autostrade//per l'italia

Specifiche tecniche RDA *383583*

Autostrade//per l'Italia

Specifiche tecniche

Acquisizione switch L2 Extreme

AD/ITS/ITC/SER

autostrade per l'italia

Specifiche tecniche RDA *383583*

[redacted]POS 10

SWTICH X460-G2-24P-10GE4, ciascun elemento costituito da:

Part #	Prodotto	Descrizione	Quantità Part # per singolo appparato
16703	X460-G2-24p-10GE4-Base	Summit X460-G2 24 10/100/1000BASE-T PoE+, 8 100/1000BASE-X unpopulated SFP (4 SFP ports shared), 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan module slot (unpopulated), ExtremeXOS Advanced Edge license with EXOS Release 22.1 or greater	1
10951	Summit 715W PoE AC PSU FB	715W AC PoE Power Supply Module for Summit X460-G2 and X450-G2 series switches with front to back airflow	2
10094	PWR CORD,10A,EUROPE,CEE7,C15	Power Cord, 10A, EUROPE, CEE7, IEC320-C15	2
10945	Summit Fan module FB	Fan Module for Summit X460-G2/X450-G2 Series Switches - front to back airflow	1
16423	Core Lic from Adv Edge - X460/-G	Core Lic from Adv Edge - X460/-G	1
97004-16703	EW NBD AHR 16703	EW NBD AHR 16703	1
98000-16423	98000-16423	98000-16423	1
10304	1m SFP+ Cable	10 Gigabit Ethernet SFP+ passive cable assembly, 1m length.	1

[redacted]POS 20

SWTICH X460-G2-48P-10GE4, ciascun elemento costituito da:

Part #	Prodotto	Descrizione	Quantità Part # per singolo appparato
16704	X460-G2-48p-10GE4-Base	Summit X460-G2 48 10/100/1000BASE-T PoE+, 4 1000/10GBaseX unpopulated SFP+ ports, Rear VIM Slot (unpopulated), Rear Timing Slot (unpopulated), 2 unpopulated PSU slots, fan	1

		module slot (unpopulated), ExtremeXOS Advanced Edge license with EXOS Release 22.1 or greater	
10951	Summit 715W PoE AC PSU FB	715W AC PoE Power Supply Module for Summit X460-G2 and X450-G2 series switches with front to back airflow	2
10094	PWR CORD,10A,EUROPE,CEE7,C15	Power Cord, 10A, EUROPE, CEE7, IEC320-C15	2
10945	Summit Fan module FB	Fan Module for Summit X460-G2/X450-G2 Series Switches - front to back airflow	1
10304	1m SFP+ Cable	10 Gigabit Ethernet SFP+ passive cable assembly, 1m length.	1
16423	Core Lic from Adv Edge - X460/-G	Core Lic from Adv Edge - X460/-G	1
97004-16704	EW NBD AHR 16704	EW NBD AHR 16704	1
98000-16423	98000-16423	98000-16423	1

Elementi comuni della POS 10 e della POS 20

Caratteristiche essenziali

- Ogni apparato deve essere dotato almeno di due alimentatori, estraibili a caldo, con tensione di ingresso 230VAC; tutte le funzionalità devono essere garantite senza degrado anche in presenza di un guasto a carico del 50% degli alimentatori (per fault di una linea di alimentazione o di un guasto HW); il guasto dell'alimentatore deve essere segnalato visivamente e remotamente. I cavi di alimentazione devono essere compresi nella fornitura. L'ingresso 230VAC degli alimentatori dovrà essere attrezzato con connettori standard che non richiedano operazioni di cablaggio per l'alimentazione (es. coppia IEC60320 C14 /C13).
- Il montaggio dovrà avvenire in rack 19'' (staffe fornite complete di viti e dadi di fissaggio, anche lato rack), con ingombro massimo in altezza di 2RU; le staffe dovranno permettere un montaggio dell'apparato arretrato rispetto al filo delle staffe del rack, così da lasciare spazio sufficiente a garantire l'alloggiamento delle FO, anche con armadio chiuso. La profondità massima ammessa, comprensiva dei connettori di alimentazione è di 49cm, così da permettere l'installazione in rack da 60cm.
- Il dispositivo dovrà garantire il supporto di configurazioni di tipo stack, anche basato su interfacce proprietarie con throughput di almeno 160Gbit/s. Le macchine dovranno risultare già equipaggiate con i relativi moduli e cavi per realizzare questa configurazione.
- Supporto di configurazioni di tipo stack distribuito da realizzare mediante porte ottiche standard a 10Gbit/s, con distanza massima 10Km (gruppi di macchine installate in siti/sale diversi devono poter essere viste, gestite e configurate come 1 sola); tale configurazione deve risultare possibile

per un numero di macchine non inferiore a 6. La macchina dovrà disporre a questo scopo di almeno 4 porte 10G SFP+ o XFP attive; per ottimizzare la densità di porte (nel caso non si utilizzi lo stack distribuito) le 4 porte devono poter essere utilizzate per traffico IP anche ad 1Gbit/s.

Dovranno essere fornite a corredo e inserite in ciascuna scatola 4 patch UTP ct.6a di lunghezza 2mt.

Per le porte in rame è richiesta:

- Porte dotate di funzionalità di auto-negoziazione della velocità;
- Porte dotate della funzionalità di selezione automatica della modalità duplex (half o full);
- Le porte devono essere dotate della modalità AutoMDI/MDIX per la selezione automatica delle coppie trasmissione-ricezione, così da poter funzionare sia con cavi dritti che incrociati;

Sono richieste le seguenti caratteristiche:

- Tutte le porte ottiche devono essere del tipo SFP/SFP+ o XFP, e supportare moduli con diagnostica digitale DDM; non devono esistere blocchi legati al vendor. Tutte le ottiche devono poter essere accettate. E' richiesto il supporto di velocità sia 100Mbit/s che 1000Mbit/s. Devono poter essere impiegati e pienamente supportati anche moduli monofibra.
- Banda minima aggregata dello switch di almeno 260 Gbps
- E' richiesta la completa integrazione in HP NNM e HP NA (rilascio driver di gestione), così da poter conoscere lo stato di tutte le interfacce, gestire le configurazioni, gli aggiornamenti FW, nonché mostrare la corretta topologia di connessione.
- Porta seriale per management locale, completa di cavo;
- Porta ETH out-of-band; la porta deve essere realizzata in maniera da risultare isolata a livello HW ed a livello di routing dalla parte di gestione del traffico, così da garantire la piena funzionalità della parte di management in condizioni di fault di traffico
- Led indicatori dello stato porte, stato stack, stato alimentazione;
- Temperatura di funzionamento 0°C - 50°C;
- GARANZIA A VITA del tipo NBD (invio presso la sede ASPI, con spese di trasporto a carico del vendor, del pezzo nuovo entro il giorno lavorativo successivo alla segnalazione del guasto) su tutti i componenti dello switch (questo deve essere garantito per almeno i 5 anni successivi alla messa in End Of Life del prodotto).
- Aggiornamenti software (sia patch che nuove release) gratuiti a vita. Il software deve poter essere aggiornato da remoto (via SFTP/FTP).
- Supporto di procedure di upgrade dello 'stack' distribuito che permettano il riavvio di una unità alla volta, preservando tutte le funzionalità di routing e switching delle altre unità
- Presenza di almeno 2 partizioni per alloggiare il FW dello switch (che devono poter essere anche diverse), con specifici comandi per passare da una all'altra.
- L'inserimento di una nuova unità, o la sostituzione di una guasta non deve provocare interruzioni di servizio sulle altre; le modalità di riallineamento FW e di configurazione devono risultare robuste rispetto a queste eventualità.
- Il tempo di down a pieno carico di una singola unità a fronte di reboot/spegnimento e successiva riaccensione deve essere inferiore a 150 secondi
- CLI management via telnet, via SSH, via console tramite password, con diversi privilegi di accesso per gli utenti
- SNMP v1/v2/v3

- Supporto Jumbo Frames
- QoS egress sia per port che per queue con funzionalità di shaping/limiting
- Supporto del protocollo 802.1d per lo spanning-tree
- Supporto del protocollo 802.1w rapid recovery spanning tree
- Supporto del protocollo 802.1s multiple spanning tree
- Supporto del protocollo 802.1q per il vlan-tagging
- Supporto del protocollo 802.1AB Link Layer Discovery Protocol (LLDP) e estensione LLDP-MED
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- Funzionalità di autenticazione locale, di autenticazione Radius e TACACS+ (lunghezza minima key 20 caratteri)
- Port loopback detection and shutdown
- Supporto delle modalità di configurazione di porte active/stand-by
- Supporto di Y.1731 per la misura dei ritardi e del jitter
- Universal port – VoIP autoconfiguration
- Supporto Multi-Switch Link Aggregation Group (MLAG) per creare link aggregate tra switch diversi dello stesso stack
- Possibilità di creare script in un linguaggio di programmazione per eseguire funzionalità in maniera continuativa o a trigger scatenante
- Gli Switch devono essere inoltre compatibili **ZTP/ZTP+** (Zero Touch Provisioning), per la configurazione via **DHCP** o **DNS**
- Mac security per controllare il numero e la tipologia di Mac Address per porta (possibilità di definire il numero ed i singoli Mac Address per ciascuna porta dello swtich configurata in modalità untagged)
- IEEE 802.1D MAC Bridges
- IEEE 802.1p Priority
- IEEE 802.1Q VLANs (supporto sia "Port based" che "MAC based")
- IEEE 802.1s Multiple Spanning Trees
- IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- IEEE 802.1ag traceroute
- IEEE 802.3 Type 10BASE-T
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- IEEE 802.3x Flow Control
- RFC 768 UDP
- RFC 783 TFTP Protocol (revision 2)
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 TELNET
- RFC 868 Time Protocol
- RFC 951 BOOTP
- RFC 1350 TFTP Protocol (revision 2)
- RFC 1542 BOOTP Extensions
- RFC 2030 Simple Network Time Protocol (SNTP) v4
- RFC 2131 DHCP v4 e v6
- ITU-T G.8032v2

- Monitoraggio
- CPU Monitoring e funzionalità di monitoraggio delle risorse dello switch via CLI/SNMP
- Tool di L2 Ping / Traceroute 802.1ag
- Supporto SSHv2 Server e Client
- Supporto SCP/SFTP Server
- Supporto SCP/SFTP Client
- Possibilità di creare Script in un linguaggio (Ruby, Python, Bash ecc. interpretato dal sistema operativo della macchina)
- Supporto a DHCPv4 (DHCPv4 server, client, relay e smart relay)
- Supporto a DHCPv6 (DHCPv6 relay, prefix delegation snooping e client)
- Capacità di UDP BOOTP relay forwarding
- IP Flow Information
- IPv4 Duplicate Address Detection (DAD)
- IPv6 Duplicate Address Detection
- Network Login via Web Based (HTTP/SSL), SSH/Telenet, 802.1x, Integration con Microsoft NAP, Multiple supplicants (multiple VLANs)
- Possibilità di creare ACLs Layer-2
- Possibilità di creare ACLs Layer-3 e superiori (sia IPv4 che IPv6)
- Supporto alle Private VLAN
- Sistema di protezione DoS (Denial of Service) delle risorse (CPU, memoria)
- IP security—DHCP Option 82—L2 mode
- IP security—DHCP Option 82—L2 mode VLAN ID
- IP security—DHCP IP lockdown
- IP security—Trusted DHCP server ports
- Possibilità di creare script CLI per monitoraggio / sicurezza (esempio script in Ruby, Python o simili)

Ridondanza

- Supporto dei protocolli Virtual Router Redundancy Protocol (VRRP) RFC 2338, HSRP (Hot Standby Routing Protocol) o simili;
- Supporto di configurazioni di tipo stack distribuito realizzate mediante porte ottiche standard a 10G, con distanza massima 10Km (gruppi di macchine installate in siti diversi devono poter essere viste, gestite e configurate come 1 sola); tale configurazione deve risultare possibile per un numero di macchine non inferiore a 6. Tutte le macchine devono risultare analoghe; non è ammesso che alcune funzionino solo se connesse alle altre;
- Supporto della funzionalità di routing statico IPv4 e IPv6
- Supporto della funzionalità di routing dinamico basato su RIP e OSPF.

Quality of Service

- Compliance allo standard 802.1p della definizione di CoS (Class of Service);
- presenza di almeno quattro code di priorità, di cui almeno una coda ad alta priorità per la gestione del traffico real-time, per ogni singola porta;
- Standard 802.1p CoS e DSCP field classification, utilizzando marking e reclassification su base pacchetto per indirizzo IP sorgente e destinazione, MAC address sorgente e destinazione, o numero di porta Layer 4 TCP o UDP.

- Classificazione al livello del campo DSCP (Differentiated Services Code Point) tramite marcatura e riclassificazione
- Limitazione del flusso di traffico definibile in base a:

  - Indirizzi IP Sorgenti o Destinazione
  - MAC Address Sorgenti o Destinazione
  - Informazioni Layer4 (TCP e UDP)
  - Una combinazione dei campi sopra citati

Protezione

- Pieno Supporto allo standard 802.1x in termini di:

  - Autenticazione Utenti
  - Assegnazione Dinamica delle VLAN
  - 802.1x con VLAN Voice (permette ad un telefono IP di accedere alla Vlan vocale "bypassando" l'autorizzazione sulla porta)
  - VLAN Guest entro cui confinare gli utenti senza "client 802.1x"
  - Meccanismi di filtraggio dei MAC address a livello porta (portsecurity).
  - funzionalità di filtraggio (ACLs) sulla base degli Header di livello 3 e 4;
  - Possibilità di configurare Regole di accesso (ACL) sulle singole interfacce
  - Supporto dei protocolli SSHv2 server e client, SNMP, Kerberos
  - Supporto e compatibilità con Server di Autenticazione, Autorizzazione e Accounting (AAA) del tipo RADIUS (Remote Authentication Dial-In User Service) e/o TACACS+ (Terminal Access Controller Access Control System Plus)
  - Possibilità di porta di mirroring per il traffico di rete con supporto
    - Remote mirroring
    - Multi session mirroring;
  - Controllo del traffico BPDU (Bridge Protocol Data Unit);
  - Supporto di filtri IGMP.

- RFC 1492 TACACS+

Gestione

- Supporto al Simple Network Management Protocol (SNMP) versioni 1, 2c e 3. Compliance con gli standard descritti da IETF RFC 1157, 1213, 1901 – 1908, 3411-3418.
- Supporto delle MIB LLDP per la scoperta e connessione dei nodi
- Supporto di RMON
- Inventario, salvataggio e ripristino delle configurazioni tramite trasmissione dati standard (TFTP, FTP, SNMP, etc.).
- Supporto a Server Syslog esterni e compliance agli standard descritti dagli IETF RFC 3164 e RFC 3195
- Funzionalità di Trace route layer2
- Salvataggio, Inventario e ripristino delle configurazioni:
- Salvataggio - Le operazioni di salvataggio delle configurazioni, Snapshot di configurazione e immagine del Sistema operativo devono poter essere effettuate periodicamente e in modo automatico.
- Inventario - Possibilità di eseguire il download dell'immagine del sistema operativo e delle configurazioni salvate e in esecuzione sul dispositivo tramite protocolli di trasferimento standard quali: FTP, SFTP, TFTP, SSH, Telnet. Tale trasferimento deve poter essere automatico.
- Ripristino – Si rende assolutamente necessaria la capacità di ripristinare remotamente la configurazione e il sistema operativo.
- Protocolli di analisi flusso di traffico sFlow in hardware e senza impatto sulle performance dello switch
- Supporto OpenFlow

Hardening

Sull'apparato di rete dovrà essere possibile:

- Cifrare le password che compaiono in configurazione
- Creare un Banner visualizzabile all'inizio di una sessione di accesso remoto
- Definire almeno un set di credenziali locali. Devono poter essere inserite password di almeno 16 caratteri
- Definire ruoli utente con privilegi diversi. Soltanto Utenti appartenenti a ruoli amministrativi devono poter modificare le configurazioni (sessioni exec).
- Autenticare gli Utenti tramite DB locale (Local Authentication) e tramite RADIUS/TACACS+ Server remoto
- Impostare un timeout per le sessioni exec locali e remote
- Disabilitare l'exec sulla porta aux
- Configurare l'accesso exec remoto in SSH
- Configurare l'accesso exec remoto in telnet per quei sistemi che non supportano il protocollo SSH
- Limitare con una ACL l'accesso exec remoto
- Settare il Network Time Protocol Client così da sincronizzare automaticamente il Clock di Sistema. Tale servizio dovrà essere compliant con il Network Time Protocol (NTP) definito da IETF RFC 1305.
- Inibire l'accesso SNMP RW (Read and Write)
- Disponibilità di meccanismi di protezione da DDoS
- Restringere l'accesso SNMP RO (read only) con Access Control List.

- Disabilitare i seguenti servizi:
  - Finger service
  - tcp-small-servers
  - udp-small-servers
  - bootp
  - service pad
  - network boot
  - DNS resolution
  - Tftp server
  - TCP Keepalive
  - ICMP redirects

Compreso nella fornitura, e senza oneri aggiuntivi per ASPI, è da prevedere anche una piattaforma di gestione

Network Management System e Network Analytics

Premessa

Ai fini di permettere una gestione efficiente, uniforme ed innovativa di tutto l'installato è necessario fornire, incluso assieme agli apparati di rete, un **Sistema di Network Management (NMS o Network Management System)**, oltre che per la **localizzazione** di un dispositivo di rete durante le operazioni di manutenzione e di intervento da parte di un operatore su uno o più dispositivi collegati. Vedasi dettaglio requisiti **B1**.

Inoltre la natura variegata del traffico di rete, l'utilizzo intensivo di applicazioni sempre più complesse ed eterogenee, alcune delle quali identificate come *Business Critical*, genera flussi di dati consistenti e variegati. Dal punto di vista della gestione della rete, la capacità di identificare il traffico al più fino al livello 4 della pila ISO/OSI non è sufficiente, in quanto la mancanza di visibilità applicativa causa una totale perdita di controllo di quello che effettivamente transita sulla rete. Si ha quindi la necessità di una pervasiva visibilità e controllo applicativi a livello di rete, gli switch devono essere predisposti al supporto di visibilità applicativa fino al livello 7 della pila ISO/OSI (brevemente **Visibility and Analytics**). Vedasi dettaglio requisiti **B2**.

Il sistema inoltre deve essere installabile su **macchine virtuali VmWare** da installare all'interno dell'infrastruttura virtuale già in essere di ASPI e non deve essere costituito da sonde aggiuntive da installare lungo la rete. Devono essere gli stessi switch le sonde per realizzare i servizi richiesti. Il sistema deve fornire in un'unica entità software, cioè una **Dashboard Web** http/https compatibile in modo nativo con tutti i moderni browser (Internet Explorer, Mozilla Firefox, Safari e Chrome) cioè senza l'utilizzo di Java Applet o Activex esterni. Questo requisito è necessario per una maggiore compatibilità con i comuni Browser e Client Microsoft Windows in uso in ASPI, oltre che per aspetti di Sicurezza Informatica.

Di seguito un maggiore dettaglio dei requisiti che il sistema deve possedere, il sistema deve essere incluso nella quotazione dei singoli switch e non deve comportare costi aggiuntivi.

Network Management System (NMS)

- Lo strumento deve permettere di effettuare operazioni di manutenzione, aggiornamento firmware e configurazione e troubleshooting di rete da remoto mediante la Dashboard Web di tutti gli apparati forniti, senza la necessità di intervenire on-site sugli apparati di rete, salvo *fault* fisico dello stesso dispositivo di rete.

- Il sistema non deve prevedere "sonde fisiche" o apparati aggiuntivi da installare, le sonde devono essere incluse all'interno degli switch di rete. Questo per evitare ulteriori installazioni di apparati.

- Il sistema deve permettere **la localizzazione** di un singolo endpoint (sensore, camera IP, telefono, server, cliente, ecc.), a partire da un indirizzo MAC (48 bit) e/o un indirizzo IP e/o un nome logico basato su LDAP / Active Directory, indicando l'esatta posizione in termini della coppia "**Device di Rete:Porta**" sul quale l'endpoint risulta collegato. Il Device deve essere individuato mediante nome logico ed indirizzo IP di management. Il sistema deve permettere anche di creare Policy per il singolo endpoint con la capacità minima di escluderlo o abilitarlo, anche per un tempo limitato, all'accesso alla rete (sistemi di autenticazione ed accesso quali ad esempio 802.1x, Kerberos, Captive Portal, Web Authentication, Mac Authentication).

- Il sistema di gestione deve fornire le funzionalità necessarie per la gestione delle configurazioni e delle release software di sistema. Deve essere possibile gestire in maniera semplice tutte le operazioni routine come i backup delle configurazioni, upgrade delle release software.

B2-Requisiti per la funzionalità di analisi del traffico (Network Visibility and Analytics)

- Possibilità di verificare quali applicazioni sono utilizzate sulla rete, quanto traffico generano,

nonché la sorgente del traffico.

- Il gestore di rete deve essere in grado di identificare al meglio il **reale trend** di utilizzo della rete, anche per una ottimale pianificazione degli investimenti di medio e lungo termine delle risorse dell'infrastruttura.

- Inoltre lo strumento di **Visibility and Analytics** deve contribuire inoltre alla sicurezza della rete stessa, permettendo di rilevare applicazioni dannose o non desiderate , ovvero *Shadow IT* sulla rete (ossia il proliferare di apparati o servizi di rete estranei all'organizzazione e non autorizzati), permettendo una rapida individuazione e successivo contenimento dell'origine della minaccia.

- Al fine di raggiungere l'obiettivo descritto gli Switch e più in generale lo Stack, attraverso l'interazione con sistema di management e senza l'utilizzo di sonde aggiuntive cioè apparati esterni, devono supportare nativamente la capacità di analizzare i flussi di traffico con visibilità fino al livello 7 della pila ISO/OSI, in particolare:

- Visibilità applicativa a Livello 7 della pila ISO/OSI (non limitandosi solo al socket TCP o indirizzo IP/Porta)

- Possibilità di personalizzazione delle applicazioni riconosciute, attraverso la creazione di nuove signature

- Analisi per flusso anziché per pacchetto. Identificazione dei flussi attraverso gli Switch/Stack di rete, fino a 2.000 flussi bidirezionali per Switch/Stack

Modalità accettazione fornitura

Gli oggetti forniti devono rispondere alle specifiche tecniche elencate nei paragrafi precedenti. Inoltre, al fine dell'accettazione della fornitura, deve essere fornito un campione di apparati finalizzato alla realizzazione di test funzionali e integrazione con i sistemi ASPI.

Da prevedere supporto di pre-configurazione e supporto remoto all'attivazione.