anahtar üzerinde 1 ya da fazla port üzerinden akan trafiği tek bir porta aynalamaya yarayan SPAN ve ERSPAN özellikleri desteklenmelidir. Eş zamanlı en az 4 SPAN oturumu desteklenmelidir.
- 3.2.1.55. Anahtar kendisi log tutabildiği gibi gerekirse harici bir log sunucusuna da log gönderebilmelidir.
- 3.2.1.56. Anahtar üzerinde güç kaynakları ve fanlar dahili yedekli ve çalışırken değiştirilebilir şekilde teklif edilmelidir. Yedek Fan ve güç kaynakları teklife dahil edilecektir.
- 3.2.1.57. Fan ve Güç kaynaklarının hava çıkış yönü için opsiyonel çözümler sunulabilmelidir. Hava akış yönü Port Side Intake olarak teklif edilmelidir.
- 3.2.1.58. Anahtar advanced network traffic monitoring, packet brokering, and tap aggregation özelliklerini veya benzerlerini destekleyecek lisans ile teklif edilmelidir.
- 3.2.1.59. Anahtar yedeklilik için VPC, virtual stacking veya benzeri protocoollerden en az birini destekleyecek şekilde yedekli olarak teklif edilecektir.
- 3.2.1.60. Yedeklilik ve diğer bağlantılar için yeterli sayıda ve uygun tipte SFP yapılan keşif veya planlamaya göreteklife dahil edilmelidir.
- 3.2.1.61. Anahtarlar standart üretici garantisine ek olarak en az 3 yıllık 8x5xNBD üretici destek paketi ile birlikte teklif edilecektir. Bu üretici support paketi en az teknik destek, ertesi iş günü değişim ve yazılım güncelleme yetkilerini kapsamalıdır.

3.2.2. Sunucu Ethernet Anahtar

- 3.2.2.1. Anahtar üzerinde en az 48 adet 10/100/1000Mbps bakır port ve 4 adet 1/10 Gig SFP+ port bulunmalıdır. Aynı anda 52 adet Port çalışabilmelidir.
- 3.2.2.2. Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.

- 3.2.2.3. Anahtarın modüler güç kaynağı desteği olmalıdır. İstenmesi halinde ikinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir. Anahtar yedekli güç kaynakalı ile birlikte teklif edilecektir.
- 3.2.2.4. Anahtarın bütün portlarında 802.3af (15W), 802.3at (30W) desteği olacaktır. Çift güç kaynağı ile en az 1440Watt Poe verebilecek donanım desteğine sahip olabilmelidir. Teklif edilecek switch çift güç kaynağı ile birlikte en az 1200 Watt Toplam PoE bütçesini destekleyecek şekilde teklif edilecektir.
- 3.2.2.5. Anahtar tekrar başlatıldığında dahi, kendine bağlı PoE cihazlarına kesintisiz güç vermeye devam edebilmelidir. Böylece anahtara bağlı PoE cihazlarının da reboot etmesi engellenmelidir.
- 3.2.2.6. Anahtarlama bant genişliği yığınlama kapasitesi hariç en az 176 Gbps olmalıdır. Anahtarın L2 anahtarlama performans değeri en az 130 Mpps olmalıdır. Yığınlama kapasitesi dahil anahtarlama bant genişliği en az 496 Gbps; L2 anahtarlama performans değeri 369 Mpps olmalıdır.
- 3.2.2.7. Anahtar en az 16MB paylaşımlı bir buffer'a sahip olmalıdır.
- 3.2.2.8. Anahtar modüler ve N+1 yedekli çalışan fan'lara sahip olmalıdır.
- 3.2.2.9. Anahtar programlanabilir bir ASIC'e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.
- 3.2.2.10. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.
- 3.2.2.11. Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini ve cihaz üzerinde Python scripting desteklemelidir.
- 3.2.2.12. Anahtar en az 8Gb DRAM ve 16Gb Flash belleğe sahip olmalıdır.
- 3.2.2.13. Anahtar üzerinde en az bir adet USB 2.0 ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır. Cihaz üzerinde uygulama barındırma ve harici SSD desteği bulunması tercih sebebidir.
- 3.2.2.14. Anahtarın 9100 byte'lık jumbo frame desteği olmalıdır.
- 3.2.2.15. Anahtarın bakır portlarında 802.3az EEE (Energy Efficient Ethernet) desteği olmalıdır.
- 3.2.2.16. Anahtar envanter yönetimi için RFID etiketi, barkod/QR kod, seri numarası veya üreticinin eşdeğer envanter yöntemine sahip olmalıdır.
- 3.2.2.17. Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi içinaçılıp kapatılabilen locator LED/beacon (Blue Beacon veya eşdeğeri) desteğine sahip olmalıdır.
- 3.2.2.18. Anahtar yazılımsal olarak Bluetooth desteğine sahip olmalıdır. Opsiyonel olarak bağlanacak bluetooth aparatı üzerinden anahtarın WEB ve komut arayüzüne erişmek, log ve işletim sistemi transferi yapmak mümkün olmalıdır.
- 3.2.2.19. Anahtar sekiz adete kadar yığılanabilmelidir.
- 3.2.2.20. Yığınlama için gerekli kit, kablo, transceiver veya DAC/AOC kablolar teklif kapsamında sağlanmalıdır. Yığınlama için dedicated stack portu veya front-plane port kullanımı üretici mimarisine göre

kabul edilecektir; yığınlama çalıştırıldığında hiç bir kullanıcı portu devre dışı kalmamalıdır. Stack kablo için en az 0.5 metre, 1 metre, 3 metre gibi opsiyonlar sunulabilmelidir.

3.2.2.21. Tüm yığın tek IP Adresi ve tek bir konfigürasyon üzerinden yönetilebilmeli ve yığın çalışırken yeni bir anahtarı yığına eklenebilmelidir.

3.2.2.22. Yığında anahtarlama bant genişliği en az 200 Gbps olmalı, yığındaki tüm anahtarlar bu bant genişliğine tam erişime sahip olmalıdır.

3.2.2.23. Yığındaki farklı anahtarlar üzerinden etherchannel yapmak mümkün olmalıdır. (multi-chassis etherchannel)

3.2.2.24. Anahtar en az Spanning Tree (802.1d, MST, Rapid), 802.1x, 802.3af, LACP, IGMP Snooping, DHCP Snooping özellikleri için SSO (Stateful Switchover) desteklemelidir.

3.2.2.25. Anahtar en az 32.000 adet MAC adresi desteklenmelidir.

3.2.2.26. En az 4000 adet aktif VLAN desteği olmalıdır.

3.2.2.27. IEEE 802.1d Spanning Tree Protocol(STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan'ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilir.

3.2.2.28. Anahtar L2 loop'ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.

3.2.2.29. Anahtar REP, ERPS veya üreticinin eşdeğer ring/loop koruma protokolünü desteklemelidir.

3.2.2.30. Fiber optik arayüzlerde, bağlantıların tek yönlü olarak fiber optik kablolarla veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan UniDirectional Link Detection(UDLD) özelliği bulunmalıdır.

3.2.2.31. Anahtar 802.1Q trunk yapılandırmasını desteklemelidir; üreticiye özel otomatik trunk oluşturma protokolleri zorunlu değildir.

3.2.2.32. Anahtar IEEE 802.3ad - LACP desteklemelidir. Cihaz üzerinde minimum 8 adet 10/100/1000 ya da 1000BaseX port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.

3.2.2.33. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.

3.2.2.34. Anahtar en az 32.000 adet IPv4 veya 16.000 adet IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.

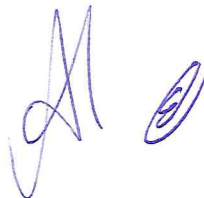
3.2.2.35. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme, ve dinamik yönlendirme protokollerinden en az OSPF desteklemelidir; RIP desteği zorunlu değildir.

3.2.2.36. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir

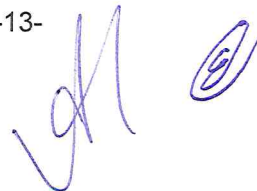
3.2.2.37. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.

3.2.2.38. Anahtar NetFlow, sFlow, IPFIX veya telemetry desteklemelidir. Flow/telemetry kapasitesi üretici dokümanı ile beyan edilmelidir.

- 3.2.2.39. Anahtarın IGMP v1, v2 ve v3 desteđi olmalıdır.
- 3.2.2.40. Anahtarın IGMP snooping ve MLD snooping desteđi olmalıdır.
- 3.2.2.41. Anahtarın, IGMP filtering özelliđi bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
- 3.2.2.42. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
- 3.2.2.43. Anahtar, TACACS+ desteđiyle ađ güvenliđinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
- 3.2.2.44. Cihaz, paketleri L2 bařlıđındaki kaynak/hedef MAC adresi, L3 bařlıđındaki kaynak/hedef IP adresi, L4 bařlıđındaki TCP/UDP port numarası bilgilerine göre eriřim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan eriřim denetim listeleri zamana bađlı olarak aktif hale getirilebilmelidir.
- 3.2.2.45. Eriřim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
- 3.2.2.46. Eriřim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
- 3.2.2.47. Anahtar en az 5000 adet ACL desteđine sahip olmalıdır.
- 3.2.2.48. Anahtar her porttan belirlenen adet kadar MAC adresinin bađlantı kurmasını sađlayabilmelidir. Belirlenen limit dıřındaki MAC adresleri isteđe bađlı olarak belirlendiđinde port kapatılabilmeli veya limit dıřı MAC adreslerinin bađlanması engellenebilmelidir.
- 3.2.2.49. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
- 3.2.2.50. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilmelidir. Anahtar yetkilendirme deđiřikliklerinde tekrar kimlik dođrulama iřlemi gerektirmemelidir (CoA-Change of Authorization).
- 3.2.2.51. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik dođrulama yapılabilmelidir.
- 3.2.2.52. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik dođrulama iřlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.
- 3.2.2.53. Aynı porttan birden fazla istemci bađlandığında her biri için ayrı ayrı 802.1x kimlik dođrulama yapılabilmelidir.
- 3.2.2.54. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteđi bulunmalıdır.
- 3.2.2.55. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
- 3.2.2.56. Anahtar uplink portlarında ve üreticinin desteklediđi port tiplerinde IEEE 802.1AE MACsec desteklemelidir; tüm downlink portlarında MACsec zorunlu deđildir.



- 3.2.2.57. Anahtar Voice VLAN yaratılmasını destekleyecektir. Bu sayede IEEE 802.1p class of service (CoS) uyumlu IP telefonların otomatik olarak tanınması ve Voice Vlan a eklenmesine olanak sağlamalıdır.
- 3.2.2.58. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Egress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
- 3.2.2.59. Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilmelidir.
- 3.2.2.60. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilir (Rate Limiting).
- 3.2.2.61. Anahtarın IPV4 ve IPV6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
- 3.2.2.62. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPV4 ve IPV6 için desteklenmelidir.
- 3.2.2.63. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) vefarklı anahtarlar arasında (RSPAN, ERSPAN veya üreticinin eşdeğer uzak aynalama teknolojisi ile) aynalama yeteneği olmalıdır.
- 3.2.2.64. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilir.
- 3.2.2.65. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
- 3.2.2.66. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilen NTP protokolünü desteklemelidir.
- 3.2.2.67. Anahtar, SNMP v1, v2c, v3, telnet ve/veya Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
- 3.2.2.68. Anahtar SNMP trap yeteneğine sahip olmalıdır.
- 3.2.2.69. En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPV4 hem IPV6 istemcilere servis sağlayabilmelidir.
- 3.2.2.70. Cihaz aynı anda en az 5 eşzamanlı SSH v2 bağlantısını desteklemelidir; telnet desteği opsiyoneldir.
- 3.2.2.71. Anahtar 10/100/1000 bakır portlarında TDR (time domain reflector) desteklemelidir. Bu sayede cihaz, bu portlardaki kablolama hatalarını teşhis edebilmeli, kabloda kopukluk olması durumunda ne kadar uzakta olduğunu tespit edebilmelidir.
- 3.2.2.72. Anahtar yukarıdaki maddelere ek olarak istenmesi halinde ek lisans paketi ile ya da lisans arttırımı ile aşağıdaki özelliklerin tamamını sağlayabilmelidir. Eğer lisans arttırımı ile sağlanamıyor ise doğrudan aşağıdaki özellikleri destekleyecek şekilde teklif edilmelidir.
- 3.2.2.72.1. Anahtar L3 statik yönlendirme ve IPV4 ve IPV6 dinamik yönlendirme protokollerinden RIP, RIPng, OSPF, OSPFv3, BGP, multiprotocol BGP ve IS-IS desteklemelidir.



3.2.2.72.2. Anahtar OSPF ve BGP protokolleri için NSF (non-stop forwarding) desteklemelidir.

3.2.2.72.3. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtar port aynalama yöntemlerinden SPAN, RSPAN ve ERSPAN özellikleri olmalıdır.

3.2.2.72.4. Anahtar anormallik tespiti yapabilen sistemler tarafından kullanılmak üzere, şifrelenmiş trafiklerle ilgili, şifrelemeyi açmadan analitik bilgileroluşturabilmeli ve netflow/IPFIX/telemetry üzerinden paylaşabilmelidir veya üreticinin eşdeğer güvenlik görünürlük teknolojisini desteklemelidir.

3.2.2.72.5. Anahtar veya üreticinin merkezi yönetim platformu uygulama tanıma, uygulama tabanlı QoS ve raporlama özelliklerini desteklemelidir; uygulama tanıma anahtar üzerinde veya merkezi yönetim platformunda yapılabilir.

3.2.2.72.6. Anahtarın işletim sistemi yazılım seviyesini değiştirmeden belli hataları düzeltmek için üretilen yamalama (Patch) yeteneğine sahip olmalıdır.

3.2.2.72.7. Anahtar packet capture (PCAP) veya eşdeğer paket yakalama desteğine sahip olmalıdır. Anahtar üzerindeki herhangi iki port arasındaki trafik yakalanıp PCAP formatında dışa aktarılabilmeli veya Wireshark uygulaması kurulu bir sisteme gönderilebilmelidir.

3.2.2.72.8. Anahtar HSRP, VRRP veya üreticinin eşdeğer üçüncü katman yedekleme protokolünü desteklemelidir.

3.2.2.72.9. Anahtar en az 8000 adet multicast route kapasitesine sahip olmalı ve L3 multicast protokollerinden en az PIM-Sparse ve Source-Specific Multicast (SSM) desteği bulunmalıdır; PIM-Bidir ve MSDP desteği opsiyoneldir.

3.2.2.72.10. Anahtar, MACsec ihtiyacı olan bağlantılar için AES-256 tabanlı IEEE 802.1AE MACsec destekli yeterli sayıda port sağlamalıdır; tüm uplink ve downlink portlarında MACsec zorunlu değildir.

3.2.2.72.11. Anahtar VRF-lite ve GRE desteklemelidir; L3-MPLS-VPN ve L2VPN (EoMPLS, VPLS) desteği opsiyoneldir.

3.2.2.72.12. Anahtar bir uç noktaya olan erişimin kalitesini (paket kaybı, gecikme, jitter) ölçmek için IP SLA veya üreticinin eşdeğer performans izleme teknolojisi desteğine sahip olmalıdır.

3.2.2.73. Anahtar standard üretici garantisine ek olarak 3 yıllık 8X7NCD ile teklif edilmelidir.

3.2.3. Omurga Ethernet Anahtar

3.2.3.1. Anahtar üzerinde en az 48 adet 1/10/25 ve 4 adet 40/100 Gbps fiber port bulunmalıdır.

3.2.3.2. Anahtarlama kapasitesi en az 3.2 Tbps olmalıdır. Anahtarın yönlendirme performans değeri en az 1 Bpps olmalıdır.

3.2.3.3. Anahtaren az 32MB buffer'a sahip olmalıdır.

3.2.3.4. Anahtar IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.

3.2.3.5. Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir. Anahtar dahili yedek güç kaynağı ile birlikte teklif edilmelidir.

- 3.2.3.6. Anahtar modüler ve N+1 veya 1+1 yedekli çalışan fan'lara sahip olmalıdır.
- 3.2.3.7. Anahtar programlanabilir bir ASIC'e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.
- 3.2.3.8. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.
- 3.2.3.9. Anahtar üzerinde üçüncü parti container çalıştırma ve harici USB/SSD desteği zorunlu olmayıp opsiyonel kabul edilecektir. Cihaz üzerinde uygulama barındırma (container) ve harici SSD desteği bulunması tercih sebebidir.
- 3.2.3.10. Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini ve cihaz üzerinde Python scripting desteklemelidir.
- 3.2.3.11. Anahtar en az 16Gb DRAM ve 16Gb Flash belleğe sahip olmalıdır.
- 3.2.3.12. Anahtar üzerinde en az bir adet USB 2.0 ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır.
- 3.2.3.13. Anahtarın 9100 byte'lık jumbo frame desteği olmalıdır.
- 3.2.3.14. Anahtar envanter yönetimi için RFID etiketi, barkod/QR kod, seri numarası veya üreticinin eşdeğer envanter yöntemine sahip olmalıdır.
- 3.2.3.15. Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi içinaçılıp kapatılabilen locator LED/beacon (Blue Beacon veya eşdeğeri) desteğine sahip olmalıdır.
- 3.2.3.16. Anahtar yazılımsal olarak Bluetooth desteğine sahip olmalıdır. Opsiyonel olarak bağlanacak bluetooth aparatı üzerinden anahtarın WEB ve komut arayüzüne erişmek, log ve işletim sistemi transferi yapmak mümkün olmalıdır.
- 3.2.3.17. Anahtar en az 82.000 adet MAC adresi desteklenmelidir.
- 3.2.3.18. En az 4000 adet aktif VLAN desteği olmalıdır.
- 3.2.3.19. IEEE 802.1d Spanning Tree Protocol(STP), 802.1w Rapid Spanning Tree ve 802.1s Multiple Spanning Tree Protocol (MSTP) desteklenmelidir. Vlan'ler arası yük dengelemesi için 802.1d ve 802.1w protokolleri her VLAN için ayrı ayrı çalıştırılabilir.
- 3.2.3.20. Anahtar L2 loop'ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
- 3.2.3.21. Anahtar REP, ERPS veya üreticinin eşdeğer ring/loop koruma protokolünü desteklemelidir.
- 3.2.3.22. Fiberoptik arayüzlerde, bağlantıların tek yönlü olarak fiberoptik kablolama veya port hatalarından dolayı arızalanması durumunda bunu algılayan ve tek yönlü olan linkleri kapatan UniDirectional Link Detection özelliği bulunmalıdır.
- 3.2.3.23. Anahtar 802.1Q trunk yapılandırmasını desteklemelidir; üreticiye özel otomatik trunk oluşturma protokolleri zorunlu değildir.



- 3.2.3.24. Anahtar IEEE 802.3ad - LACP desteklemelidir. Cihaz üzerinde minimum 8 adet 10/100/1000 ya da 1000BaseX port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.
- 3.2.3.25. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.
- 3.2.3.26. Anahtar en az 64.000 adet IPv4 veya 32.000 adet IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.
- 3.2.3.27. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme, ve dinamik yönlendirme protokollerinden en az OSPF desteklemelidir; RIP desteği zorunlu değildir.
- 3.2.3.28. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir
- 3.2.3.29. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
- 3.2.3.30. AnahtarNetFlow, sFlow, IPFIX veya telemetry desteklemelidir. Flow/telemetry kapasitesi üretici dokümanı ile beyan edilmelidir.
- 3.2.3.31. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
- 3.2.3.32. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.
- 3.2.3.33. Anahtaren az 8.000 adet IGMP snooping girdisi desteklemelidir.
- 3.2.3.34. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
- 3.2.3.35. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
- 3.2.3.36. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
- 3.2.3.37. Cihaz, paketleri L2 başlığındaki kaynak/hedef MAC adresi, L3 başlığındaki kaynak/hedef IP adresi, L4 başlığındaki TCP/UDP port numarası bilgilerine göre erişim denetiminden (ACL) geçirebilmelidir. Cihaz üzerinde tanımlanan erişim denetim listeleri zamana bağlı olarak aktif hale getirilebilmelidir.
- 3.2.3.38. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
- 3.2.3.39. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
- 3.2.3.40. Anahtar en az 5000 adet ACL desteğine sahip olmalıdır.
- 3.2.3.41. Anahtar her porttan belirlenen adet kadar MAC adresinin bağlantı kurmasını sağlayabilmelidir. Belirlenen limit dışındaki MAC adresleri isteğe bağlı olarak belirlendiğinde port kapatılabilmeli veya limit dışı MAC adreslerinin bağlanması engellenebilmelidir.
- 3.2.3.42. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.

- 3.2.3.43. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
- 3.2.3.44. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapılabilir.
- 3.2.3.45. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilir ve bir HTTP sunucuya yönlendirme yapılabilir.
- 3.2.3.46. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilir.
- 3.2.3.47. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
- 3.2.3.48. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
- 3.2.3.49. Anahtar Voice VLAN yaratılmasını destekleyecektir. Bu sayede IEEE 802.1p class of service (CoS) uyumlu IP telefonların otomatik olarak tanınması ve Voice Vlan a eklenmesine olanak sağlamalıdır.
- 3.2.3.50. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Egress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
- 3.2.3.51. Anahtarın "QoS (Quality of Service)" desteği bulunmalıdır. Üçüncü seviyede (L3) DiffServ Code Point (IP ToS/DSCP) ya da ikinci seviyede (L2) IEEE 802.1p CoS (Class of Service) ile sınıflandırılmış paketlerin öncelik değerlerini anlayabilmeli, gerektiğinde bu öncelik değerlerini değiştirebilir.
- 3.2.3.52. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilir (Rate Limiting).
- 3.2.3.53. Anahtarın IPV4 ve IPV6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapılabilir.
- 3.2.3.54. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPV4 ve IPV6 için desteklenmelidir.
- 3.2.3.55. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) vefarklı anahtarlar arasında (RSPAN, ERSPAN veya üreticinin eşdeğer uzak aynalama teknolojisi ile) aynalama yeteneği olmalıdır.
- 3.2.3.56. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilir.
- 3.2.3.57. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
- 3.2.3.58. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilen NTP protokolünü desteklemelidir.
- 3.2.3.59. Anahtar, SNMP v1, v2c, v3, telnet ve/veya Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilir.
- 3.2.3.60. Anahtar SNMP trap yeteneğine sahip olmalıdır.

- 3.2.3.61. En az 4 grup RMON (history, statistics, alarms, events) desteđi olmalıdır. HTTP (web) yönetim sunucusu hem IPv4 hem IPv6 istemcilere servis sağlayabilmelidir.
- 3.2.3.62. Cihaz aynı anda en az 5 eşzamanlı SSH v2 bağlantısını desteklemelidir; telnet desteđi opsiyoneldir.
- 3.2.3.63. Anahtar L3 statik yönlendirme ve IPv4 ve IPV6 dinamik yönlendirme protokollerinden en az Full OSPF, OSPFv3, BGP ve multiprotocol BGP desteklemelidir; RIP, RIPng ve IS-IS desteđi opsiyoneldir.
- 3.2.3.64. Anahtar HSRP, VRRP veya üreticinin eşdeđer üçüncü katman yedekleme protokolünü desteklemelidir.
- 3.2.3.65. Anahtar en az 4 adet 25G ve 2 adet 100G portunda AES-256 tabanlı IEEE 802.1AE MACsec desteklemelidir; tüm uplink ve downlink portlarında MACsec zorunlu deđildir
- 3.2.3.66. Anahtar VRF/VRF-lite, GRE, VXLAN ve BGP-EVPN desteklemelidir; MPLS, L3-MPLS-VPN, L2VPN (EoMPLS, VPLS), LISP, TrustSec/CMD ve SGT üreticiye özel özellikler olup opsiyonel kabul edilecektir.
- 3.2.3.67. Anahtar istenmesi halinde yedeklilik için VPC, Virtual stacking veya benzeri bir özelliđi desteklemelidir.
- 3.2.3.68. Keşif sonuçlarına göre anahtar ile birlikte gerekli SFP ve DAC kablolar, yeterli adette teklife eklenmelidir.
- 3.2.3.69. Anahtar en az 3 yıllık 8x5xNBD üretici destek paketi ile teklif edilmelidir. Destek paketi Teknik destek, software güncelleme, ertesi iş günü deđişim haklarını içermelidir.



3.3. Ambalajlama ve Etiketleme İstekleri

3.3.1. Tüm donanım, yazılım ve benzeri cihaz ve malzemeler, orijinal ambalajlarında, kırılmaya, ezilmeye, toza, suya, neme, ısıya ve benzeri her türlü dış etken ve hasara karşı tüm önlemler alınmış olarak gönderilecektir (nakledilecek ve taşınacaktır).

3.3.2. Bütün nakliye ve taşıma masrafları yüklenici tarafından karşılanacaktır.

3.3.3. Tüm donanımlar üzerine, en az 3 cm eninde, en az 4 cm boyunda, yüklenici firma kaşesinin bulunduğu etiket yapıştırılacaktır. Etiket kolayca görünür yerde bulunacak ve üzerinde garanti süresinin başladığı ve bittiği tarih, arızalanması durumunda aranacak tlf. numarası veya fax numarası ve e-posta adresi yazılı olacaktır.

4. DENETİM VE MUAYENE

4.1. Fiziki Muayene: Mal teslim yerinde Ayniyat Müdürlüğü tarafından yapılacaktır. Ürünlerin sayımı, kullanılmamış olması, kırık, çizik, ambalaj ve deformasyon gibi hususların kontrolü maksadıyla el/göz ile muayene edilecektir.

4.2. Fonksiyon Muayenesi: Bilgi İşlem Daire Başkanlığı tarafından yapılacaktır. Satın alınan ürünlerin teknik şartname kriterlerini karşılayıp karşılamadığı canlı ortamda kontrol edilecektir.

5. EKLER

EK Topoloji Krokisi

TEKNİK ŞARTNAMEYİ HAZIRLAYANLAR


Mustafa Önderci
Network Yönetim
Uzmanı


Ensar Erdoğan
Bilgi Sistem Yönetim
Uzmanı

ONAYLAYAN


H. Volkan İslim
Bilgi İşlem Daire Başkanı

TOPOLOJİ KROKİSİ

