



İSTANBUL AYDIN ÜNİVERSİTESİ
KABLOSUZ ERİŞİM NOKTASI VE AĞ ANAHTARLARI ALIMI
TEKNİK ŞARTNAMESİ

SARTNAME NU: 2026-AĞ-SARTNAME

TARİH:

Temmuz 2026

1. Bu onaylı teknik şartname, yayım tarihinden itibaren yürürlüğe girer.
2. Bu onaylı teknik şartnamenin yürürlükten kaldırılma tarihi
30 Aralık 2028
3. Bu onaylı teknik şartname üzerinde değişiklik yapılamaz.
4. Bu onaylı teknik şartname kapak dâhil toplam 24 sayfadan ibarettir.

İÇİNDEKİLER

1. KONU	2
2. GENEL HUSUSLAR.....	2
3. İSTEK VE ÖZELLİKLER	5
4. DENETİM VE MUAYENE	21
5. EKLER	22



1. KONU

Bu teknik şartname, satın alınacak kablosuz erişim noktası ve ağ anahtarlarının 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. Resmî tatil günleri ve hafta sonu (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 ödmeden 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. Yüklenici

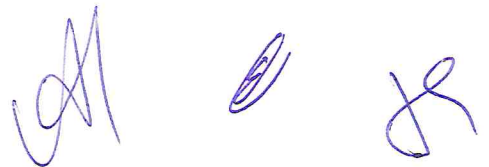
2.1.11.1. Başkası için yapı ve ticaretle ilgili bir işi yapmayı üstüne alan kimse, üstenci.

2.1.12. Yazılım

2.1.12.1 Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelerlerin 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
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 Emiting Diode
LLDP	Link Layer Discovery Protocol
MACsec	Media Access Control Security (IEEE 802.1AE)
mGig	Multigigabit Ethernet (IEEE 802.3bz)
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
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
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
VRP	Virtual Router Redundancy Protocol
VXLAN	Virtual Extensible LAN
°C	Santigrat derece

3. İSTEK VE ÖZELLİKLER

3.1. Genel İstekler

3.1.1. Bu şartname kapsamındaki donanımlar montaj, kurulum, konfigürasyon ve çalıştırılması dâhil, anahtar teslim 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 donanım ve donanım modülü ürünün üreticisi tarafından satıştan veya destekten kaldırılmamış olacaktır (end of sale / end 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 (ikiyüzirmisi) 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, 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.

3.2. Teknik İstekler

3.2.1. Ağ Donanımları

3.2.1.1. Kablosuz Erişim Noktası (Access Point-AP)

3.2.1.1.1. Önerilecek olan AP, 2,4 GHz, 5 GHz ve 6 GHz frekans bandında çalışabilecektir.

3.2.1.1.2. AP; 2.4 Ghz, 5 Ghz ve 6 Ghz için aynı anda 4x4 MU-MIMO destekleyecektir.

3.2.1.1.3. AP, Wifi Controller tarafından yönetilip istenilen SSID'lerin trafiğini merkezi, istenilen SSID'lerin trafiğini lokal olarak anahtarlatabilmelidir.

3.2.1.1.4. AP, 2.4 Ghz bandında ETSI standartlarında 13 adet çalışma kanalını desteklemelidir. 3 adet kablosuz erişim noktası aynı ortamda yan yana frekans örtüşmesi olmadan çalışabilmelidir.

3.2.1.1.5. AP yeni nesil 6 GHz frekans bandını destekleyen 802.11be, IEEE 802.11ax, ikinci nesil IEEE 802.11ac, IEEE 802.11n, IEEE 802.11a ve IEEE 802.11g standartlarını tam uyumlu olarak destekleyecektir.

3.2.1.1.6. AP, IEEE 802.11n için, en az 4x4 multiple-input, multiple-output (MIMO), 4 spatial streams, 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), cyclic shift diversity (CSD) ve 20, 40 MHz kanallarını desteklemelidir.

3.2.1.1.7. AP, IEEE 802.11ac için, en az 4x4 downlink multiple-input, multiple-output (MIMO), 4 spatial streams, 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), cyclic shift diversity (CSD) ve 20, 40, 80, 160 MHz kanallarını desteklemelidir. dual 4x4 160 MHz on 5 GHz desteği sunabilmelidir.

3.2.1.1.8. AP, IEEE 802.11ax için, en az 4x4 uplink/downlink multiple-input, multiple-output (MIMO), 4 spatial streams, 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), cyclic shift diversity (CSD) ve 20, 40, 80, 160 MHz kanallarını desteklemelidir. Uplink ve downlink yönünde OFDMA desteğine ek olarak BSS coloring desteği bulunmalıdır.

3.2.1.1.9. AP, IEEE 802.11be için, en az 4x4 uplink/downlink multiple-input, multiple-output (MIMO), 4 spatial streams, 802.11 dynamic frequency selection (DFS), maximal ratio combining (MRC), Preamble puncturing, Multilink operation, cyclic shift diversity (CSD) ve 20, 40, 80, 160, 320 MHz kanallarını desteklemelidir. Uplink ve downlink yönünde OFDMA desteğine ek olarak BSS coloring desteği bulunacaktır.

3.2.1.1.10. AP, 2.4 GHz, 5 GHz ve 6 GHz bantlarında RF optimizasyonu, parazit/girişim tespiti, otomatik kanal ve güç ayarlama özelliklerine sahip olmalıdır. Bu işlevler özel tarama radyosu, paylaşımlı radyo, yazılım tabanlı RF optimizasyonu, yapay zekâ destekli RF yönetimi veya üreticinin eşdeğer teknolojisi ile sağlanabilmelidir.

3.2.1.1.11. AP üzerinde konumlandırma ve IoT servisleri için GNSS/GPS, BLE, Zigbee/802.15.4, 802.11az FTM, BLE channel sounding, UWB veya üreticinin eşdeğer hassas konumlandırma teknolojilerinden biri veya birkaçı desteklenmelidir. UWB desteği zorunlu olmayıp eşdeğer hassas konumlandırma teknolojileri kabul edilecektir. AP üzerinde dahili sensör veya yazılımsal/harici aparat destekli konum doğrulama özelliği bulunmalıdır.

3.2.1.1.12. AP, 802.11be / Wi-Fi 7 standardını desteklemelidir. AP üzerinde 2.4 GHz, 5 GHz ve 6 GHz bantları için üç ayrı radyo bulunmalı ve her üç radyo da en az 4x4 MIMO desteklemelidir. AP, 6 GHz bandında 320 MHz, 5 GHz bandında en az 160 MHz kanal genişliğini desteklemelidir. Toplam teorik PHY/aggregate veri hızı en az 18 Gbps olmalıdır. AP üzerinde en az 1 adet 10GbE/mGig Ethernet portu bulunmalıdır.

3.2.1.2. Tip-1 Ağ Anahtarı

3.2.1.2.1. Anahtar üzerinde en az 48 adet 10M/100M/1G/2.5G/5G/10G destekli MgiG port bulunmalıdır. Herhangi bir fiber uplink portu kullanıldığında bu portlardan herhangi biri kullanım dışı kalmamalıdır.

3.2.1.2.2. Anahtarın uplink portları modüler uplink modülü, line-card veya modüler şasi mimarisi ile sağlanabilmelidir. Cihaz üzerinde en az 8 adet 1/10/25G SFP/SFP+/SFP28 veya en az 4 adet 40/100G QSFP/QSFP28 uplink portu sağlanmalıdır. Uplink portları teklif edilen cihaz üzerinde dahili, modüler uplink kartı veya line-card olarak sunulabilir.

3.2.1.2.3. Anahtar, IPv4 ve IPv6 protokolleri için tıkanmasız yapıda çalışmalıdır.

3.2.1.2.4. Anahtarın modüler güç kaynağı desteği olmalıdır. İstenmesi halinde ikinci ve üçüncü dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Yedek güç kaynakları anahtar çalışmaya devam ederken değiştirilebilmelidir. Anahtar en az 2 adet, her biri en az 1600W veya üzeri

kapasiteye sahip güç kaynağı ile teklif edilecektir. İstenmesi halinde üçüncü dahili güç kaynağı veya eşdeğer yedekli güç mimarisi desteklenmelidir.

3.2.1.2.5. Anahtar tüm downlink portlarında IEEE 802.3af, IEEE 802.3at ve IEEE 802.3bt Type 3/Type 4 PoE standartlarını desteklemelidir. Tüm downlink portlarında port başına 90W'a kadar PoE desteği, 802.3bt Class 8 veya üreticinin eşdeğer yüksek güçlü PoE teknolojisi ile sağlanmalıdır.

3.2.1.2.6. Cihaz istendiğinde tercih edilecek güç kaynağına göre en az 4320 Watt Toplam PoE kapasitesi sunabilmelidir.

3.2.1.2.7. Anahtarın veya teklif edilen modüler şasi/stack/virtual stack mimarisinin anahtarlama kapasitesi en az 1760 Gbps, L2 anahtarlama performansı en az 1300 Mpps olmalıdır. Yığınlama, virtual stacking, VSF, VSX, StackWise, modüler şasi veya eşdeğer mimari kullanılması halinde toplam sistem kapasitesi üretici dokümanları ile beyan edilmelidir.

3.2.1.2.8. Anahtar, cihaz/şasi genelinde toplam en az 32MB paket buffer kapasitesine sahip olmalıdır. Buffer değeri kart başına, ASIC başına veya paylaşımlı toplam olarak üretici dokümanı ile beyan edilebilir.

3.2.1.2.9. Anahtar modüler ve N+1 yedekli çalışan en az 3 adet fan desteklemelidir.

3.2.1.2.10. Anahtar programlanabilir bir ASIC'e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.

3.2.1.2.11. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.

3.2.1.2.12. Anahtar veya üreticinin merkezi yönetim/analitik platformu; REST API, telemetry, Python, otomasyon, izleme, olay analizi veya üreticinin eşdeğer ağ analitik/otomasyon özelliklerini desteklemelidir. Cihaz üzerinde üçüncü parti container çalıştırma ve harici SSD desteği zorunlu olmayıp opsiyonel kabul edilecektir; cihaz üzerinde üçüncü parti uygulama barındırma (container) ve harici SSD desteği bulunması tercih sebebidir.

3.2.1.2.13. Anahtar; NETCONF, RESTCONF, REST API, gNMI, OpenConfig, YANG, Python scripting veya üreticinin eşdeğer programlanabilir yönetim/otomasyon arayüzlerinden en az birini desteklemelidir.

3.2.1.2.14. Anahtar en az 16Gb DRAM ve 18 GB Flash belleğe sahip olmalıdır.

3.2.1.2.15. 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.

3.2.1.2.16. Anahtarın 9100 byte'lık jumbo frame desteği olmalıdır.

3.2.1.2.17. Anahtar; StackWise, VSF, VSX, MLAG, virtual stacking, modüler şasi veya üreticinin eşdeğer yüksek erişilebilirlik/yığınlama mimarisini desteklemelidir. Çözüm tek yönetim arayüzü, merkezi yönetim platformu veya üreticinin eşdeğer yönetim mimarisi ile yönetilebilmelidir. Farklı fiziksel anahtarlar veya modüller üzerinden LACP/port-channel, multi-chassis link aggregation, MLAG, VSX, StackWise veya eşdeğer bağlantı yedekliliği desteklenmelidir. Yığınlama/şasi/virtual stacking için gerekli modül, kablo, transceiver, DAC/AOC veya lisanslar teklif kapsamında sağlanmalıdır. Güç yedekliliği; yedek güç kaynağı, N+1/1+1 PSU mimarisi, modüler şasi güç havuzu veya üreticinin eşdeğer güç yedekliliği teknolojisi ile sağlanmalıdır. Power-stack kablosu zorunlu değildir.

3.2.1.2.18. Anahtar veya teklif edilen çözüm; yüksek erişilebilirlik, stateful failover, nonstop forwarding, ISSU, VSF/VSX, StackWise, modüler şasi yedekliliği veya üreticinin eşdeğer süreklilik teknolojilerinden en az birini desteklemelidir.

3.2.1.2.19. Anahtar en az 32.000 adet MAC adresi desteklenmelidir.

3.2.1.2.20. En az 4000 adet aktif VLAN desteği olmalıdır.

3.2.1.2.21. 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.

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

3.2.1.2.23. Anahtar REP, ERPS, MSTP/RSTP tabanlı koruma, loop protection veya üreticinin eşdeğer ring/loop protection teknolojilerinden en az birini desteklemelidir.

3.2.1.2.24. 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(UDLD) özelliği bulunmalıdır.

3.2.1.2.25. Anahtar 802.1Q VLAN trunking, LLDP/LLDP-MED ve statik trunk yapılandırmasını desteklemelidir. Üreticiye özel otomatik trunk protokolleri zorunlu değildir.

3.2.1.2.26. 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.

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

3.2.1.2.28. Anahtar en az 60.000 IPv4 ve 60.000 IPv6 route kapasitesine sahip olmalı; daha yüksek route ölçeği modül/lisans ile artırılabilir olması tercih sebebidir.

3.2.1.2.29. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme ve dinamik yönlendirme için OSPF/OSPFv3 veya BGP gibi standart yönlendirme protokollerinden en az birini desteklemelidir. EIGRP gibi üreticiye özel protokoller zorunlu değildir.

3.2.1.2.30. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir.

3.2.1.2.31. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.

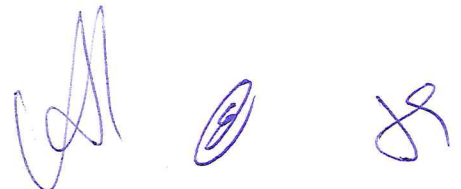
3.2.1.2.32. Anahtar NetFlow, Flexible NetFlow, IPFIX, sFlow, telemetry veya üreticinin eşdeğer trafik görünürlük teknolojilerinden en az birini desteklemelidir. Flow/telemetry kapasitesi üretici dokümanı ile beyan edilmelidir.

3.2.1.2.33. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.

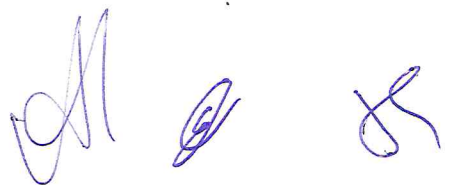
3.2.1.2.34. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.

3.2.1.2.35. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.

- 3.2.1.2.36. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
- 3.2.1.2.37. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
- 3.2.1.2.38. 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.
- 3.2.1.2.39. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
- 3.2.1.2.40. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
- 3.2.1.2.41. Anahtar en az 5000 adet ACL desteğine sahip olmalıdır.
- 3.2.1.2.42. 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.
- 3.2.1.2.43. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
- 3.2.1.2.44. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilirdir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
- 3.2.1.2.45. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapılabilirdir.
- 3.2.1.2.46. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilirdir ve bir HTTP sunucuya yönlendirme yapılabilirdir.
- 3.2.1.2.47. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilirdir.
- 3.2.1.2.48. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
- 3.2.1.2.49. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
- 3.2.1.2.50. Anahtar uplink/line-card portlarından en az 8 adet 25G veya en az 4 adet 100G port üzerinde IEEE 802.1AE MACsec (AES-256) desteği sağlamalıdır.
- 3.2.1.2.51. 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.
- 3.2.1.2.52. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Egress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.



- 3.2.1.2.53. 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.
- 3.2.1.2.54. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilir (Rate Limiting).
- 3.2.1.2.55. Anahtarın IPV4 ve IPV6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
- 3.2.1.2.56. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPV4 ve IPV6 için desteklenmelidir.
- 3.2.1.2.57. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN, ERSPAN veya üreticinin eşdeğer uzak aynalama teknolojisi ile) aynalama yeteneği olmalıdır.
- 3.2.1.2.58. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilir.
- 3.2.1.2.59. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
- 3.2.1.2.60. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilen NTP protokolünü desteklemelidir.
- 3.2.1.2.61. Anahtar, SNMP v1, v2c, v3, telnet ve/veya SSH v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözetilebilmelidir.
- 3.2.1.2.62. Anahtar SNMP trap yeteneğine sahip olmalıdır.
- 3.2.1.2.63. En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPV4 hem IPV6 istemcilere servis sağlayabilmelidir.
- 3.2.1.2.64. Cihaz aynı anda 5 adete kadar telnet ve/veya SSH bağlantısını ve 5 SSH bağlantısını destekleyebilmelidir.
- 3.2.1.2.65. Anahtar bakır portlarında TDR (time domain reflector) desteklemelidir. Bu sayede cihaz, bu portlardaki kablolu hatalarını teşhis edebilmeli, kabloda kopukluk olması durumunda ne kadar uzakta olduğunu tespit edebilmelidir.
- 3.2.1.2.66. Anahtar en az 3 yıllık 8x5xNBD üretici destek paketi ile birlikte teklif edilmelidir. Bu paket içerisinde 7x24 case açma yetkisi, software güncelleme hakkı ve arıza durumunda ertesi iş günü değişim dahil olmalıdır.
- 3.2.1.2.67. Anahtar yukarıdaki maddelere ek olarak istenmesi halinde lisans paketi eklenerek ya da artırılarak aşağıdaki özelliklerin tamamını sağlayabilmelidir. Eğer lisans arttırımı ile sağlanamıyor ise direkt olarak aşağıdaki özellikleri destekleyecek şekilde teklif edilmelidir.
- 3.2.1.2.68. Anahtar L3 statik yönlendirme ve IPV4 ve IPV6 dinamik yönlendirme protokollerinden RIP, RIPv2, OSPF, OSPFv3, BGP, multiprotocol BGP ve IS-IS desteklemelidir.
- 3.2.1.2.69. Anahtar OSPF ve BGP protokolleri için NSF (non-stop forwarding) desteklemelidir.



3.2.1.2.70. Anahtar veya üreticinin merkezi yönetim/güvenlik platformu, şifreli trafiği çözmeden anomali tespiti, flow analizi, telemetry, yapay zekâ destekli trafik analizi veya üreticinin eşdeğer güvenlik görünürlük teknolojisini desteklemelidir.

3.2.1.2.71. Anahtar veya üreticinin merkezi yönetim/güvenlik platformu uygulama görünürlüğü, uygulama tabanlı politika, QoS sınıflandırması veya trafik analizi özelliklerini desteklemelidir. Uygulama tanıma işlemi switch üzerinde, controller üzerinde veya merkezi yönetim platformu üzerinde yapılabilir.

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

3.2.1.2.73. Anahtar local/remote port mirroring, packet capture, PCAP export, SPAN/RSPAN/ERSPAN veya üreticinin eşdeğer trafik analiz yöntemlerinden en az birini desteklemelidir.

3.2.1.2.74. Anahtar HSRP, VRRP veya üreticinin eşdeğer first-hop redundancy protokolünü desteklemelidir.

3.2.1.2.75. Anahtar en az 8000 adet multicast route kapasitesine sahip olmalı ve L3 multicast protokollerinden en az PIM-Sparse ve SSM desteklenmelidir; PIM-BiDir ve MSDP opsiyoneldir.

3.2.1.2.76. Anahtar VRF/VRF-lite, EVPN/VXLAN, BGP-EVPN, GRE veya üreticinin eşdeğer segmentasyon/fabric teknolojilerinden en az birini desteklemelidir. MPLS, EoMPLS ve VPLS özellikleri zorunlu olmayıp opsiyonel kabul edilecektir.

3.2.1.2.77. Anahtar veya üreticinin yönetim/analitik platformu; paket kaybı, gecikme, jitter ve erişim kalitesini ölçmek için IP SLA, active monitoring, synthetic test, telemetry, NAE veya üreticinin eşdeğer performans izleme teknolojisini desteklemelidir.

3.2.1.3. Tip2 – Ağ Anahtarı

3.2.1.3.1. Anahtar üzerinde en az 48 adet 10/100/1000Mbps port ve 4 adet 10GbaseX bulunmalıdır. Herhangi bir fiber uplink portu kullanıldığında bu portlardan herhangi biri kullanım dışı kalmamalıdır.

3.2.1.3.2. Anahtarın bütün portlarında 802.3af (15W), 802.3at (30W) desteği olacaktır. İstenirse çift güç kaynağı ile 48 porttan aynı anda PoE (30W) sağlayabilecek donanıma sahip olmalıdır.

3.2.1.3.3. Anahtarın standalone anahtarlama kapasitesi en az 176 Gbps, L2 anahtarlama performansı en az 130 Mpps olmalıdır. Yığınlama, VSF, StackWise, virtual stacking veya eşdeğer mimari kullanılması halinde toplam sistem kapasitesi üretici dokümanları ile beyan edilmelidir.

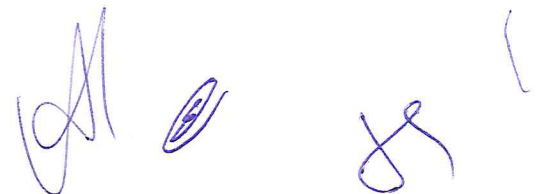
3.2.1.3.4. Anahtar üretici tarafından dokümente edilmiş paket buffer mimarisine sahip olmalıdır. Buffer değeri port başına, toplam veya shared buffer olarak beyan edilebilir.

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

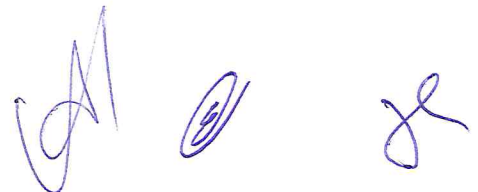
3.2.1.3.6. Anahtarın modüler güç kaynağı desteği olmalıdır. Anahtar en az bir adet güç kaynağı takılı olarak teklif edilecek; takılı güç kaynağı ile en az 700W PoE bütçesi sağlanacaktır. İstenmesi halinde ikinci bir dahili güç kaynağı, anahtar çalışmaya devam ederken (hot-swap) takılarak güç kaynağı yedeklemesi sağlanabilmelidir; ikinci güç kaynağı yuvası cihaz üzerinde hazır bulunacak ve boş yuva kapakla kapatılmış olarak teslim edilecektir.

3.2.1.3.7. Anahtar programlanabilir bir ASIC'e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.

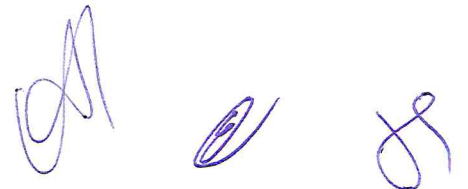
- 3.2.1.3.8. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.
- 3.2.1.3.9. Anahtar; NETCONF, RESTCONF, REST API, gNMI, OpenConfig, YANG, Python scripting veya üreticinin eşdeğer programlanabilir yönetim/otomasyon arayüzlerinden en az birini desteklemelidir.
- 3.2.1.3.10. Anahtar en az 2Gb DRAM ve 4Gb Flash belleğe sahip olmalıdır.
- 3.2.1.3.11. 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.
- 3.2.1.3.12. Anahtarın 9000 byte'lık jumbo frame desteği olmalıdır.
- 3.2.1.3.13. Anahtarın bakır portlarında 802.3az EEE (Energy Efficient Ethernet) desteği olmalıdır.
- 3.2.1.3.14. Anahtar seri numarası, LLDP, SNMP, API, merkezi yönetim platformu, barkod/QR kod, RFID veya üreticinin eşdeğer yöntemi ile envanterlenebilmelidir. Cihazın fiziksel konumunun tespiti LED locator, beacon, merkezi yönetim üzerinden cihaz bulma, LLDP/SNMP/API tabanlı envanter veya üreticinin eşdeğer yöntemiyle sağlanabilmelidir. Bluetooth desteği opsiyonel kabul edilecektir.
- 3.2.1.3.15. Anahtar istenmesi halinde StackWise, VSF, virtual stacking veya üreticinin eşdeğer stacking teknolojisiyle en az 8 üyeye kadar tek yönetim altında çalışabilmelidir. Yığınlama için dedicated stack port veya front-plane port kullanımı üretici mimarisine göre kabul edilecektir. Farklı üyeler üzerinden LACP/port-channel, multi-chassis etherchannel, VSF/VSX/MLAG veya eşdeğer bağlantı yedekliliği desteklenmelidir.
- 3.2.1.3.16. Anahtar veya stack/virtual stack çözümü; yüksek erişilebilirlik, protokol sürekliliği, stateful failover, nonstop forwarding, VSF/StackWise veya üreticinin eşdeğer HA mekanizmasını desteklemelidir.
- 3.2.1.3.17. Anahtar en az 16.000 adet MAC adresi desteklenmelidir.
- 3.2.1.3.18. 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.
- 3.2.1.3.19. Anahtar L2 loop'ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
- 3.2.1.3.20. 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(UDLD) özelliği bulunmalıdır.
- 3.2.1.3.21. Anahtar 802.1Q VLAN trunking, LLDP/LLDP-MED ve statik trunk yapılandırmasını desteklemelidir. Üreticiye özel otomatik trunk protokolleri zorunlu değildir.
- 3.2.1.3.22. 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.
- 3.2.1.3.23. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme ve dinamik yönlendirme için OSPF/OSPFv3 veya üreticinin eşdeğer L3 access routing teknolojisini desteklemelidir. RIP desteği zorunlu değildir.
- 3.2.1.3.24. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir.



- 3.2.1.3.25. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
- 3.2.1.3.26. Anahtar NetFlow, Flexible NetFlow, IPFIX, sFlow, telemetry veya üreticinin eşdeğer trafik görünürlük teknolojilerinden en az birini desteklemelidir. Flow/telemetry kapasitesi üretici dokümanı ile beyan edilmelidir.
- 3.2.1.3.27. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
- 3.2.1.3.28. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.
- 3.2.1.3.29. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
- 3.2.1.3.30. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
- 3.2.1.3.31. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
- 3.2.1.3.32. 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.
- 3.2.1.3.33. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
- 3.2.1.3.34. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
- 3.2.1.3.35. Anahtar en az 1500 adet ACL desteğine sahip olmalıdır.
- 3.2.1.3.36. 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.
- 3.2.1.3.37. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
- 3.2.1.3.38. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilmelidir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
- 3.2.1.3.39. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapılabilmelidir.
- 3.2.1.3.40. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.
- 3.2.1.3.41. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilmelidir.
- 3.2.1.3.42. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.



- 3.2.1.3.43. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
- 3.2.1.3.44. Anahtar, MACsec ihtiyacı olan bağlantılar için IEEE 802.1AE MACsec desteği sağlayabilmelidir. MACsec desteği uplink portlarında veya üreticinin desteklediği port tiplerinde sağlanabilir; tüm downlink portlarında MACsec zorunlu değildir.
- 3.2.1.3.45. 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.
- 3.2.1.3.46. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Egress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
- 3.2.1.3.47. 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.
- 3.2.1.3.48. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilir (Rate Limiting).
- 3.2.1.3.49. Anahtarın IPV4 ve IPV6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapılabilir.
- 3.2.1.3.50. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPV4 ve IPV6 için desteklenmelidir.
- 3.2.1.3.51. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN, ERSPAN veya üreticinin eşdeğer uzak aynalama teknolojisi ile) aynalama yeteneği olmalıdır.
- 3.2.1.3.52. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilir.
- 3.2.1.3.53. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
- 3.2.1.3.54. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecek NTP protokolünü desteklemelidir.
- 3.2.1.3.55. Anahtar, SNMP v1, v2c, v3, telnet ve/veya SSH v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
- 3.2.1.3.56. Anahtar SNMP trap yeteneğine sahip olmalıdır.
- 3.2.1.3.57. En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPV4 hem IPV6 istemcilere servis sağlayabilmelidir.
- 3.2.1.3.58. Cihaz telnet ve/veya SSH bağlantısını destekleyebilmelidir.
- 3.2.1.3.59. 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.



3.2.1.3.60. Anahtar L3 statik yönlendirme, IPv4/IPv6 inter-VLAN routing ve OSPF/OSPFv3 veya üreticinin eşdeğer L3 access routing teknolojisini desteklemelidir. RIP/RIPng desteği opsiyonel kabul edilecektir.

3.2.1.3.61. Anahtar istenmesi durumunda lisans veya yazılım özelliği ile OSPF/OSPFv3, BGP, VRRP, multicast routing, active monitoring/IP SLA veya üreticinin eşdeğer L3 ve performans izleme özelliklerini destekleyebilmelidir. EIGRP ve HSRP gibi üreticiye özel protokoller zorunlu değildir.

3.2.1.3.62. Anahtar veya üreticinin merkezi yönetim/güvenlik platformu, şifreli trafiği çözmeden anomali tespiti, flow analizi, telemetry, yapay zekâ destekli trafik analizi veya üreticinin eşdeğer güvenlik görünürlük teknolojisini desteklemelidir.

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

3.2.1.4. Tip3 Ağ Anahtarı

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

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

3.2.1.4.3. Anahtar en az 32 MB packet buffer'a veya üretici tarafından dokümente edilmiş eşdeğer buffer mimarisine sahip olmalıdır. Buffer değeri toplam/shared buffer olarak beyan edilebilir.

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

3.2.1.4.5. 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.

3.2.1.4.6. Anahtar modüler ve N+1 veya 1+1 yedekli çalışan fan'lara sahip olmalıdır.

3.2.1.4.7. Anahtar programlanabilir bir ASIC'e sahip olmalıdır. Yazılım güncellemesi ile ileride gereksinim desteği gerekebilecek olan yeni protokollerin de anahtarlanmasına açık olmalıdır.

3.2.1.4.8. Anahtarın kontrol ve yönetim katmanı için kullandığı işlemci mimarisi çok çekirdekli yapıda olmalıdır.

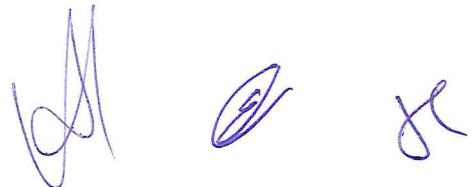
3.2.1.4.9. Anahtar veya üreticinin merkezi yönetim/analitik platformu; REST API, telemetry, Python, otomasyon, izleme, olay analizi veya üreticinin eşdeğer ağ analitik/otomasyon özelliklerini desteklemelidir. Cihaz üzerinde üçüncü parti container çalıştırma ve harici SSD desteği zorunlu olmayıp opsiyonel kabul edilecektir; cihaz üzerinde üçüncü parti uygulama barındırma (container) ve harici SSD desteği bulunması tercih sebebidir.

3.2.1.4.10. Anahtar; NETCONF, RESTCONF, REST API, gNMI, OpenConfig, YANG, Python scripting veya üreticinin eşdeğer programlanabilir yönetim/otomasyon arayüzlerinden en az birini desteklemelidir.

3.2.1.4.11. Anahtar en az 16Gb DRAM ve 16Gb Flash belleğe sahip olmalıdır.

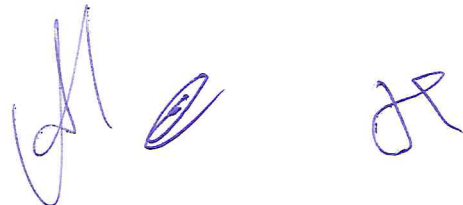
3.2.1.4.12. Anahtar üzerinde en az bir adet USB 2.0 ara yüz bulunmalıdır. Bu arayüz üzerinden anahtara işletim sistemi yüklemek veya log dosyalarını aktarmak mümkün olmalıdır.

- 3.2.1.4.13. Anahtarın 9100 byte'lık jumbo frame desteği olmalıdır.
- 3.2.1.4.14. Anahtar seri numarası, LLDP, SNMP, API, merkezi yönetim platformu, barkod/QR kod, RFID veya üreticinin eşdeğer yöntemi ile envanterlenebilmelidir. Cihazın fiziksel konumunun tespiti LED locator, beacon, merkezi yönetim üzerinden cihaz bulma, LLDP/SNMP/API tabanlı envanter veya üreticinin eşdeğer yöntemiyle sağlanabilmelidir. Bluetooth desteği opsiyonel kabul edilecektir.
- 3.2.1.4.15. Anahtar en az 82.000 adet MAC adresi desteklenmelidir.
- 3.2.1.4.16. En az 4000 adet aktif VLAN desteği olmalıdır.
- 3.2.1.4.17. 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 çalıştırılabilmelidir.
- 3.2.1.4.18. Anahtar L2 loop'ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
- 3.2.1.4.19. Anahtar REP, ERPS, MSTP/RSTP tabanlı koruma, loop protection veya üreticinin eşdeğer ring/loop protection teknolojilerinden en az birini desteklemelidir.
- 3.2.1.4.20. 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.
- 3.2.1.4.21. Anahtar 802.1Q VLAN trunking, LLDP/LLDP-MED ve statik trunk yapılandırmasını desteklemelidir. Üreticiye özel otomatik trunk protokolleri zorunlu değildir.
- 3.2.1.4.22. 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.
- 3.2.1.4.23. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.
- 3.2.1.4.24. Anahtar en az 64.000 adet IPv4 veya 32.000 adet IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.
- 3.2.1.4.25. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme ve dinamik yönlendirme için OSPF/OSPFv3, BGP veya üreticinin eşdeğer L3 routing teknolojilerinden en az birini desteklemelidir. RIP desteği zorunlu değildir.
- 3.2.1.4.26. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir
- 3.2.1.4.27. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
- 3.2.1.4.28. Anahtar NetFlow, Flexible NetFlow, IPFIX, sFlow, telemetry veya üreticinin eşdeğer trafik görünürlük teknolojilerinden en az birini desteklemelidir. Flow/telemetry kapasitesi üretici dokümanı ile beyan edilmelidir.
- 3.2.1.4.29. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
- 3.2.1.4.30. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.



- 3.2.1.4.31. Anahtar en az 8.000 adet IGMP snooping girdisi desteklemelidir.
- 3.2.1.4.32. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
- 3.2.1.4.33. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
- 3.2.1.4.34. Anahtar, TACACS+ desteğiyle ağ güvenliğinin bir TACACS sunucu tarafından yönetimini desteklemelidir.
- 3.2.1.4.35. 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.
- 3.2.1.4.36. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
- 3.2.1.4.37. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
- 3.2.1.4.38. Anahtar en az 5000 adet ACL desteğine sahip olmalıdır.
- 3.2.1.4.39. 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.
- 3.2.1.4.40. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
- 3.2.1.4.41. Anahtar 802.1x desteklemeli, bir RADIUS sunucu üzerinden dinamik ACL ve VLAN Ataması yapılabilirdir. Anahtar yetkilendirme değişikliklerinde tekrar kimlik doğrulama işlemi gerektirmemelidir (CoA-Change of Authorization).
- 3.2.1.4.42. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapabilmelidir.
- 3.2.1.4.43. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilirdi ve bir HTTP sunucuya yönlendirme yapılabilirdir.
- 3.2.1.4.44. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilirdir.
- 3.2.1.4.45. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
- 3.2.1.4.46. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
- 3.2.1.4.47. 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.
- 3.2.1.4.48. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Egress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.

- 3.2.1.4.49. 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.
- 3.2.1.4.50. Anahtar üzerindeki 10/100/1000 portlarının hızı sınırlandırılabilir (Rate Limiting).
- 3.2.1.4.51. Anahtarın IPV4 ve IPV6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
- 3.2.1.4.52. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPV4 ve IPV6 için desteklenmelidir.
- 3.2.1.4.53. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN, ERSPAN veya üreticinin eşdeğer uzak aynalama teknolojisi ile) aynalama yeteneği olmalıdır.
- 3.2.1.4.54. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilir.
- 3.2.1.4.55. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
- 3.2.1.4.56. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecek NTP protokolünü desteklemelidir.
- 3.2.1.4.57. Anahtar, SNMP v1, v2c, v3, telnet ve/veya SSH v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
- 3.2.1.4.58. Anahtar SNMP trap yeteneğine sahip olmalıdır.
- 3.2.1.4.59. En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPV4 hem IPV6 istemcilere servis sağlayabilmelidir.
- 3.2.1.4.60. Cihaz aynı anda 5 adete kadar telnet ve/veya SSH bağlantısını ve 5 SSH bağlantısını destekleyebilmelidir.
- 3.2.1.4.61. Anahtar HSRP, VRRP veya üreticinin eşdeğer first-hop redundancy protokolünü desteklemelidir.
- 3.2.1.4.62. Anahtar, MACsec ihtiyacı olan bağlantılar için IEEE 802.1AE MACsec desteği sağlayabilmelidir. MACsec desteği AES-128, AES-256 veya üreticinin desteklediği eşdeğer şifreleme yöntemiyle sağlanabilir. Tüm uplink ve downlink portlarında MACsec zorunlu değildir.
- 3.2.1.4.63. Anahtar VRF/VRF-lite, VXLAN, EVPN, BGP-EVPN, GRE veya üreticinin eşdeğer segmentasyon/fabric teknolojilerinden en az birini desteklemelidir. MPLS, L3-MPLS-VPN, L2VPN, EoMPLS, VPLS, LISP, TrustSec/CMD ve SGT gibi üreticiye özel veya servis sağlayıcı odaklı özellikler zorunlu olmayıp opsiyonel kabul edilecektir.
- 3.2.1.4.64. Anahtar istenmesi halinde yedeklilik için vPC, VSX, MLAG, StackWise Virtual, virtual stacking veya üreticinin eşdeğer çift cihaz yedeklilik teknolojilerinden birini desteklemelidir.
- 3.2.1.4.65. Keşif sonuçlarına göre anahtar ile birlikte gerekli SFP ve DAC kablolar, yeterli adette teklife eklenmelidir.



3.2.1.4.66. Anahtar en az 3 yıllık 8x5xNBD üretici destek paketi ile teklif edilmelidir. Destek paketi Teknik destek, software güncelleme, ertesi iş günü değişim haklarını içermelidir.

3.2.1.5. OEM 10GBASE-LR SFP+ Transceiver Modül

3.2.1.5.1. Hız ve Standart: Modüller SFP+ form faktöründe olmalı, IEEE 802.3ae 10GBASE-LR standardını ve en az 10 Gbps tam çift yönlü (Full-Duplex) iletim hızını desteklemelidir.

3.2.1.5.2. Tekli Mod (Single-Mode - SMF) altyapıya uygun olmalı, 1310 nm dalga boyunda çalışmalı ve standart fiber kablo (G.652) üzerinden en az 10 km mesafeye kadar kayıpsız iletim sağlamalıdır.

3.2.1.5.3. Üzerinde Duplex LC fiber optik konektör bulunmalı ve cihaz açıkken sökülüp takılabilmeyi sağlayan Hot-Swappable mimariye sahip olmalıdır.

3.2.1.5.4. Kurum envanterindeki aktif ağ cihazları (switch/router) ile donanımsal ve yazılımsal olarak %100 uyumlu olmalı; işletim sistemleri tarafından doğrudan tanınarak ek bir komut/lisans gerektirmeden tak-çalıştır çalışmalıdır.

3.2.1.5.5. DOM/DDM (Digital Diagnostic Monitoring) desteği sayesinde sıcaklık, voltaj ve optik güç (Tx/Rx) değerleri anlık izlenebilmeli; 0°C ila 70°C ticari sıcaklık aralığında kararlı çalışmalıdır.

3.2.1.5.6. Tip-1,Tip-2, Tip-3 Anahtarlar ile uyumlu olacaktır.

3.2.1.6. 10G/25G Dual-Rate LR SFP28 Transceiver Modül

3.2.1.6.1. Hız ve Standart: Modüller SFP28/SFP+ form faktöründe olmalı, çift hız (Dual-Rate) özelliğini destekleyerek hem 10GBASE-LR hem de 25GBASE-LR standartlarında en az 10 Gbps ve 25 Gbps tam çift yönlü (Full-Duplex) iletim hızlarında çalışacaktır.

3.2.1.6.2. Tekli Mod (Single-Mode - SMF) altyapıya uygun olmalı, 1310 nm dalga boyunda çalışmalı ve standart fiber kablo (G.652) üzerinden en az 10 km mesafeye kadar kayıpsız iletim sağlayacaktır.

3.2.1.6.3. Hot-Swappable mimariye sahip olacaktır.

3.2.1.6.4. Tak çalıştır mimariye sahip olacaktır.

3.2.1.6.5. DOM/DDM (Digital Diagnostic Monitoring) desteği sayesinde sıcaklık, voltaj ve optik güç (Tx/Rx) değerleri anlık izlenebilmeli; 0°C ila 70°C ticari sıcaklık aralığında kararlı çalışmalıdır.

3.2.1.6.6. Tip-1,Tip-2, Tip-3 Anahtarlar ile uyumlu, orijinal ürün olacak, OEM ürün olmayacaktır.

3.2.1.7 Identity Services Engine Lisansı (ISE)

3.2.1.7.1. Kurum bünyesinde kullanılmakta olan mevcut Cisco Identity Services Engine 3.0.0.458 altyapısının lisans yenilemesi yapılacaktır.

3.2.1.7.2. Mevcut sistemde 1 adet Cisco ISE Virtual Machine lisansı bulunduğundan, bu alım kapsamında 2 adet ilave Cisco ISE Virtual Machine lisansı sağlanacaktır.

3.2.1.7.3. Cisco Identity Services Engine Essentials Subscription lisansı, ISE-E-LIC SKU kodu ile 10.000 adet olarak sağlanacaktır.

3.2.1.7.4. Cisco Support Basic for ISE desteği, SVS-ISE-SUP-B SKU kodu ile 1 adet olarak sağlanacaktır.

3.2.1.7.5. Cisco Identity Services Engine Advantage Subscription lisansı, ISE-A-LIC SKU kodu ile 2.000 adet sağlanacaktır.

3.2.1.7.6. Cisco ISE Virtual Machine Common PID lisansı, R-ISE-VMC-K9= SKU kodu ile 2 adet sağlanacaktır.

3.2.1.7.7. Cisco ISE Virtual Machine yazılım desteği, CON-L1SW-RISE9KVM SKU kodu ile 2 adet sağlanacaktır.

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

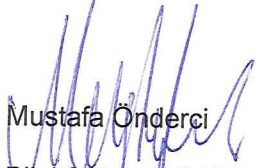
4.1. **Fiziki Muayene:** Mal teslim yerinde Ayniyat Müdürlüğü tarafından yapılacaktır. Ürünlerin sayımı, kullanılmamış olması, kırık, çizik, ambalaj ve deformasyon gibi hususların kontrolü maksadıyla el/göz ile muayene edilecektir.

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

5. EKLER

Topoloji Krokisi.

TEKNİK ŞARTNAMEYİ HAZIRLAYANLAR


Mustafa Önderci
Bilgi Sistem Ağ Uzmanı


Ensar Erdoğan
Bilgi Sistem Yönetim Uzmanı

ONAYLAYAN


H. Volkan İslim
Bilgi İşlem Daire Başkanı

TOPOLOJİ KROKİSİ

