

T.C.
MERSİN ÜNİVERSİTESİ HASTANESİ

TEKLİF İSTEME FORMU

20/05/2025

İlan No : 2025-05-1888
İstem No : 80679
Alım No :
Talep Eden Birim : İdari Bölümler / Bilgi İşlem -Yazılım
Konu : SWITCH ALIM

G.T.

Talep Edilen Hasta :

Son Teslim Tarihi & Saat : 23/05/2025 17:00:00

S.No	Malzeme Açıklaması	Miktar	Birim	Birim Fiyat	Toplam Tutar	Marka	UBB kodu	Tesl. Süresi (Gün)
1	SWITCH, 48 PORTLU, POE	19	Adet					

Mersin Üniversitesi Hastanesince aşağıda cins,miktar ve özellikleri belirtilen malzemelerin satın alınmasına ihtiyaç duyulmuştur. Proforma faturanın aşağıdaki şartlara göre düzenlenerek Satınalma Bürosuna gönderilmesini rica ederim.

- 1-Tekliflerin yazılı olması,
- 2-İhale dökümanının tamamen okunup kabul edildiğinin belirtilmesi,
- 3-Teklif verilen malzemelerin teslim süreleri, barkod numarası, markaları ve ambalaj şekillerinin yazılması,
- 4-TL (Türk Lirası) olarak fiyat verilir,birim fiyatlarının rakamla ve yazıyla yazılması,
- 5-Üzerinde kazıntı,silinti,düzeltilme bulunmaması,
- 6-Ad,Soyad veya ticaret unvanı yazılmak suretiyle yetkili kişilerce imzalanmış olması,
- 7-Teklif verilmeyecekse FAKS mesajının bir açıklama ile gönderilmesi,
- 8- Malzemeler ilgili firma yetkilisince depoya teslim edilecektir.Kurum bilgisi ve izni dışında kargo ile yapılan malzeme,fatura,irsaliye teslimatları kesinlikle kabul edilmeyecektir.
- 9- Teklif verilen malzemelerin, idarenin kesin siparişine müteakip teslim sürelerinin teklif mektubunda bildirilmesi zorunludur.Teslim süresi ve opsiyon süresi bildirilmeyen teklifler kesinlikle kabul edilmeyecektir.
- Önemli 10- Fiyat teklif cetveline teslimat süreleri mutlaka yazılmalıdır**

TESLİMAT SÜRESİ,UBB KODU,MARKA BELİRTİLMİYEN TEKLİFLER DEĞERLENDİRME DIŞI OLACAKTIR,TEKLİFLER SIRA NUMARASINA GÖRE VERİLMELİDİR.

İrtibat Fax: 0324 241 00 90 TLF: 0324 241 00 00 - 22570-22593-22598

Mail adresi: hastanesatinalma@mersin.edu.tr

Fiyat opsiyonu en az 45 gün olacaktır.

Büyüamin Gültekin

Hastane Müdür Yrd.

NOT : İlanlarımız www.mersin.edu.tr adresinde yayımlanmaktadır.

48 Port PoE+ Switch Şartnamesi

1. Teklif edilecek cihaz üreticisi 2020'de açıklanan "Gartner Wired and Wireless LAN Infrastructure Magic Quadrant" sonuçlarında liderler (leaders) bölümünde yer almalıdır.
2. Anahtar üzerinde en az 48 adet 10Base-T/100Base-TX/1000Base-T port ve 4 adet 10Gbit SFP+ port bulunmalıdır. Aynı anda 52 port aktif olarak çalışabilmelidir.
3. IEEE 802.3af PoE ve IEEE 802.3at PoE+ özellikleri anahtar bazında tüm UTP portlarda standart olarak bulunmalıdır. Anahtar 370 Watt PoE bütçesi sağlamalıdır.
4. SFP+ portlara 1000BaseT, 1000BaseSX, 1000BaseLX, 10G SR ve 10G LR portlar takılabilmelidir. SFP/SFP+'lar Hot-Swappable olmalı cihaz çalışırken sökülüp takılabilmeli, bu işlem anahtarın çalışmasını etkilememelidir.
5. 10/100/1000 portlar Auto-MDIX özelliğine sahip olmalı böylelikle çapraz veya düz bağlantı ayarlaması otomatik olarak yapılmalıdır.
6. Cihazın anahtarlama kapasitesi en az 176 Gbps, data iletim kapasitesi en az 98 Mpps olmalıdır.
7. Birden fazla konfigürasyon dosyası tutulması için yeterli Flash bellek ile teklif edilmelidir.
8. İşletim sistemi (cihaz yazılımı) güncellenmesi esnasında yedeklilik için birbirinden bağımsız iki imaj desteği olmalıdır.
9. Latency (gecikme) değeri gigabit ve 10 gigabit portlar için 2 mikrosaniyeden fazla olmamalıdır.
10. Adres tablosunda en az 8000 adet MAC adresi desteği olmalıdır.
11. Anahtarın statik yönlendirme desteği olacaktır ve bu özelliklerin kullanılabilmesi için bir lisans gerekiyor ise teklife dahil edilecektir.
12. Yönlendirme tablosunda en az 512 adet IPv4, 512 adet IPv6 yön bilgisi tutulabilmelidir.
13. Anahtarın L3 VLAN interface desteği olmalıdır.
14. Anahtarın en az 12MB packet buffer kapasitesi olmalıdır.
15. IEEE 802.1Q (4,094 VLAN ID) VLAN ID'si işaretleme desteği ve en az 512 adet port bazında VLAN tanımlanabilmelidir. MVRP veya benzeri bir protokol ile otomatik olarak VLAN'ları öğrenebilmeli ve atama yapabilmelidir.
16. IEEE 802.1D STP, IEEE 802.1s MSTP, IEEE 802.1w RSTP protokollerini desteklemelidir.
17. BPDU ataklarına karşı STP BPDU port koruması bulunmalıdır. STP Root olarak seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı koruma özelliği bulunmalıdır.
18. İstek dışı multicast baskınlarına karşı IP multicast snooping desteği bulunmalıdır.
19. LACP (IEEE 802.3ad link-aggregation-control protocol) anahtar üzerinde desteklenecektir. IEEE 802.3ad link aggregation özelliği ile en az 8 portu destekleyen statik ve dinamik bağlantı noktası (Trunk veya LAG) oluşturulabilmelidir. IEEE 802.3ad link aggregation özelliği ile en az 8 adet bağlantı noktası (Trunk veya LAG) oluşturulabilmelidir.
20. Anahtarın en az 9200 byte büyüklüğünde yüksek boyutlu iletim birimi (Jumbo Frame) desteği bulunmalıdır.
21. Link Layer Discovery Protocol (LLDP) IEEE 802.1ab (sekiz yüz iki nokta bir AB) ve Cisco Discovery Protocol v2 (CDPv2) desteği ile lokal ağda bağlı bulunan cihazların yönetsel bilgileri alınabilmelidir. Protokole uyumlu IP Telefon gibi uç cihazların QoS ve Vlan gibi ayarlarının otomatik olarak yapılabilmesi için LLDP-MED protokolü desteği bulunmalıdır.
22. Gereksiz yayın trafiğinin engellenmesi için IGMP v1/v2/v3 desteği olmalıdır. Anahtar multicast veri trafiğinin sadece talep edilen sistemlerden alınmasını ve böylece ağın performansının korunmasını sağlayan IGMP snooping özelliğine sahip olmalıdır.
23. Anahtar (Multicast Listener Discovery) MLDv1, MLDv2 protokollerini desteklemelidir. Anahtar IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping özelliğine sahip olmalıdır.
24. IP kaynak/hedef adreslerine göre, UDP/TCP port numarasına göre Access Control List'ler (ACL) yazılabilmelidir.
25. Port güvenliği özelliği ile kullanıcı listeleri oluşturularak sadece belli MAC adreslerinin ilgili portlara bağlantı kurmasına izin verilebilmelidir. Bu sayede izinsiz kullanıcı ve cihazların ağa girişleri engellenebilmelidir.

Yusuf Turhan TEKİN
Mühendis

Doç. Dr. Evren DEĞİRMENCI
Mersin Üniversitesi Hastanesi
Koordinatör

26. RADIUS ve TACACS+ protokolleri ile kimlik tanımlama özelliklerini desteklemelidir. Anahtarı yönetmek isteyen kişiler Radius sorgulama protokolü tarafından sorgulanabilmelidirler.
27. IEEE 802.1x kimlik tanımlama protokolü desteği bulunmalıdır. Port bazında Web tabanlı ve MAC adresi tabanlı kimlik tanımlama metodunu desteklemelidir.
28. Port başına aynı anda birden fazla kimlik tanımlama metoduna (802.1x, Web Tabanlı, Mac Tabanlı) ve port başına aynı anda birden fazla 802.1x kullanıcısı desteği bulunmalıdır.
29. Kimlik kontrolüne bağlı dinamik VLAN ataması gerçekleştirilebilmelidir.
30. Kimlik kontrolüne bağlı erişim kontrolü (ACL) yapılabilirdir.
31. Yetkisiz kullanıcıların ağa erişmesini önlemek için trafiği filtrelemeye yada kaynakları korumak için ağ trafiğinin denetlenmesine sağlayan hem IPv4 hem de IPv6 için erişim kontrol listesi (ACL) desteği olmalıdır. Kurallar Layer2 üstbilgisi ve Layer3 protokol üstbilgisi ile sağlanabilmelidir.
32. ICMP DoS ataklarına karşın ICMP Throttling veya benzeri bir güvenlik metodunun desteği bulunmalıdır.
33. İstenmeyen ARP Broadcast saldırılarına karşın güvenlik önlemi olarak ARP koruması özelliği bulunmalıdır.
34. Port başına gereksiz yayın (broadcast) trafiğini engelleme mekanizması olmalıdır.
35. Hangi anahtarlama portlarının birbirleriyle görüşeceğini kontrol etmek için kaynak port filtrelemesi veya benzeri özelliği bulunmalıdır.
36. SSHv2 Secure Shell protokolü ile uzaktan güvenli şekilde yönetilebilir olmalıdır.
37. SNMP v1,v2,v3 ve RMON protokolleri desteklenmelidir. HTTPS protokolleri ile uzaktan yönetilebilir olmalıdır. Secure Sockets Layer (SSL) protokolü desteklenmelidir.
38. sFlow veya NetFlow gibi veri akışı izleme protokollerinin en az birinin desteği bulunmalıdır.
39. Network trafiğini takip etmek için Port-Monitoring özelliği bulunmalıdır.
40. TFTP Protocol (revision 2) dosya transfer protokolü desteği bulunmalıdır. TFTP protokolü ile anahtar yazılımı (firmware) güncellemesi yapılabilirdir. Anahtarın konfigürasyon yedeği Secure FTP veya benzeri bir protokol ile güvenli bir şekilde alınabilmelidir.
41. Anahtarın üzerinde USB portu olmalıdır.
42. Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı Uni-Directional Link Detection (UDLD) veya benzeri bir özellik desteklenecektir
43. IEEE 802.1p trafik önceliklendirme desteği olmalıdır. Strict priority (SP) queuing desteklenecektir. CoS Class of Service özelliği ile, 802.1p önceliklendirmeler IP adresi, IP Type of Service, Layer 3 protokol, TCP/UDP port numarası, DiffServ ve kaynak portuna göre yapılabilirdir. TCP/UDP Port numaralarına göre Layer 4 düzeyinde trafik önceliklendirme desteği olmalıdır.
44. Cihaz port trafiğini giriş ve çıkış (ingress/egress) bir izleme portuna yansıtmak için Port Mirroring desteğine sahip olmalıdır ve en az 4 yansıtm grubu desteklemelidir.
45. Anahtarın saat ve tarih bilgisi, ağ üzerindeki diğer tüm anahtarlarla senkron hale getirilebilecektir. Anahtarlama cihazı ağ üzerindeki tüm cihazlarla senkron olabilmek için NTP protokolünün desteklemelidir.
46. Ürün SDN temelli uygulamalar için REST API desteği olmalıdır.
47. Hız sınırlama (Rate Limiting) özelliği olmalıdır.
48. Anahtar IEEE 802.3az standartını desteklemelidir.
49. Anahtar yazılım güncellemeleri en az 10 (on) yıl boyunca ücretsiz yapılabilecek şekilde teklif verilmelidir
50. Ürün en az 5 (beş) yıl garantili olmalıdır. Garanti süresince oluşabilecek arızalarda onarım, güç kaynağı, modül gibi parça değişim veya ürün değişimi için herhangi bir ücret talep edilmeyecek şekilde teklif verilmelidir.
51. Her bir ürünle birlikte 10G SFP+ LC LR 10km SM modülden toplam da 4 adet teslim edilecektir.
52. Tüm ağ anahtarlarının kurulumu ve konfigürasyonu yüklenici firma tarafından yapılacaktır.

Usuf Turhan TEKİN
Mühendis

Doç. Dr. Evren DEĞİRMENCI
Mersin Üniversitesi Hastanesi
Koordinator