İAOSB EBSO HİZMET BİNASI SWITCH VE ACCESS POINT

SATIN ALIM İŞİ TEKNİK ŞARTNAMESİ

Kurumumuzda mevcut network sistemleri Cisco Meraki portalı üzerinden yönetilmektedir. Teklif edilecek tüm ürünler Cisco Meraki portalından yönetilebilecek yapıda olmalıdırlar. Bunun için lisans gerekiyor ise en az 3 yıllık lisansları ile verilmelidir.

Access Point (25 Adet)

1.1. Erişim noktası 2.4Ghz frekans bandında 2x2:2 MU-MIMO özeliklerine sahip olmalıdır.
1.2. Erişim noktası 5Ghz frekans bandında 2x2:2 MU-MIMO özeliklerine sahip olmalıdır.
1.3. Erişim noktası 6Ghz frekans bandında 2x2:2 MU-MIMO özeliklerine sahip olmalıdır.
1.4. Erişim noktası Wifi 7 standardında çalışabilmelidir.
1.5. Erişim noktası kullanıcılara verdiği wifi hizmeti etkilenmeden 7x24 WIDS/WIPS ve spektrum analizi yapabilmelidir.
1.6. Erişim noktasının entegre bluetooth anteni bulunmalıdır.
1.7. Erişim noktası 20, 40, 80 ve 160Mhz'lik kanal genişliklerini destekleyebilmelidir.
1.8. Erişim noktası 802.11ax standardının gerekliliği olan DL-OFDMA, UL-OFDMA, TWT, BSS Coloring, UL MU-MIMO ve DL MU-MIMO desteklemelidir.
1.9. Erişim noktasının ihtiyaç duyduğu maksimum güç 30W olmalıdır.
1.10. Erişim noktası DC input sağlayan adaptör veya PoE üzerinden çalıştırılabilmelidir.
1.11. Erişim noktası en az 1 adet 100/1000/2.5G ethernet portuna sahip olmalıdır.
1.12. Erişim noktası ile beraber standart montaj kiti beraberinde teslim edilmelidir.
1.13. Erişim noktası üzerinde dahili Integrated omni-directional antenler bulunmalıdır. Anten kazanımları en az 2.4Ghz de 4dBi, 5Ghz de 5dBi ve 6Ghz de 5dbi olmalıdır.
1.14. Yüksek kullanım ömrü için cihaz üzerinde havalandırma delikleri bulunmamalı, kapalı tasarım olmalıdır.
1.15. Erişim noktası 9Gbps toplam teorik hız sağlayabilecek kapasiteye sahip olmalıdır.
1.16. Erişim noktası tak-çalıştır mantığında çalışmalı, hiçbir müdahale olmadan merkezi yönetim platformuna erişebilmeli ve kendisi için atanmış konfigürasyon ve yazılım versiyonunu çekerek çalışmaya başlayabilmelidir.
1.17. Her bir erişim noktası layer 2 izolasyon ve layer 4-7 firewall çalıştırabilmelidir. Firewall özelliğinin çalışması için trafiğin bir controller üzerine tünellenmesi gerekmemelidir, erişim noktası bu işlemleri kendisi yapabilecek kapasitede olmalıdır. Bu özellğin çalışması için gerekli lisans vs varsa teklife dahil edilmelidir.
1.18. Her bir erişim noktası QoS yeteneğine sahip olmalı, istemci/SSID başına bant genişliği ataması ve uygulama tabanlı traffic shaping desteklemelidir.
1.19. Erişim noktaları her bir SSID için ayrı izolasyon, firewall ve QoS politikaları uygulayabilmelidir.
1.20. Erişim noktaları farklı kullanıcı grupları için ayrı politikalar uygulayabilmelidir. Aynı SSID'ye bağlı kullanıcılara farklı VLAN, firewall, QoS politikaları atanabilmelidir. Bu atamalar herhangi bir Radius sunucusu üzerinden yapılabileceği gibi, cihaz tipine göre veya manüel de yapılabilmelidir.
1.21. Erişim noktalarının hotspot/misafir SSID desteği bulunmalıdır. Bağlanan kullanıcının bir URL'e yönlendirilmesi ve kimlik doğrulaması öncesi erişim denetimi erişim noktası tarafında gerçekleştirilmelidir.
1.22. Erişim noktası hotspot/misafir SSID erişimlerini bir radius sunucu üzerinden sağlayabileceği gibi sistem kendisi de ek bileşen gerekmeden bu bağlantılar için gerekli servisleri sunabilmelidir.
1.23. Erişim noktasının pre-shared key ile bağlanması gerekli cihazların yarattığı SSID kirliliğini azaltmak ve tek bir SSID altında birden fazla pre-shared key kullanılmasını

sağlamak için Identity Pre-Shared Key (iPSK) desteği bulunmalıdır. Bu özelliği bir Radius sunucu üzerinden sağlayabileceği gibi Radius sunucu ihtiyacı olmadan kendi yönetim platformu üzerinden de sağlayabilmelidir.

1.24. SSID'lerin yayınlanması ile ilgili takvimler oluşturulabilmeli, belli gün ve saatlerde yayın yapılması sağlanabilmelidir.
1.25. SSID yayınlarının hangi AP'lerde yapılacağı esnek şekilde belirlenebilmelidir.
1.26. Erişim noktalarının roaming'i iyileştirme amaçlı olarak 802.11r ve 802.11k desteği bulunmalıdır.
1.27. Erişim noktaları bağlanan istemcileri bir vlan'e düşürerek bağlantı sağlayabilecekleri gibi kendi IP adreslerine NAT'layarak da ağa bağlayabilmelidirler. Ayrıca istenirse SSID bazlı olarak merkezi bir noktaya tünelleme gerçekleştirebilecek yapı da desteklenmelidir.
1.28. Erişim noktaları SSID'lerde DHCP kullanımını zorunlu tutabilmeli ve statik IP'li cihazların bağlanmasını engelleyebilmelidirler.
1.29. Erişim noktaları yük dengelemesi sağlayabilmek adına 802.11v protokolünü desteklemelidir.
1.30. Farklı ortam ve ihtiyaçlara göre erişim noktaları farklı radyo profilleri kullanabilmelidir.
1.31. Erişim noktaları yayın hücre büyüklüklerini ayarlayabilecek mekanizmalara sahip olmalıdır.
1.32. Erişim noktaları kanal genişliklerinin otomatik olarak belirlenmesini desteklemelidir.
1.33. Erişim noktaları wIPS kapsamında istemci yayınında performans kaybı yaşatmaksızın sürekli RF taraması yapabilmeli, etraftaki korsan erişim noktalarını, taklit SSID, zararlı broadcast ve packet flood'ları yakalayabilmelidir. Korsan erişim noktası yayınları için kara liste veya beyaz listeler hazırlanabilmeli ve otomatik engelleme çalıştırılabilmelidir. Bu özellikler için gerekli ek lisans vb. varsa teklife eklenmelidir.
1.34. Erişim noktası lokasyon bazlı servisler için üzerine bağlı ya da bağlı olmayan wifi ve bluetooth istemcilerin kat planı üzerindeki kordinat bilgilerini ve sinyal seviyelerini API üzerinden 1 saniyelik hassasiyette paylaşabilmelidir. Bunun için gerekli ek bir lisans veya platform varsa teklife dahil edilmelidir.
1.35. Erişim noktası üzerinde entegre bir bluetooth anten bulunmalı ve bu anten aracılığıyla etraftaki bluetooth client'ları tespit edebilmeli, API vasıtasıyla onların kordinatlarını saniyelik güncellemeler şeklinde paylaşabilmelidir.
1.36. Erişim noktası bir beacon gibi davaranarak bluetooth üzerinden major, minor, UUID gibi değerleri yayınlayabilmelidir.
1.37. Üretici; yeni ve tavsiye edilen yazılım versiyonu çıkarttığında tüm erişim noktaları talep edilen zaman aralığında otomatik olarak ve kendi kendine yazılımlarını güncelleyebilmelidir. Yazılım güncellemesi yapılırken istemcilerin minimum etkilenmesi adına sıralı güncellemeyi sistem otomatik olarak ayarlayabilmelidir.
1.38. Bir erişim noktası üzerinden istenildiğinde spektrum analizi alınabilmelidir. Bu analizde tüm kanallardaki yoğunluk durumu ve çakışma yaşanan başka erişim noktaları raporlanmalıdır.
1.39. Erişim noktasının Hotspot 2.0 desteği bulunmalıdır.
1.40. Tüm erişim noktaları tek bir merkezi platform üzerinden yönetilmelidir. Bu platform üzerinden birden fazla lokasyon ayrı ayrı konfigürasyonlara sahip olacak şekilde çalışabilmelidir.
1.41. Aynı yönetim platformundan yönetilen erişim noktaları farklı lokasyonlarda farklı yazılım versiyonları kullanabilmelidir.
1.42. Bir lokasyondaki istemcilerin yarattıkları trafik miktarı, kullanılan uygulamalar ve uygulama bazlı trafik miktarları grafiksel ve liste olarak gösterilebilmelidir. Ayrıca aynı bilgiye istemci bazlı da ulaşmak mümkün olmalı, her bir istemcinin trafik miktarı ve bunların uygulama kırılımları görüntülenebilmelidir.

1.43. Erişim noktaları üzerlerinden geçen DHCP isteklerinin, RADIUS sorgulamalarının, DNS sorgulamalarının ve ARP sorgulamalarının cevaplarının gelip gelmediğini ve ne kadar sürede cevap geldiğini takip edebilmeli, merkezi yönetim platformunda bunu raporlayabilmeli ve bununla ilgili uyarılar gönderebilmelidir.
1.44. Sistem kablosuz ağa bağlanmaya çalılşan ve bağlanan kullanıcıların deneyimini, yaşadıkları problemleri, problemlerin tiplerini, bir önceki peryoda göre artış/azalış durumlarını ve sebeplerini raporlayabilmelidir. Bağlanma, kimlik doğrulama, DHCP'den IP alma ve DNS sorgulamasına cevap alma gibi kullanıcı deneyimi kriterlerindeki olumsuz artışlardan ağ yöneticisi haberdar edilmeli ve arayüz üzerinden trend değişikliklerini görebilmelidir.
1.45. Sistem kablosuz ağa bağlanmış olan kullanıcıların kablosuz ağında yaşadıkları trafik gecikmesi miktarını raporlayabilmeli, en çok gecikme yaşayan kullanıcı ve erişim noktalarını detaylandırabilmelidir.
1.46. Erişim noktaları kat planı üzerinde yerleştirilebilecekleri gibi entegre bir harita sistemi üzerinden de coğrafi lokasyonlarına yerleştirilebilmeli, harita görünümünden farklı lokasyonlar izlenebilmelidir.
1.47. Erişim noktası istemcilere hizmet vermeye devam ederken merkezi yönetim platformu üzerinden kablolu veya kablosuz arayüzünden packet capture sağlayabilmelidir. Packet capture çıktısı arayüzden incelenebileceği gibi pcap dosyası olarak export da edilebilmelidir.
1.48. Ağ yöneticisine gönderilecek olan bildirimler mail yolu ile gönderilebileceği gibi webhook olarak da alınabilmeli ve Chat uygulamalarına mesaj olarak ulaştırılması sağlanabilmelidir.
1.49. Merkezi yönetim plaformu üzerinde ağ yönetimi için rol bazlı erişim desteği bulunmalıdır. Tüm sistemin yöneticisi tam yetki veya read-only yetkilere sahip olabilmelidir. Buna ek olarak sistem; sadece belli lokasyonlara tam yetki, read-only veya monitor-only yetkiler verebilmesine olanak sağlamalıdır.
1.50. Erişim noktası istenildiğinde üzerindeki işletim sistemi dönüştürülerek aynı üreticiye ait kablosuz erişim kontrol cihazı üzerinden de yönetilebilmelidir.
1.51. Cihaz ile birlikte 3 yıllık merkezi yönetim yazılımı ve support paketi teklife dahil edilmelidir.

2. Tip 1 PoE SWITCH (12 adet)

2.1. Anahtarın en az 40 adet 10/100/1000Mbps ve 8 adet 2.5G multigigabit olmak üzere toplamda 48 adet downlink portu bulunmalıdır. Anahtar üzerinde uplink için en az 4 adet 10Gbps hızında SFP+ port bulunmalıdır.
2.2. Anahtarın tüm bakır portları PoE/PoE+ desteklemelidir. Her bakır portu 30W'a kadar güç verebilecek özellikte olmalıdır.
2.3. Anahtarın toplamda en az 740W PoE bütçesi bulunmalıdır.
2.4. Anahtar üzerindeki tüm portları tıkanmasız çalıştırabilecek anahtarlama performansına sahip olmalıdır, en az 200 Gbps anahtarlama performansına sahip olmalıdır.
2.5. Anahtarın MTBF değeri en az 390.000 saat olmalıdır.
2.6. Anahtar tak-çalıştır mantığında çalışmalı, hiçbir müdahale olmadan merkezi yönetim platformuna erişebilmeli ve kendisi için atanmış konfigürasyon ve yazılım versiyonunu çekerek çalışmaya başlayabilmelidir.
2.7. Tüm anahtarlar tek bir merkezi platform üzerinden yönetilmelidir. Bu platform üzerinden birden fazla lokasyon ayrı ayrı konfigürasyonlara sahip olacak şekilde çalışabilmelidir.

2.8. Aynı yönetim platformundan yönetilen anahtarlar farklı lokasyonlarda farklı yazılım versiyonları kullanabilmelidir.
2.9. Bir veya birden fazla anahtar içeren bir lokasyondaki istemcilerin yarattıkları trafik miktarı, kullanılan uygulamalar ve uygulama bazlı trafik miktarları grafiksel ve liste olarak gösterilebilmelidir. Ayrıca aynı bilgiye istemci bazlı da ulaşmak mümkün olmalı, her bir istemcinin trafik miktarı ve bunların uygulama kırılımları görüntülenebilmelidir.
2.10. Anahtar istemcilere hizmet vermeye devam ederken merkezi yönetim platformu üzerinden istenilen anahtar portu için packet capture sağlayabilmelidir. Packet capture çıktısı arayüzden incelenebileceği gibi pcap dosyası olarak export da edilebilmelidir.
2.11. Ağ yöneticisine gönderilecek olan bildirimler mail yolu ile gönderilebileceği gibi webhook olarak da alınabilmeli ve Chat uygulamalarına mesaj olarak ulaştırılması sağlanabilmelidir.
2.12. Merkezi yönetim plaformu üzerinde ağ yönetimi için rol bazlı erişim desteği bulunmalıdır. Tüm sistemin yöneticisi tam yetki veya read-only yetkilere sahip olabilmelidir. Buna ek olarak sistem; sadece belli lokasyonlara tam yetki, read-only veya monitor-only yetkiler verebilmesine olanak sağlamalıdır.
2.13. Üretici; yeni ve tavsiye edilen yazılım versiyonu çıkarttığında tüm anahtarlar talep edilen zaman aralığında otomatik olarak ve kendi kendine yazılımlarını güncelleyebilmelidir. Birden fazla anahtarın olduğu ortamlarda yazılım güncellemesi yapılırken istemcilerin minimum etkilenmesi adına sıralı güncellemeyi programlanabilmelidir.
2.14. Anahtar üzerindeki bakır portlar için kablo testi yapılabilmeli, kablonun tahmini uzunluğu tespit edilebilmeli, kablonun problemli çiftleri varsa görüntülenebilmelidir.
2.15. Merkezi yönetim platformu üzerinde her bir lokasyon için otomatik oluşmuş layer 2 ve layer 3 topoloji görüntüleri sağlanmalı, aynı üreticiye ait gateway, erişim noktası vb varsa onlar da topolojiye dahil olmalıdır.
2.16. Bir lokasyonda bulunan anahtarların portları birbirleri ile stack yapılsa da yapılmasa da toplu olarak yönetilebilmelidir. Bu toplu yönetim için anahtarların topolojideki yerleri veya birbirlerine bağlı olup olmamaları gerekli olmamalıdır. Portlar port numarası, VLAN, port tipi, trunk, access vb parametrelere göre filtrelenip topluca konfigürasyon yapılabilmelidir.
2.17. Anahtar link-aggregation desteklemeli ve 8 porta kadar link aggregation'a port eklenebilmelidir. Stack olanlarda ise ayrı stack üyelerinden portlar link-aggregation'a dahil edilebilmelidir.
2.18. Anahtar üzerinde port aynalama desteklenmelidir.
2.19. Anahtar IGMP snooping ve multicast filtering destteklemelidir.
2.20. Anahtarın 802.1x desteği bulunmalıdır. Portlar 802.1x, MAB ve hybrit kimlik doğrulama destekleyebilmelidir. Kimlik doğrulamada single-host, multi-host, multi-authentication ve multi-domain yöntemleri desteklenebilmelidir.
2.21. Anahtar hibrit kimlik doğrulamada MAB ve 802.1x sorgusunu eş zamanlı yaparak kimlik doğrulamayı hızlandırabilmelidir.
2.22. Anahtar NAC uygulamaları için kritik olan Radius CoA (change of authorization) özelliğini desteklemelidir.
2.23. Anahtar portların MAC sınırlaması, yapışkan MAC özellikleri ayarlanabilmelidir.
2.24. Anahtarın DHCP snooping desteği bulunmalı, DHCP sunucuları hem tespit edilebilmeli hem de izin verilebilmeli ya da bloklanabilmelidir.
2.25. Anahtarın dynamic ARP inspection desteği bulunmalıdır.
2.26. Anahtar IPv4 ve IPv6 ACL desteklemelidir.
2.27. Anahtar farklı group politikalarının ve politika içerisindeki erişim kontrol listelerinin (ACL) bir Radius tarafından dinamik olarak uygulanmasına izin vermelidir. Böylelikle bir kullanıcı kimlik doğrulamasından geçtiğinde bir erişim hakkına sahip olurken başka bir kullanıcı başka bir erişim hakkına sahip olabilmelidir.

2.28. Anahtar DHCP server'lık yapabileceği gibi DHCP relay işlemi de yapabilmelidir.
2.29. Anahtarın portları bir zaman çizelgesine bağlanarak istenen gün ve saatlerde açık ya da kapalı olması sağlanabilmelidir.
2.30. Anahtar ile birlikte en az 1 adet en az 1mt stack kablosu verilmelidir.
2.31. Anahtar portları birbirinden izole edilebilmeli, aynı VLAN'de dahi olsalar birbirlerine ulaşımları tamamen engellenebilmelidir.
2.32. Her bir anahtar ile birlikte en az 3 yıllık merkezi yönetim platformu lisansı teklife dahil edilmelidir. Ve bu lisansa yazılım ve donamım desteği dahil olmalıdır.

3. TİP 2 PoE SWITCH (2 adet)

3.1. Anahtarın en az 18 adet 10/100/1000Mbps ve 6 adet 2.5G multigigabit olmak üzere toplamda 24 adet downlink portu bulunmalıdır. Anahtar üzerinde uplink için en az 4 adet 10Gbps hızında SFP+ port bulunmalıdır.
3.2. Anahtarın tüm bakır portları PoE/PoE+ desteklemelidir. Her bakır portu 30W'a kadar güç verebilecek özellikte olmalıdır.
3.3. Anahtarın toplamda en az 370W PoE kapasitesi bulunmalıdır.
3.4. Anahtar üzerindeki tüm portları tıkanmasız çalıştırabilecek anahtarlama performansına sahip olmalıdır, en az 146 Gbps anahtarlama performansına sahip olmalıdır.
3.5. Anahtarın MTBF değeri en az 670.000 saat olmalıdır.
3.6. Anahtar tak-çalıştır mantığında çalışmalı, hiçbir müdahale olmadan merkezi yönetim platformuna erişebilmeli ve kendisi için atanmış konfigürasyon ve yazılım versiyonunu çekerek çalışmaya başlayabilmelidir.
3.7. Tüm anahtarlar tek bir merkezi platform üzerinden yönetilmelidir. Bu platform üzerinden birden fazla lokasyon ayrı ayrı konfigürasyonlara sahip olacak şekilde çalışabilmelidir.
3.8. Aynı yönetim platformundan yönetilen anahtarlar farklı lokasyonlarda farklı yazılım versiyonları kullanabilmelidir.
3.9. Bir veya birden fazla anahtar içeren bir lokasyondaki istemcilerin yarattıkları trafik miktarı, kullanılan uygulamalar ve uygulama bazlı trafik miktarları grafiksel ve liste olarak gösterilebilmelidir. Ayrıca aynı bilgiye istemci bazlı da ulaşmak mümkün olmalı, her bir istemcinin trafik miktarı ve bunların uygulama kırılımları görüntülenebilmelidir.
3.10. Anahtar istemcilere hizmet vermeye devam ederken merkezi yönetim platformu üzerinden istenilen anahtar portu için packet capture sağlayabilmelidir. Packet capture çıktısı arayüzden incelenebileceği gibi pcap dosyası olarak export da edilebilmelidir.
3.11. Ağ yöneticisine gönderilecek olan bildirimler mail yolu ile gönderilebileceği gibi webhook olarak da alınabilmeli ve Chat uygulamalarına mesaj olarak ulaştırılması sağlanabilmelidir.
3.12. Merkezi yönetim plaformu üzerinde ağ yönetimi için rol bazlı erişim desteği bulunmalıdır. Tüm sistemin yöneticisi tam yetki veya read-only yetkilere sahip olabilmelidir. Buna ek olarak sistem; sadece belli lokasyonlara tam yetki, read-only veya monitor-only yetkiler verebilmesine olanak sağlamalıdır.
3.13. Üretici; yeni ve tavsiye edilen yazılım versiyonu çıkarttığında tüm anahtarlar talep edilen zaman aralığında otomatik olarak ve kendi kendine yazılımlarını güncelleyebilmelidir. Birden fazla anahtarın olduğu ortamlarda yazılım güncellemesi yapılırken istemcilerin minimum etkilenmesi adına sıralı güncellemeyi programlanabilmelidir.
3.14. Anahtar üzerindeki bakır portlar için kablo testi yapılabilmeli, kablonun tahmini uzunluğu tespit edilebilmeli, kablonun problemli çiftleri varsa görüntülenebilmelidir.

3.15. Merkezi yönetim platformu üzerinde her bir lokasyon için otomatik oluşmuş layer 2 ve layer 3 topoloji görüntüleri sağlanmalı, aynı üreticiye ait gateway, erişim noktası vb varsa onlar da topolojiye dahil olmalıdır.
3.16. Bir lokasyonda bulunan anahtarların portları birbirleri ile stack yapılsa da yapılmasa da toplu olarak yönetilebilmelidir. Bu toplu yönetim için anahtarların topolojideki yerleri veya birbirlerine bağlı olup olmamaları gerekli olmamalıdır. Portlar port numarası, VLAN, port tipi, trunk, access vb parametrelere göre filtrelenip topluca konfigürasyon yapılabilmelidir.
3.17. Anahtar link-aggregation desteklemeli ve 8 porta kadar link aggregation'a port eklenebilmelidir. Stack olanlarda ise ayrı stack üyelerinden portlar link-aggregation'a dahil edilebilmelidir.
3.18. Anahtar üzerinde port aynalama desteklenmelidir.
3.19. Anahtar IGMP snooping ve multicast filtering destteklemelidir.
3.20. Anahtarın 802.1x desteği bulunmalıdır. Portlar 802.1x, MAB ve hybrit kimlik doğrulama destekleyebilmelidir. Kimlik doğrulamada single-host, multi-host, multi-authentication ve multi-domain yöntemleri desteklenebilmelidir.
3.21. Anahtar hibrit kimlik doğrulamada MAB ve 802.1x sorgusunu eş zamanlı yaparak kimlik doğrulamayı hızlandırabilmelidir.
3.22. Anahtar NAC uygulamaları için kritik olan Radius CoA (change of authorization) özelliğini desteklemelidir.
3.23. Anahtar portların MAC sınırlaması, yapışkan MAC özellikleri ayarlanabilmelidir.
3.24. Anahtarın DHCP snooping desteği bulunmalı, DHCP sunucuları hem tespit edilebilmeli hem de izin verilebilmeli ya da bloklanabilmelidir.
3.25. Anahtarın dynamic ARP inspection desteği bulunmalıdır.
3.26. Anahtar IPv4 ve IPv6 ACL desteklemelidir.
3.27. Anahtar farklı group politikalarının ve politika içerisindeki erişim kontrol listelerinin (ACL) bir Radius tarafından dinamik olarak uygulanmasına izin vermelidir. Böylelikle bir kullanıcı kimlik doğrulamasından geçtiğinde bir erişim hakkına sahip olurken başka bir kullanıcı başka bir erişim hakkına sahip olabilmelidir.
3.28. Anahtar DHCP server'lık yapabileceği gibi DHCP relay işlemi de yapabilmelidir.
3.29. Anahtarın portları bir zaman çizelgesine bağlanarak istenen gün ve saatlerde açık ya da kapalı olması sağlanabilmelidir.
3.30. Anahtar portları birbirinden izole edilebilmeli, aynı VLAN'de dahi olsalar birbirlerine ulaşımları tamamen engellenebilmelidir.
3.31. Her bir anahtar ile birlikte en az 3 yıllık merkezi yönetim platformu lisansı teklife dahil edilmelidir. Ve bu lisansa yazılım ve donamım desteği dahil olmalıdır.

4. Fiber Anahtar 2 adet

4.1. Üzerinde en az 24 adet 1/10/25 Gbps hızında çalışabilecek SFP28 yuva olacaktır.
4.2. Anahtar üzerinde en az 1 adet genişleme uplink yuvası olacaktır.
4.3. İleride istenildiği takdirde uplink modül yuvasına 8 adet 10 Gbps hızında RJ45 portu olan yada 8 adet 1/10/25 Gbps hızında SFP28 portu olan yada 2 adet 40/100 Gbps hızında QSFP28 portu yada 4 adet 40/100 Gbps hızında QSFP28 portu olan uplink modülleri takılabilecektir.
4.4. Yığınlanabilir (Stackable) veya şasi mimarisinde olabilecektir.
4.5. Yığınlama için özel yığınlama (stack) arayüzleri kullanılmalı ve yığın çalıştırıldığında hiçbir kullanıcı portu ve uplink portu kullanılmamalıdır. Bir yığın içinde en az 8 adet anahtar bulunmalıdır.
4.6. Anahtarın yığın (stack) bant genişliği en az 1 Tbps olacaktır.
4.7. Anahtarlar ile birlikte yığın kablosu teklife dahil edilecektir.

4.8. Yığındaki farklı anahtarlar üzerinden etherchannel yapmak mümkün olmalıdır. (multi-chassis etherchannel)
4.9. Anahtar, yığın içinde çalışırken istenildiğinde yığındaki diğer anahtarlarla güç kaynağı paylaşımı yapabilmeli, ya da istenildiğinde yığındaki güç havuzundan yararlanarak güç yedekli modda çalışabilmelidir. Güç kaynağı yığınlama olarak adlandırılan bu özellik için gerekli stack kabloları teklife dahil edilmelidir.
4.10. Anahtar en az Spanning Tree (802.1d, MST, Rapid), 802.1x, 802.3af, LACP, IGMP Snooping, DHCP Snooping özellikleri için SSO (Stateful Switchover) desteklemelidir.
4.11. Backplane kapasitesi en az 2000 Gbps'a kadar ölçeklenebilir olacaktır.
4.12. Toplam paket iletim kapasitesi en az 1488 Mpps'e kadar ölçeklenebilir olacaktır.
4.13. en az 16 GB DRAM ve en az 16 GB Flash bellek anahtar üzerinde olacaktır.
4.14. Üzerindeki işlemci en az 4 çekirdekli (quad core) ve en az 2.4 GHz hızında olacaktır.
4.15. En az 32.000 (otuzikibin) adet MAC adresi destekleyecektir.
4.16. En az 4000 adet aktif VLAN desteği olmalıdır.
4.17. Anahtarın 9100 byte'lık jumbo frame desteği olmalıdır.
4.18. 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 çalıştırılabilmelidir.
4.19. Port Isolation veya Private VLAN protokol desteği olacaktır.
4.20. Anahtar L2 loop'ları engelleme konusunda Spanning Tree yardımcı özelliklerinden, BPDU guard, Root Guard, LoopGuard özelliklerini desteklemelidir.
4.21. Anahtar Resilient Ethernet Protokolünü (REP) desteklemelidir.
4.22. 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(UDLD) özelliği bulunmalıdır.
4.23. Anahtarın iki cihaz arasında otomatik olarak L2 trunk oluşturmak için bir protokol desteği bulunmalıdır.
4.24. Anahtar IEEE 802.3ad- LACP desteklemelidir. Cihaz üzerinde minimum 8 adet port, aynı kanal altında toplanıp, tek port gibi çalışabilmelidir.
4.25. Anahtar, 802.1AB protokolünü desteklemelidir. Bu sayede kendisine doğrudan bağlı diğer anahtarları öğrenme (neighbor learning) özelliğine sahip olacaktır.
4.26. Anahtar en az 39.000 adet IPv4 veya 19.500 adet IPv6 route bilgisini tutabilecek bir donanım yapısına sahip olmalıdır.
4.27. Anahtar statik yönlendirme, VLAN'ler arası IP yönlendirme ve dinamik yönlendirme protokollerinden RIP ve OSPF desteklemelidir.
4.28. Anahtar VRRP gibi üçüncü katman bir yedekleme protokolü desteklemelidir.
4.29. Anahtar politika tabanlı yönlendirme (PBR) desteklemelidir.
4.30. Anahtar örnekleme yapmadan Netflow veya SFlow desteklemelidir. Üzerinde en az 128.000 adet flow bilgisi tutabilmelidir.
4.31. Anahtarın IGMP v1, v2 ve v3 desteği olmalıdır.
4.32. Anahtarın IGMP snooping ve MLD snooping desteği olmalıdır.
4.33. Anahtarın, IGMP filtering özelliği bulunacaktır. Bu sayede multicast grubuna üye olmayan kullanıcıların multicast yetkilendirmesi ve port bazında multicast yayın sınırlandırması yapılabilecektir.
4.34. Anahtar, RADIUS authentication, authorization ve accounting (AAA) servislerini desteklemelidir.
4.35. Anahtar, 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.

4.36. Erişim kontrol listeleri Port, VLAN ve SVI (Switched virtual interface) seviyesinde uygulanabilmelidir.
4.37. Erişim kontrol listeleri donanım tabanlı olarak kullanılmalıdır.
4.38. Anahtar en az 8000 adet ACL desteğine sahip olmalıdır.
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.
4.40. Anahtar DHCP, ARP ve IP ataklarını engellemek için DHCP snooping, Dynamic ARP Inspection ve IP Source Guard özelliklerine sahip olmalıdır.
4.41. 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).
4.42. 802.1x desteklemeyen cihazlar için bir RADIUS sunucu üzerinden MAC adres tabanlı kimlik doğrulama yapabilmelidir.
4.43. 802.1x desteklemeyen cihazlar için WEB tabanlı kimlik doğrulama işlemi yapılabilmeli ve bir HTTP sunucuya yönlendirme yapılabilmelidir.
4.44. Aynı porttan birden fazla istemci bağlandığında her biri için ayrı ayrı 802.1x kimlik doğrulama yapılabilmelidir.
4.45. Anahtarın 802.1x desteklemeyen istemciler için misafir VLAN desteği bulunmalıdır.
4.46. Anahtar kontrol katmanını korumak için CoPP (Control Plane Policing) desteklemelidir.
4.47. Anahtar hem uplink hem de downlink portlarında 802.1AE, MACSec desteklemelidir.
4.48. Anahtar en az 32MB paylaşımlı bir buffer'a sahip olmalıdır.
4.49. 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.
4.50. Anahtar üzerindeki her portun en az 8 adet çıkış öncelik kuyruğu (Engress Queue) bulunmalı ve kuyruk uzunluklarını kontrol ederek tıkanıklıkları engelleyen otomatik sistemi bulunmalıdır.
4.51. 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 değiştirebilmelidir.
4.52. Anahtarın IPV4 ve IPv6 için DHCP istemci ve sunucu desteği olmalıdır. Hem statik hem dinamik olarak istemcilere atamalar yapabilmelidir.
4.53. Anahtar uzak lokasyondaki DHCP sunuculara DHCP isteklerini iletmek için DHCP relay desteğine sahip olmalıdır. Bu özellik IPv4 ve IPv6 için desteklenmelidir.
4.54. Anahtarda detaylı gerçek zamanlı trafik analizi yapabilmek için VLAN ve port bazında port aynalama desteği bulunmalıdır. Anahtarın aynı anahtar üzerinde (SPAN) ve farklı anahtarlar arasında (RSPAN) aynalama yeteneği olmalıdır.
4.55. TFTP, FTP, SCP protokolleri ile işletim sistemi güncellemesi yapılabilmelidir.
4.56. Anahtar syslog sunuculara log gönderebilmeli, hata, kaynak kullanımı ve zaman aşımı gibi bilgileri raporlayabilmelidir. Raporlanacak bilgi başlıkları seçilebilir olmalıdır.
4.57. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilek NTP protokolünü desteklemelidir.
4.58. Anahtar, SNMP v1, v2c, v3, telnet, Secure Shell (SSH) v2, HTTP (web), SSL, konsol ve ethernet yönetim portu aracılığı ile yönetilebilmeli veya gözlenebilmelidir.
4.59. Anahtar SNMP trap yeteneğine sahip olmalıdır.
4.60. En az 4 grup RMON (history, statistics, alarms, events) desteği olmalıdır. HTTP (web) yönetim sunucusu hem IPv4 hem IPv6 istemcilere servis sağlayabilmelidir.

4.61. Anahtar aynı anda 16 adete kadar telnet bağlantısını ve 5 SSH bağlantısını destekleyebilmelidir.
4.62. Anahtar üzerinde en az 1 adet RJ45 veya 1 adet USB/mini-USB konsol portu olacaktır.
4.63. 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.
4.64. Anahtar 3. parti uygulamaların çalıştırılabileceği bir container altyapısı bulunmalı ve bu altyapıyı destekleyebilecek CPU ve bellek kapasitesi olmalıdır. Anahtar bu 3. Parti uygulamalar tarafından kullanılabilecek en az bir adet USB 3.0 SSD hafıza ara yüzüne sahip olmalıdır. İleride istendiği taktirde bu arayüze 240GB kapasitesine kadar pluggable USB3.0 SSD storage takılabilecektir.
4.65. Anahtarın işletim sistemi modern programlama dillerinden NETCONF, RESTCONF ve YANG modellerini ve cihaz üzerinde Python scripting desteklemelidir.
4.66. Anahtar üzerinde veri merkezi içinde yerinin kolay bulunabilmesi için açılıp kapatılabilen mavi ışık (Blue Beacon) desteğine sahip olmalıdır.
4.67. Anahtar envanter yönetimi için kullanılacak bir RFID etiketine sahip olmalıdır.
4.68. Anahtar Embedded Event Manager (EEM) destekleyecektir.
4.69. Anahtarın modüler güç kaynağı desteği olmalıdır. İkinci bir dahili güç kaynağı takılarak güç kaynağı yedeklemesine sahip olabilmelidir. Anahtarın üzerinde dahili yedek güç kaynağı bulunmalıdır. Yedek güç kaynağı anahtar çalışmaya devam ederken değiştirilebilmelidir.
4.70. Anahtar modüler ve N+1 yedekli çalışan fan'lara sahip olmalıdır.
4.71. Anahtar hat (link) yedekliliği sağlamak amacıyla flexlink veya flexlink+ özelliğini destekleyecektir.
4.72. Anahtarlar ileride istendiği taktirde lisans artımı ile HSRP 'yi (Hot-Standby Router Protocol – Hızlı Yedekli Yönlendirme Protokolü) destekleyecektir.
4.73. Anahtar gerektiğinde lisans artırımı ile ağ sanallaştırma ve izolasyon yöntemlerini desteklemek amacıyla VRF, VXLAN ve LISP mekanizmalarını desteklemelidir.
4.74. Anahtar ileride lisans artırımı ile BGP, IS-IS, PIM Sparse Mode (PIM-SM), Source-Specific Multicast (SSM) ve Multicast Source Discovery Protocol (MSDP) protokollerini destekleyebilecektir.
4.75. Anahtar, ömür boyu üretici garantisine sahip olacaktır.
4.76. Anahtar merkezi bir yazılım ile üzerinde politika tabanlı kurallar yazılabilip, konfigürasyon ve izleme yapılabilmesi için Software-Defined Networks (SDN) özelliklerini desteklemelidir. Bunun için gerekli lisanslar en az 3 yıllık olarak verilecektir. Yazılım desteği bu lisansların kapsamı dahilinde olacaktır.
4.77. Anahtarlar en az 3 yıl üretici firma garantisi altında olmalı ve hafta içi mesai saatlerinde üretici firmadan destek alınabilmelidir.

5. SFP Modüller

5.1. En az 20 adet teklif edilen ürün ile aynı marka tam uyumlu 10G LR Sfp teklife eklenilmelidir.

6. Çok Faktörlü Kimlik Doğrulama Yazılımı (5 adet)

6.1. Teklif edilecek yazılım, Cisco Meraki yönetim ara yüzüne güvenli erişim için gerekli olan aşağıdaki özellikleri sağlamalıdır.
6.2. Çözüm, kullanıcıların kimlik doğrulama için birden fazla cihaz kaydetmesine izin vermelidir.
6.3. Çözüm, kullanıcıların kimlik doğrulama için tercih edilen bir cihazı seçmesine izin vermelidir.

6.4. Çözüm, kullanıcıların birincil cihazları mevcut değilse alternatif bir cihaz (o kullanıcı için sağlanan) seçmesine izin vermelidir.
6.5. Çözüm, kullanıcıların idari iş yükünü azaltmak için cihazlarını güvenli bir şekilde yönetmesine izin vermelidir
6.6. Çözüm, kullanıcıların mobil bir akıllı telefona gönderilen bir anlık bildirimle kimlik doğrulaması yapmasına izin vermelidir
6.7. Çözüm, kullanıcıların bir SMS yöntemiyle kimlik doğrulaması yapmasına izin vermelidir
6.8. Çözüm, kimlik doğrulama için birden fazla Mobil Platformu desteklemelidir (iOS, Android, Windows Mobile, Akıllı Olmayan Telefonlar)
6.9. Çözüm, hem cep telefonları hem de dahili hatlar için bant dışı bir telefon görüşmesi yöntemiyle kimlik doğrulamasını desteklemelidir
6.10. Çözüm, bir donanım belirteci ile kimlik doğrulamasını desteklemelidir
6.11. Çözüm, herhangi bir üçüncü taraf OATH uyumlu donanım belirtecini desteklemelidir
6.12. Çözüm, üçüncü taraf Yubikey belirteçlerini desteklemelidir
6.13. Çözüm, bir mobil uygulamadan oluşturulan tek seferlik bir parola ile kimlik doğrulamasını desteklemelidir
6.14. Çözüm, kimlik doğrulaması için baypas kodları sağlamalıdır
6.15. Çözüm, herhangi bir veri veya ağ bağlantısı olmadan çalışabilen ikinci faktör kimlik doğrulama yöntemi sağlamalıdır
6.16. Çözüm, mobil uygulamanın bir QR kodu kullanılarak sağlanmasını desteklemelidir
6.17. Çözüm, mobil uygulamanın SMS yoluyla gönderilen bir bağlantı kullanılarak sağlanmasını desteklemelidir
6.18. Çözüm, IP Beyaz Listelemesini desteklemelidir
6.19. Çözüm, saat ve/veya gün bazında Güvenilir Cihazları desteklemelidir
6.20. Çözüm, bir web portalı üzerinden oturum açarken kullanıcılara tüm mevcut kimlik doğrulama seçenekleri için sezgisel olarak istemde bulunmalıdır
6.21. Çözüm, esneklik için yedek kimlik doğrulama cihazlarına sahip kullanıcıları desteklemelidir
6.22. Çözüm, tarayıcı tabanlı uygulamalarda kimlik doğrulaması için U2F belirteçlerini desteklemelidir
6.23. Çözüm, grup veya uygulamaya göre riski kontrol etmek için güncel olmayan tarayıcı yazılımına sahip kullanıcıları engellemek için özel politikalara izin vermelidir
6.24. Çözüm, grup ve/veya uygulamaya göre riski kontrol etmek için güncel olmayan tarayıcı yazılımına sahip kullanıcıları uyarmak/uyarmak (ancak engellemek değil) için özel politikalara izin vermelidir
6.25. Çözüm, grup veya uygulamaya göre riski kontrol etmek için güncel olmayan tarayıcıları kendi kendine düzeltmelerine yardımcı olmalıdır
6.26. Çözüm, grup veya uygulamaya göre riski kontrol etmek için belirli coğrafi konumlardaki kullanıcılar için kimlik doğrulamayı engellemek veya artırmak için özel politikalara izin vermelidir
6.27. Çözüm, grup veya uygulamaya göre riski kontrol etmek için jailbreak yapılmış/kök erişimli cihazlara sahip kullanıcıları engellemek için özel politikalara izin vermelidir
6.28. Çözüm, TOR ve I2P, HTTP/HTTPS proxy'leri veya anonim VPN'ler tarafından sağlananlar gibi bilinen anonim IP adreslerinden kaynaklanan kimlik doğrulama girişimlerini önlemek için özel politikalara izin vermelidir
6.29. Çözüm, grup veya uygulamaya göre riski kontrol etmek için bu cihazlarda kimlik doğrulamaları onaylarken mobil cihazlarda etkin bir ekran kilidi gerektirmesine izin vermelidir
6.30. Çözüm, grup veya uygulamaya göre riski kontrol etmek için bu cihazlarda kimlik doğrulamaları onaylarken mobil cihazlarda parmak izi/dokunmatik kimlik doğrulaması kullanımını gerektirmesine izin vermelidir

6.31. Çözüm, grup veya uygulamaya göre riski kontrol etmek için bu cihazlarda kimlik doğrulamaları onaylarken mobil cihazlarda tam disk şifrelemesi gerektirmesine izin vermelidir
6.32. Çözüm, mobil cihazlarda kimlik doğrulama uygulaması için güncel güvenlik yamaları gerektirmesine izin vermelidir Bu cihazlarda riski kontrol etmek için kimlik doğrulamaları, grup veya uygulamaya göre
6.33. Çözüm, grup veya uygulamaya göre riski kontrol etmek için kimlik doğrulama için kullanılabilen kimlik doğrulama yöntemlerini kısıtlamak üzere özel politikalara izin vermelidir
6.34. Çözüm, yönetici oturum açma işlemleri için iki faktörlü kimlik doğrulaması gerektirmelidir
6.35. Çözüm, yöneticilerin hangi kullanıcıların/grupların belirli kimlik doğrulama faktörlerine (yani push, telefon görüşmesi, SMS, vb.) erişebileceğini kontrol etmesine izin vermelidir
6.36. Çözüm, mevcut kullanıcıları AD'den senkronize etmek için otomatik sağlama araçları sağlamalıdır
6.37. Çözüm, kullanıcıların CSV içe aktarma yoluyla eklenmesine izin vermelidir
6.38. Çözüm, yöneticilerin kullanıcıları programatik olarak Restful API'leri aracılığıyla sağlamasını desteklemelidir
6.39. Çözüm, yöneticilerin dağıtım zaman dilimlerini azaltmak için son kullanıcılar için bir kendi kendine kayıt sürecini etkinleştirmesine izin vermelidir
6.40. Çözüm, yöneticilerin kullanıcıları bir e-posta yoluyla kaydetmesini ve sağlamasını desteklemelidir
6.41. Çözüm, yöneticilerin kullanıcıları e-posta yoluyla kaydediyorsa özel bir kayıt e-posta mesajı oluşturmasına izin vermelidir
6.42. Çözüm, yöneticilerin gruplar için kullanıcı üyeliğine göre belirli entegrasyonlar/uygulamalar için erişimi sınırlamasına izin vermelidir.
6.43. Teklif edilen yazılım 5 kullanıcı için en az 3 yıl sağlanmalıdır.