acquistinretepa

# Reti Locali 8

## Lotto 1

# ALLEGATO 2 ALLA GUIDA ALLA CONVENZIONE – APPARATI ATTIVI

Ultimo aggiornamento: 15/11/2023

## SOMMARIO

# 1. Descrizione degli apparati attivi

Questo documento contiene la descrizione di dettaglio di tutti gli apparati attivi presenti nella convenzione: switch, prodotti SD-WAN e apparati wireless. Sono descritti, inoltre, in dettaglio anche gli UPS.

# 2. Switch

## 2.1. Switch Tipo 1

### 2.1.1. Cisco - C9200L-24T-4XC

Gli switch Cisco Catalyst 9200L sono switch Gigabit Ethernet stackable a configurazione fissa che estendono la potenza della rete intent-based e dell'innovazione hardware e software della moderna famiglia Catalyst 9000. Con 24 porte rame 10/100/1000 e 4 uplink 1/10G, operano con il nuovo software Cisco IOS-XE e supportano la gestione semplice e sicura della rete. Questi switch completamente gestibili supportano funzionalità avanzate di Layer 2 e base Layer 3. Progettati per semplificare l'operatività al fine di ridurre il costo totale di gestione, consentono trasporto scalabile, sicuro ed efficiente dal punto di vista energetico, con l'aggiunta di servizi e funzionalità intelligenti, quali Routed Access (RIP, EIGRP Stub, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO, AutoQoS, Perpetual PoE e Fast PoE (sui modelli PoE), Netflow.

Inoltre, gli stessi switch possono far parte dell'innovativa architettura di rete Cisco Software-Defined Access (SD-Access), che, attraverso automazione e funzionalità avanzate, consente una gestione centralizzata, potente e semplificata della sicurezza e dell'affidabilità di rete, con l'obiettivo di garantire conformità, efficienza operativa, visibilità ed esperienza utente semplificata.

L'offerta in Convenzione prevede un modello con 24 porte rame RJ45 10/100/1000 e 4 porte di uplink 1/10G.
Per maggiori informazioni, riferirsi al data sheet ufficiale online:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

### 2.1.2. Aruba - JL259AC

Gli switch HPE Aruba Networking 2930F appartengono alla tipologia 1 in convenzione Reti Locali 8 sono switch wire-speed, con funzionalità Layer 3, adatti ad offrire alle Amministrazioni una rete agile ed intelligente. Lo switch (da rack standard 19") dispone di 24 porte autosensing 10/100/1000-Mbps Base-T, di 4 porte 1GbE SFP. In aggiunta dispone di una porta seriale e di una porta USB micro-B per la gestione locale e l'accesso in console.

La banda della matrice di switching è pari a 56 Gbps e il throughput aggregato è tale da garantire prestazioni wire-speed su tutte le porte.

*Aruba 2930F 24GbE 4SFP*

Le funzionalità Layer 3 supportate da questa famiglia di switch sono: routing statico con un massimo di 256 rotte; routing dinamico con RIPv1, RIPv2 e RIPng per un massimo di 10000 rotte; OSPF su singola area su un massimo di 8 interfacce IP e Policy-based routing.

La tecnologia di clustering Virtual Switching Framework (VSF) consente all'amministratore di rete di configurare un Virtual Chassis che include fino ad un massimo di 8 apparati della serie Aruba 2930F. semplificando e consolidando la gestione e l'indirizzamento IP dell'infrastruttura. La tecnologia VSF permette di configurare interfacce aggregate LACP tra apparati diversi inclusi nello stesso Virtual Chassis

riducendo pertanto la necessità di implementare protocolli di ridondanza come Spanning-Tree e VRRP ed incrementando pertanto l'affidabilità e la resilienza della soluzione.

- Caratteristiche Generali:
    - Auto-MDIX per l'adeguamento automatico dei cavi dritti o crossover su tutte le porte 10/100-Mbps e 10/100/1000-Mbps;
    - Uplink Gigabit con porte per connettività 1GbE su moduli di tipo SFP;
    - Fino a 32.768 MAC address per fornire l'accesso ad un numero elevato di dispositivi Layer 2;
- Funzionalità Layer 2:
    - Supporto e tagging VLAN: supporta IEEE 802.1Q, con 4094 ID VLAN simultanei; supporta VLAN basate su porta, su MAC e su protocollo;
    - Protocollo Spanning Tree (STP) Multiple STP o Rapid STP per la prevenzione di loop di rete nelle topologie Layer 2 nella gestione dei link ridondati;
    - Link Aggregation Control Protocol (LACP) e Port trunking consente di incrementare il livello di throughput da switch a switch e ridondanza a livello di collegamento, con supporto per aggregazione di collegamenti basati su standard (IEEE 802.3ad); supporta fino a 128 trunk, con max 8 collegamenti (porte) per ciascun trunk;
    - Supporto e tagging VLAN: supporta IEEE 802.1Q, con 4094 ID VLAN simultanei; supporta VLAN basate su porta, su MAC e su protocollo;
    - Supporto della tecnologia di overlay VxLAN;
- Servizi Layer 3:
    - Il protocollo ARP consente di determinare il MAC address di un altro host IP nella stessa sottorete;
    - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
    - Routing statico e dinamico con supporto dei protocolli RIPv2, RIPng e OSPF su singola area;
    - Indirizzamento IPv6 con possibilità di configurare routing statico o dinamico attraverso il protocollo RIPng.

- ACL (access control list) in wire-speed basate su hardware per l'implementazione di ACL ricche di funzionalità a garanzia di elevati livelli di sicurezza e facilità di amministrazione senza impatto sulle prestazioni di rete

- Servizi di Sicurezza
  - Configurazione e gestione in modalità remota: disponibile tramite browser Web sicuro o interfaccia a linea di comando (CLI);
  - Privilegi di livello responsabile e operatore: consentono l'accesso in sola lettura (operatore) o lettura e scrittura (manager) alle interfacce CLI e di gestione di browser Web;
  - GUI Web protetta: offre interfaccia grafica sicura di facile utilizzo per la configurazione del modulo mediante HTTPS;
  - Autorizzazione di comandi: utilizza RADIUS per il collegamento di un elenco personalizzato di comandi CLI al login di un singolo amministratore di rete.
- Gestione e configurazione
  - Semplifica il nome delle porte mediante assegnazione di nomi descrittivi alle interfacce fisiche;
  - IL Local User Role definisce un set di politiche di accesso allo switch come sicurezza, di autenticazione e QoS. Uno User Role può essere applicato a gruppi di utenti o switch. L'applicazione del roulo può avvenire mediante la configurazione dell'apparato o utilizzando il Policy Manager ClearPass;
  - Per-port tunneled node consente la configurazione di un tunnel sicuro per il trasporto del traffico di rete di una porta dello switch verso un Controller Aruba. Le politiche di accesso verranno applicate dal controller;
  - Dynamic Host Configuration Protocol (DHCP): semplifica la gestione di reti IP di grandi dimensioni e supporta client e server;
  - Gli switch della serie Aruba 2930F supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema.
- Servizi Quality of Services (QoS)
  - QoS per la gestione della congestione e prioritizzazione del traffico attraverso impostazione del tag CoS IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS),

protocollo L3, port number TCP/UDP, porta sorgente e DiffServ, accodamento Strict Priority (SP), Egress Queue Rate-limiting, Guaranteed Bandwidth Minimums, Port e Priority-based Rate Limiting, Selectable Queuing Configurations;

- Controllo di flusso mediante lo standard IEEE 802.3x, per la di ridurre la congestione in situazioni di traffico intenso;
- Meccanismo di controllo del traffico broadcast per limitare la quantità di pacchetti di tipo broadcast, unknown unicast e multicast che possono portare a congestioni all'interno della rete.

- Specifiche Tecniche
  - 24 porte 10/100/1000 Mbps BaseT autosensing;
  - 4 porte SFP 100/1000 Mbps;
  - Capacità di switching 56 Gbps;
  - Supporta fino a 32768 indirizzi MAC;
  - Supporta fino a 2000 prefissi IPv4 unicast e 1000 rotte IPv6 prefissi in hardware;
  - Supporta fino 200 prefissi OSPF, 256 prefissi statici e 10000 prefissi RIP;
  - Latenza inferiore 3,8 microsecondi (pacchetti di 64 Byte);
  - Assorbimento massimo 293W;
  - Dissipazione 100BTU/ora;
  - Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
  - Umidità operativa da 15% a 95% a 40°C, di stoccaggio da 15% a 95% a 65°C;
  - Occupazione spazio rack: 1 Rack Unit (RU);
  - Dimensioni: 44,25cm (L) x 20,02 (P) x 4,39 (A);
  - Peso 2,41 Kg.

### 2.1.3. Extreme Networks - 5320-24t-8XE_C

Lo switch Extreme Networks 5320-24T-8XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 208 Gbps di capacità di switching;

- 24 porte 10/100/1000BASE-T full/half duplex ports;
- 8 porte di uplink 1/10Gb Uplink SFP+ 10Gb;
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 40Gb;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- MACsec (opzionale – licenza aggiuntiva) sulle porte di accesso e uplink per garantire una crittografia sicura del collegamento.

*Extreme Networks 5320-24T-8XE*

Scheda Tecnica Extreme Networks 5320

### 2.1.4. Juniper - EX2300-24T-VC-C

Gli switch ethernet della serie EX2300 sono apparati compatti ed efficienti, ideali per il livello di accesso in ambito branch, retail e campus. Sono switch "cloud-ready" e abilitati per l'installazione zero-touch (ZTP) senza configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 4 switch EX2300 tra loro, come se fossero in singolo apparato.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo *Enhanced Limited Lifetime*; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia *Limited Lifetime* prevede la possibilità per l'end user di accedere a tutti gli upgrade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

https://support.juniper.net/support/pdf/warranty/990240.pdf

**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 24 x 1GbE + 4 x 1/10GbE SFP/SFP+ |
| Switch capacity | 128 Gbps |
| Fabric | Virtual Chassis |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 4 EX2300 e di gestirli come un solo dispositivo e riduce i costi operativi, semplificando la gestione.

La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

**QoS con 8 code di priorità**

Lo switch ha 8 code per porta che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

#### 2.1.5. Huawei - S5735-L24T4XQA-V2-C

Il modello Ethernet CloudEngine S5735-L24T4XQA-V2 fa parte della series CloudEngine S5735-L-Q-V2. È uno switch Layer 3 con supporto di routing statico, RIP e OSPF. Installabile a rack 19", equipaggia 24 porte 10/100/1000 Ethernet su rame e 4 porte 10G ottico su SFP. In dotazione è fornito un cavo di stack da 1 metro da usare su una delle 4 porte ottiche e con cui è possibile metterlo in stack con i modelli della stessa series S5735-L- Q -V2. L'intera serie di switch CloudEngine S5735-L-Q-V2 sono silenziosi e a risparmio energetico grazie al loro design senza ventola, che li rende ideali per vari settori, come la sanità,retails, l'estrazione mineraria e Internet.

L'apparato ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e throughput fino a 128 Gbps.

E' gestibile (configurazione, monitoraggio e allaramistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller nella soluzione Cloud Campus.

*CloudEngine S5735-L24T4XQA-V2*

## 2.2. Switch Tipo 2

#### 2.2.1. Cisco - C9200L-24P-4XC

Gli switch Cisco Catalyst 9200L sono switch Gigabit Ethernet stackable a configurazione fissa che estendono la potenza della rete intent-based e dell'innovazione hardware e software della moderna famiglia Catalyst 9000. Con 24 porte rame 10/100/1000 e 4 uplink 1/10G, operano con il nuovo software Cisco IOS-XE e supportano la gestione semplice e sicura della rete. Questi switch completamente gestibili supportano funzionalità avanzate di Layer 2 e base Layer 3. Progettati per semplificare l'operatività al

fine di ridurre il costo totale di gestione, consentono trasporto scalabile, sicuro ed efficiente dal punto di vista energetico, con l'aggiunta di servizi e funzionalità intelligenti, quali Routed Access (RIP, EIGRP Stub, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO, AutoQoS, Perpetual PoE e Fast PoE (sui modelli PoE), Netflow.

Inoltre, gli stessi switch possono far parte dell'innovativa architettura di rete Cisco Software-Defined Access (SD-Access), che, attraverso automazione e funzionalità avanzate, consente una gestione centralizzata, potente e semplificata della sicurezza e dell'affidabilità di rete, con l'obiettivo di garantire conformità, efficienza operativa, visibilità ed esperienza utente semplificata.

L'offerta in Convenzione prevede un modello con 24 porte rame RJ45 10/100/1000, con funzionalità IEEE 802.3at (PoE fino a 30W) supportata sulle porte di accesso e 4 porte di uplink 1/10G. Per maggiori informazioni, riferirsi al data sheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

### 2.2.2. Aruba - JL261AC

Gli switch HPE Aruba Networking 2930F appartenenti alla tipologia 2 in convenzione Reti Locali 8 sono switch wire-speed, Layer 3, adatti ad offrire alle Amministrazioni una rete agile ed intelligente. Lo switch (da rack standard 19") dispone di 24 porte autosensing 10/100/1000 Base-T PoE+, di 4 porte 1GbE SFP. In aggiunta dispone di una porta seriale e di una porta USB micro-B per la gestione locale.

La banda della matrice di switching è pari a 56 Gbps e il throughput aggregato è tale da garantire prestazioni wire-speed su tutte le porte.

*Aruba 2930F 24GbE PoE+ 4SFP*

Le funzionalità Layer 3 supportate da questa famiglia di switch sono: routing statico con un massimo di 256 rotte; routing dinamico con RIPv1, RIPv2 e RIPng per un massimo di 10000 rotte; OSPF su singola area su un massimo di 8 interfacce IP e Policy-based routing.

La tecnologia di clustering Virtual Switching Framework (VSF) consente all'amministratore di rete di configurare un Virtual Chassis che include fino ad un massimo di 8 apparati della serie Aruba 2930F. semplificando e consolidando la gestione e l'indirizzamento IP dell'infrastruttura. La tecnologia VSF permette di configurare interfacce aggregate LACP tra apparati diversi inclusi nello stesso Virtual Chassis riducendo pertanto la necessità di implementare protocolli di ridondanza come Spanning-Tree e VRRP ed incrementando pertanto l'affidabilità e la resilienza della soluzione.

- Caratteristiche Generali:
    - Auto-MDIX per l'adeguamento automatico dei cavi dritti o crossover su tutte le porte 10/100-Mbps e 10/100/1000-Mbps;
    - Uplink Gigabit con porte per connettività 1GbE su moduli di tipo SFP;
    - Fino a 32.768 MAC address per fornire l'accesso ad un numero elevato di dispositivi Layer 2;
    - Supporto Power over Ethernet (PoE+) standard IEEE 802.3at in grado di erogare fino a 30W per porta Base-T per l'alimentazione di dispositivi locali quali: telefoni IP, access-point e videocamere di sicurezza.
- Funzionalità Layer 2:
    - Supporto e tagging VLAN: supporta IEEE 802.1Q, con 4094 ID VLAN simultanei; supporta VLAN basate su porta, su MAC e su protocollo;
    - Protocollo Spanning Tree (STP) Multiple STP o Rapid STP per la prevenzione di loop di rete nelle topologie Layer 2 nella gestione dei link ridondati;
    - Link Aggregation Control Protocol (LACP) e Port trunking consente di incrementare il livello di throughput da switch a switch e ridondanza a livello di collegamento, con

supporto per aggregazione di collegamenti basati su standard (IEEE 802.3ad); supporta fino a 128 trunk, con max 8 collegamenti (porte) per ciascun trunk;

- Supporto e tagging VLAN: supporta IEEE 802.1Q, con 4094 ID VLAN simultanei; supporta VLAN basate su porta, su MAC e su protocollo;
- Supporto della tecnologia di overlay VxLAN;

- Servizi Layer 3:
  - Il protocollo ARP consente di determinare il MAC address di un altro host IP nella stessa sottorete;
  - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
  - Routing statico e dinamico con supporto dei protocolli RIPv2, RIPng e OSPF su singola area;
  - Indirizzamento IPv6 con possibilità di configurare routing statico o dinamico attraverso il protocollo RIPng;
  - ACL (access control list) in wire-speed basate su hardware per l'implementazione di ACL ricche di funzionalità a garanzia di elevati livelli di sicurezza e facilità di amministrazione senza impatto sulle prestazioni di rete;
- Servizi di Sicurezza:
  - Configurazione e gestione in modalità remota: disponibile tramite browser Web sicuro o interfaccia a linea di comando (CLI);
  - Privilegi di livello responsabile e operatore: consentono l'accesso in sola lettura (operatore) o lettura e scrittura (manager) alle interfacce CLI e di gestione di browser Web;
  - GUI Web protetta: offre interfaccia grafica sicura di facile utilizzo per la configurazione del modulo mediante HTTPS;
  - Autorizzazione di comandi: utilizza RADIUS per il collegamento di un elenco personalizzato di comandi CLI al login di un singolo amministratore di rete.
- Gestione e configurazione
  - Semplifica il nome delle porte mediante assegnazione di nomi descrittivi alle interfacce fisiche;
  - IL Local User Role definisce un set di politiche di accesso allo switch come sicurezza, di autenticazione e QoS. Uno User Role può essere applicato a gruppi di utenti o switch.

L'applicazione del roulo può avvenire mediante la configurazione dell'apparato o utilizzando il Policy Manager ClearPass;

- Per-port tunneled node consente la configurazione di un tunnel sicuro per il trasporto del traffico di rete di una porta dello switch verso un Controller Aruba. Le politiche di accesso verranno applicate dal controller;
- Dynamic Host Configuration Protocol (DHCP): semplifica la gestione di reti IP di grandi dimensioni e supporta client e server;
- Gli switch della serie Aruba 2930F supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema.

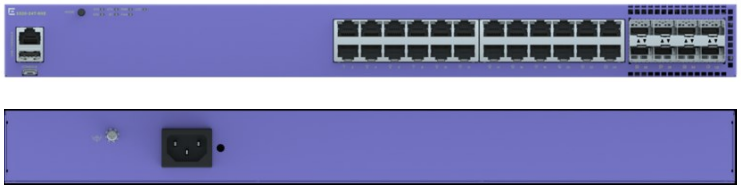
- Servizi Quality of Services (QoS)
  - QoS per la gestione della congestione e prioritizzazione del traffico attraverso impostazione del tag CoS IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo L3, port number TCP/UDP, porta sorgente e DiffServ, accodamento Strict Priority (SP), Egress Queue Rate-limiting, Guaranteed Bandwidth Minimums, Port e Priority-based Rate Limiting, Selectable Queuing Configurations;
  - Controllo di flusso mediante lo standard IEEE 802.3x, per la di ridurre la congestione in situazioni di traffico intenso;
  - Meccanismo di controllo del traffico broadcast per limitare la quantità di pacchetti di tipo broadcast, unknown unicast e multicast che possono portare a congestioni all'interno della rete;
- Specifiche Tecniche:
  - 24 porte 10/100/1000 Mbps BaseT autosensing PoE+ IEEE 802.1at;
  - 4 porte SFP 100/1000 Mbps;
  - Capacità di switching 56 Gbps;
  - Supporta fino a 32768 indirizzi MAC;
  - Supporta fino a 2000 prefissi IPv4 unicast e 1000 prefissi IPv6 unicast in hardware;
  - Supporta fino 200 prefissi OSPF, 256 prefissi statici e 10000 prefissi RIP;
  - Latenza inferiore 3,8 microsecondi (pacchetti di 64 Byte);
  - Assorbimento massimo 445W;
  - Dissipazione 258BTU/ora;

- Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
- Umidità operativa da 15% a 95% a 40°C, di stoccaggio da 15% a 95% a 65°C;
- Occupazione spazio rack: 1 Rack Unit (RU);
- Dimensioni: 44,25cm (L) x 30,42 (P) x 4,39 (A);
- Peso 3,10 Kg.

### 2.2.3. Extreme Networks - 5320-24p-8XE_C

Lo switch Extreme Networks 5320-24P-8XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 208 Gbps di capacità di switching;
- 24 porte 10/100/1000BASE-T full/half duplex ports;
- 8 porte di uplink 1/10Gb Uplink SFP+ 10Gb;
- Supporto PoE da 30W (IEEE 802.3at): lo switch supporta la tecnologia Power over Ethernet (PoE) con una potenza massima di 30 watt, conforme allo standard IEEE 802.3at su tutte le porte. Supporto del PoE fast (le periferiche PoE connesse vengono immediatamente alimentate appena lo switch è acceso) e perpetuo (le periferiche PoE connesse non si spengono in caso di riavvio dello switch);
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 40Gb;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- MACsec (opzionale – licenza aggiuntiva) sulle porte di accesso e uplink per garantire una crittografia sicura del collegamento.



*Extreme Networks 5320-24P-8XE*

Scheda Tecnica Extreme Networks 5320

### 2.2.4. Juniper - EX2300-24P-VC-C

Gli switch ethernet della serie EX2300 sono apparati compatti ed efficienti, ideali per il livello di accesso in ambito branch, retail e campus. Sono switch "cloud-ready" e abilitati per l'installazione zero-touch (ZTP) senza configurazione manuale, tramite il servizio di Wired Assurance. Gli switch supportano la tecnologia Virtual Chassis ed è possibile connettere e gestire fino a 4 switch EX2300 tra loro, come se fossero in singolo apparato logico.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo *Enhanced Limited Lifetime*; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia *Limited Lifetime* prevede la possibilità per l'end user di accedere a tutti gli upgrade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

https://support.juniper.net/support/pdf/warranty/990240.pdf

**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 24x1GbE + 4 x 1/10GbE SFP/SFP+ |
| Power | **PoE su tutte le porte e PoE+ fino a 30W su 12 porte** |
| Switch capacity | **128 Gbps** |
| Fabric | **Virtual Chassis** |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 4 EX2300 e di gestirli come un solo dispositivo e riduce i costi operativi, semplificando la gestione.

La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

**QoS con 8 code di priorità**

Lo switch ha 8 code per porta che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

### 2.2.5. Huawei - S5735-L24P4S-A-V2-C

Il modello Ethernet Switch CloudEngine S5735-L24P4S-A-V2 fa parte della series CloudEngine S5735-L-V2. È uno switch Layer 3 con supporto di routing statico, RIP e OSPF. Installabile a rack 19”, equipaggia 24 porte 10/100/1000 Ethernet PoE+ su rame e 4 porte 1G ottico su SFP. In aggiunta dispone di una porta

seriale per la gestione locale. In dotazione è fornito un cavo di stack da 1 metro da usare su una delle 4 porte ottiche e con cui è possibile metterlo in stack con i modelli della stessa series CloudEngine S5735-L-V2 .L'apparato ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e throughput fino a 56 Gbps e puo` gestire tutte le 24 porte in modalita` PoE+. Gli switch S5735-L-V2 si distinguono per caratteristiche interessanti come stack intelligente (iStack), rete Ethernet flessibile e controllo di sicurezza diversificato.

E' gestibile (configurazione, monitoraggio e allaramistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller nella soluzione Cloud Campus.

*CloudEngine S5735-L24P4S-A-V2*

## 2.3. Switch Tipo 3

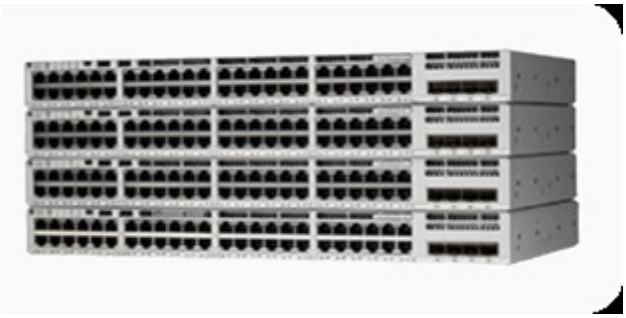
### 2.3.1. Cisco - C9200L-48T-4XC

Gli switch Cisco Catalyst 9200L sono switch Gigabit Ethernet stackable a configurazione fissa che estendono la potenza della rete intent-based e dell'innovazione hardware e software della moderna famiglia Catalyst 9000. Con 48 porte rame 10/100/1000 e 4 uplink 1/10G-X, operano con il nuovo software Cisco IOS-XE e supportano la gestione semplice e sicura della rete. Questi switch completamente gestibili supportano funzionalità avanzate di Layer 2 e base Layer 3. Progettati per semplificare l'operatività al fine di ridurre il costo totale di gestione, consentono trasporto scalabile, sicuro ed efficiente dal punto di vista energetico, con l'aggiunta di servizi e funzionalità intelligenti, quali Routed Access (RIP, EIGRP Stub, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO, AutoQoS, Perpetual PoE e Fast PoE (sui modelli PoE), Netflow.

Inoltre, gli stessi switch possono far parte dell'innovativa architettura di rete Cisco Software-Defined Access (SD-Access), che, attraverso automazione e funzionalità avanzate, consente una gestione

centralizzata, potente e semplificata della sicurezza e dell'affidabilità di rete, con l'obiettivo di garantire conformità, efficienza operativa, visibilità ed esperienza utente semplificata.

L'offerta in Convenzione prevede un modello con 48 porte rame RJ45 10/100/1000 e 4 porte di uplink 1/10G-X.
Per maggiori informazioni, riferirsi al data sheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html



### 2.3.2. Aruba - R8Q69AC

Gli switch HPE Aruba Networking CX 6200M, appartenenti alla tipologia 3 in convenzione Reti Locali 8, sono switch Layer 3 Ethernet in grado di supportare diversi servizi layer 2 e layer 3, offrendo alle Amministrazioni 48 porte Ethernet Base-T modulabili a 100-Mbps o 1000-Mbps, più quattro porte 10-Gigabit Ethernet (GbE) e power supply ridondato interno. Consentono il forwarding IPv4 e IPv6 e supportano i principali protocolli di routing dinamico quali RIPv2, RIPng e OSPF.

*HPE Aruba Networking CX 6200M 48G 4SFP+*

La serie Aruba CX 6200M è basato su una architettura ASIC Aruba di 7° generazione, offre un accesso da 1-GbE e può essere utilizzata nel perimetro di accesso (edge) del network o per collegare i cluster dei server nei data center.

Il sistema operativo Aruba AOS-CX, basato su microservizi, garantisce stabilità e resilienza del sistema stesso, consentendo l'integrazione dei servizi e mettendo a disposizione dell'utente finale funzionalità di programmabilità via REST-API, ma anche una migliore visibilità delle informazioni di stato della rete.

La tecnologia di clustering Aruba Virtual Stacking Framework (VSF) consente la configurazione di un virtual chassis di dimensione massima di 8 apparati attraverso le porte uplink 10-GbE presenti su questo modello di switch, consentendo una rapida scalabilità a supporto delle esigenze delle Amministrazioni. I modelli 6200M sono dotati di alimentazione modulare e pertanto possono implementare una alimentazione ridondata di tipo N+1.

- Caratteristiche Generali:
    - Supporto 48 porte IEEE 802.3 (100Mbps/1000Mbps) con 4 uplink 1-GbE/10-GbE;
    - Auto-MDIX consente l'adeguamento automatico per cavi dritti o crossover su tutte le porte 100/1000Mbps;
    - Configurazione Jumbo Frames per la gestione di frame di grandezza massima fino a 9198 Bytes;
    - Funzionalità di aggregazione dei link IEEE 802.3ad basata su protocollo LACP supportando fino a 32 interfacce aggregate con un massimo di 8 porte per interfaccia aggregata;
    - Individuazione dei link unidirezionali Uni-directional Link Detection (UDLD) consentendo di disattivare una porta qualora venga individuato traffico unidirezionale su un collegamento e prevenendo loop all'interno di una topologia Layer 2 con protocollo Spanning-Tree attivo;
    - Meccanismi di protezione contro packet storm broadcast, unknown unicast e multicast mediante la configurazione di soglie definite dall'utente;
    - Gli switch Aruba 6200M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 3 è disponibile il Power Supply X371 12VDC 250W AC. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum;
    - Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività;

- Funzionalità Layer 2:
    - Segmentazione Vlan e Vlan tagging IEEE 802.1Q fino a 4094 Vlan ID e 2000 Vlan simultanee;
    - Spanning Tree Protocol per la prevenzione dei loop di rete a protezione delle topologie Layer 2, supporto IEEE 802.1d standard Spanning-Tree Protocol, IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) e IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP);
    - Port Mirroring per la duplicazione del traffico in ingresso e uscita da una porta verso una porta di monitoring;
    - Protocollo di tunneling VXLAN per l'implementazione di reti virtualizzate che consentono una maggiore scalabilità;
    - Internet Group Management Protocol (IGMP) per la gestione e l'inoltro del traffico Multicast all'interno di una topologia Layer 2;
- Servizi Layer 3:
    - Supporto IPv4 e IPv6 con possibilità di implementazione dual-stack per consentire l'implementazione di entrambi i protocolli e facilitare la transizione dareti IPv4 a reti solo IPv6;
    - Address Resolution Protocol (ARP) per la risoluzione dei MAC address appartenenti ad un indirizzo IP presenti all'interno di una sottorete;
    - Protocolli di routing dinamici RIPv2, RIPng e OSPF per la gestione dinamiche del routing delle reti;
    - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
    - Access Control List (ACL) consentono di filtrare il traffico IP prevenendo accessi non autorizzati o implementare un controllo del traffico consentendo o bloccando l'inoltro dei pacchetti;
- Servizi di Sicurezza:
    - Servizi RADIUS e TACACS+ consentono di implementare strumenti di autenticazione per accesso ai dispositivi ed implementare controlli di accesso alla rete attraverso implementazione di meccanismi di autenticazione dei client;
    - Supporto per l'autenticazione IEEE 8092.1x e autenticazione centralizzata dei degli indirizzi MAC che controlla i permessi di accesso degli utenti alla rete secondo indirizzamento MAC e porte dello switch;

  - Management sicuro mediante implementazione di accesso CLI, GUI o MIB mediante protocolli SSHv2, HTTPS e SNMPv3;
  - Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP;

- Gestione e configurazione:
  - Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI) e Web network management per facilitare la gestione del sistema;
  - Accesso sicuro al dispositivo attraverso linea di comando (CLI) o web GUI attraverso l'implementazione di protocolli sicuri SSHv2 e HTTPS;
  - Sistema operativo modulare a microservizi a garanzia di una elevata stabilità ed una migliore ridondanza del sistema stesso;
  - Le Policy di segmentazione dinamica (Aruba Dynamic Segmentation) consentono di configurare i parametri di accesso alla rete automaticamente e consistenti su tutta l'infrastruttura per i client wired e wireless;
  - L'integrazione con Aruba Clearpass consente di riconoscere il client wired all'accesso e operare una configurazione ad-hoc della porta a cui il client è attestato, eliminando la necessità di configurare manualmente la porta per ogni client;
  - Interfaccia REST-API per la programmazione e l'automazione dei task configurativi.
- Quality of Services (QoS):
  - Gestione dei meccanismi di anti-congestione e prioritizzazione del traffico attraverso impostazione della Class of Services (CoS) mediante tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo Layer 3, port number TCP/UDP e DiffServ;
  - Meccanismi di accodamento Strict Priority (SP) e Deficit Weighted Round Robin (DWRR) e prioritizzazione del traffico per classificazione in tempo reale;
  - Tecnologia LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza la banda per tipologie di traffico time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce;

  - Virtual Output Queing (VOQ) consente di isolare le congestioni, prevendendo situazioni di head of line blocking a garanzia dell'inoltro del traffico in uscita dalle porte dello switch;

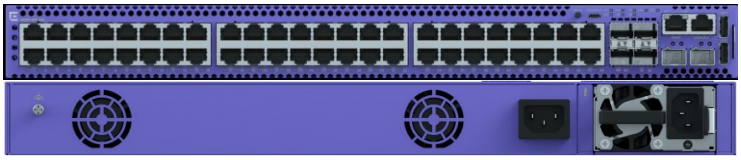
- Specifiche Tecniche:
  - 48 porte 10/100/1000 Mbps BaseT autosensing;
  - 4 porte SFP+ 100M/1/10 Gbps;
  - Capacità di stacking fino a 8 elementi della serie Aruba CX 62xx 24/48 porte;
  - Capacità di switching 176 Gbps;
  - Supporta fino a 32768 indirizzi MAC;
  - Supporta fino a 2048 prefissi IPv4 unicast e 1024 prefissi IPv6 unicast;
  - Latenza media 2,28 microsecondi 1 Gbps e 1,46 microsecondi 10 Gbps (con pacchetti di 64 Byte);
  - Assorbimento 60W con il 100% del traffico;
  - Dissipazione 232BTU/ora;
  - Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
  - Umidità operativa da 5% a 95% a 40°C, di stoccaggio da 5% a 95% a 65°C;
  - Occupazione spazio rack: 1 Rack Unit (RU);
  - Dimensioni: 44,2cm (L) x 38,5 (P) x 4,4 (A);
  - Peso 5,73 Kg.

### 2.3.3. Extreme Networks - 5420F-48T-4XE_C

Lo switch Extreme Networks 5420F-48T-4XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 256 Gbps di capacità di switching;
- 48 porte 10/100/1000BASE-T full/half duplex ports;
- 4 porte di uplink 1/10Gb Uplink SFP+ 10Gb;
- 2 porte di uplink/stacking SFPDD 10G/20G;
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 80Gb;

- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Supporto dei protocolli Fabric (sia Fabric Connect che Extreme IP Fabric) per la realizzazione di reti in tecnologia Fabric/SDN;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- MACsec sulle porte di accesso e uplink per garantire una crittografia sicura del collegamento;
- Ridotti consumi energetici (max 75 watt), silenzioso (35.3 dB), leggero e adatto ad armadi poco profondi (330 mm);
- Supporto protocolli SPBm – Fabric Connect;
- Supporto protocolli ad anello G.8032 e EAPS;
- Lo switch può essere gestito e configurato dalla CLI, via interfaccia Web, su piattaforma Cloud ExtremeCloudIQ o da piattaforma di gestione locale;
- Secondo alimentatore hot swappable opzionale.



*Extreme Networks 5420F-48T-4XE*

Scheda Tecnica Extreme Networks 5420

### 2.3.4. Juniper - EX3400-48T-C

Gli switch ethernet della serie EX3400 sono apparati ad alte prestazioni, in grado di soddisfare i requisiti delle reti enterprise convergenti (VoIP, video e data), ad un costo vantaggioso. Gli switch EX3400 sono switch compatti e forniscono prestazioni di categoria superiore ed elevata' affidabilità hardware e software.

Gli EX3400 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX3400 tra loro, come se fossero in singolo apparato logico.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo *Enhanced Limited Lifetime*; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia *Limited Lifetime* prevede la possibilità per l'end user di accedere a tutti gli upgade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

https://support.juniper.net/support/pdf/warranty/990240.pdf

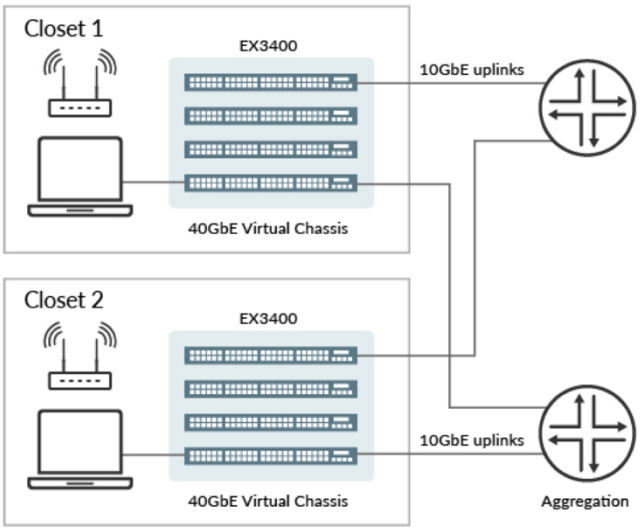
**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 48 x 1GbE + 4 x 1/10GbE SFP/SFP+ + 2 x 40GbE QSFP+ |
| Form Factor | 1RU |
| Power | Alimentazione ridondata |
| Switch capacity | 336 Gbps |

| | |
|---|---|
| Fabric | Virtual Chassis fino a 10 switch |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 10 EX3400 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.




**MACsec**

Gli switch EX3400 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer. Gli switch garantiscono 88Gbps di throughput con cifratura a livello hardware sulle porte 1/10Gbps.

***QoS con 12 code di priorità***

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

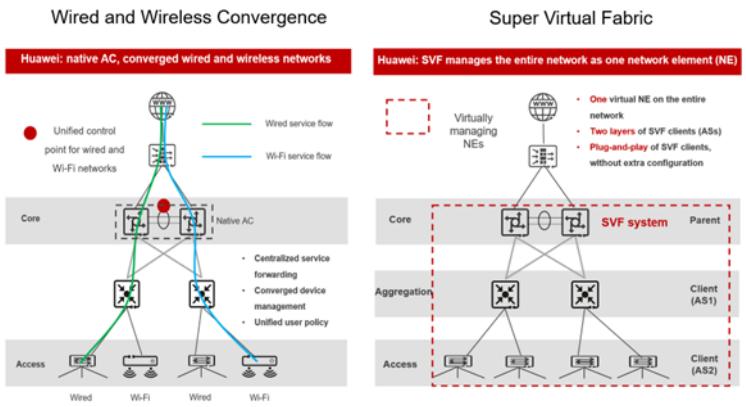
### 2.3.5. Huawei - S5731-H48T4XC-C

Il modello Ethernet Switch S5731-H48T4XC fa parte della series enhanced S5731-H. E' uno switch Full Layer 3 con supporto di IP routing statico, RIP e OSPF, BGP, IS-IS, VRRP. Grazie a funzionalità avanzate di MPLS è ideale anche in contesti metropolitani per realizzare infrastrutture uniche per più VPN. Inoltre, il supporto del VxLAN e del protocollo di control-plane BGP EVPN lo rende adatto anche come elemento di Edge per la soluzione CloudCampus di Huawei o per trasportare VLAN tra un sito all'altro connesso attraverso una rete di livello 3.

Può quindi essere dispiegato sia come switch di Accesso che di Aggregazione. Installabile a rack 19", profondo 42 cm, equipaggia 48 porte 10/100/1000 Ethernet su rame e 4 porte 10GE ottico su SFP+. In dotazione è fornito un cavo di stack da 1 metro e un modulo aggiuntivo con 8 porte 10G SFP+ installato sul retro. È possibile instaurare lo stack con i modelli della stessa series S5731-H. In termini di alimentazione, è dotato e fornito con un un alimentatore estraibile in AC che può essere ridondato nell'opportuno slot sul retro dell'apparato.


L'apparato ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed grazie alla switching capacity fino a 672 Gbit/s, supporta funzionalità di multicast di livello 2 e livello 3 (IGMP, MLD, PIM) e meccanismi loop prevention di livello 2 sia per reti ad anello che ad albero.

La famiglia S5731-H fornisce la funzionalità di WLAN AC Controller integrate (già licenziato per gestire 16 AP) che permette di gestire fino a 1024 AP ed evitando di utilizzare un appliance WLAN AC dedicato esterno, funzionalità particolarmente utile in realtà aziendali piccole/medie. Gestisce una capacità di switching per la componente Wireless fino a 543 Gbit/s e permette di gestire in maniera unificata l'autenticazione (supporta 802.1x, MAC e Portal) degli utenti wired e wireless semplificando la user experience di accesso dei terminali.




E' gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller nella soluzione Cloud Campus.

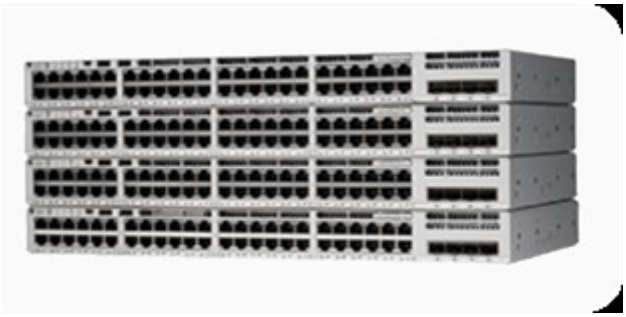
## 2.4. Switch Tipo 4

### 2.4.1. Cisco - C9200L-48P-4XC

Gli switch Cisco Catalyst 9200L sono switch Gigabit Ethernet stackable a configurazione fissa che estendono la potenza della rete intent-based e dell'innovazione hardware e software della moderna famiglia Catalyst 9000. Con 48 porte rame 10/100/1000 e 4 uplink 1/10G-X, operano con il nuovo software Cisco IOS-XE e supportano la gestione semplice e sicura della rete. Questi switch completamente gestibili supportano funzionalità avanzate di Layer 2 e base Layer 3. Progettati per semplificare l'operatività al fine di ridurre il costo totale di gestione, consentono trasporto scalabile, sicuro ed efficiente dal punto di vista energetico, con l'aggiunta di servizi e funzionalità intelligenti, quali Routed Access (RIP, EIGRP Stub, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder, SSO, AutoQoS, Perpetual PoE e Fast PoE (sui modelli PoE), Netflow.

Inoltre, gli stessi switch possono far parte dell'innovativa architettura di rete Cisco Software-Defined Access (SD-Access), che, attraverso automazione e funzionalità avanzate, consente una gestione centralizzata, potente e semplificata della sicurezza e dell'affidabilità di rete, con l'obiettivo di garantire conformità, efficienza operativa, visibilità ed esperienza utente semplificata.

L'offerta in Convenzione prevede un modello con 48 porte rame RJ45 10/100/1000, con funzionalità IEEE 802.3at (PoE fino a 30W) supportata sulle porte di accesso e 4 porte di uplink 1/10G-X. Per maggiori informazioni, riferirsi al data sheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html



### 2.4.2. Aruba - R8Q70AC

Gli switch HPE Aruba Networking 6200M, appartenenti alla tipologia 4 in convenzione Reti Locali 8, sono switch Layer 3 Ethernet in grado di supportare diversi servizi layer 2 e layer 3, offrendo alle Amministrazioni 48 porte Ethernet Base-T modulabili a 100-Mbps o 1-Gbps con supporto Power over Ethernet (PoE) di classe 4, più quattro porte 1/10 Gigabit Ethernet (GbE) e power supply ridondato interno. Consentono il forwarding IPv4 e IPv6 e supportano i principali protocolli di routing dinamico quali RIPv2, RIPng e OSPF.

*HPE Aruba Networking CX 6200M 48G Class 4 PoE 4 SFP+*

La serie HPE Aruba Networking CX 6200M è basato su una architettura ASIC Aruba di 7° generazione, offre un accesso da 1-GbE e può essere utilizzato nel perimetro di accesso (edge) del network o per collegare i cluster dei server nei data center.

Il sistema operativo Aruba AOS-CX, basato su microservizi, garantisce stabilità e resilienza del sistema stesso, consentendo l'integrazione dei servizi e mettendo a disposizione dell'utente finale funzionalità di programmabilità via REST-API, ma anche una migliore visibilità delle informazioni di stato della rete.

La tecnologia di clustering Aruba Virtual Stacking Framework (VSF) consente la configurazione di un virtual chassis di dimensione massima di 8 apparati attraverso le porte uplink 10-GbE presenti su questo modello di switch, consentendo una rapida scalabilità a supporto delle esigenze delle Amministrazioni. I modelli 6200M sono dotati di alimentazione modulare e pertanto possono implementare una alimentazione ridondata di tipo N+1.

- Caratteristiche Generali:
    - Supporto 48 porte IEEE 802.3 (100Mbps/1000Mbps) con 4 uplink 1-GbE/10-GbE;
    - Auto-MDIX consente l'adeguamento automatico per cavi dritti o crossover su tutte le porte 100/1000Mbps;
    - Configurazione Jumbo Frames per la gestione di frame di grandezza massima fino a 9198 Bytes;
    - Il supporto PoE standard IEEE 802.3at fornisce fino a 30 W sulle single porte per alimentazione di dispositivi locali;
    - Funzionalità di aggregazione dei link IEEE 802.3ad basata su protocollo LACP supportando fino a 32 interfacce aggregate con un massimo di 8 porte per interfaccia aggregata;
    - Individuazione dei link unidirezionali Uni-directional Link Detection (UDLD) consentendo di disattivare una porta qualora venga individuato traffico unidirezionale su un collegamento e prevenendo loop all'interno di una topologia Layer 2 con protocollo Spanning-Tree attivo;
    - Meccanismi di protezione contro packet storm broadcast, unknown unicast e multicast mediante la configurazione di soglie definite dall'utente;
    - Gli switch Aruba 6200M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 4 è disponibile il Power Supply Aruba X372 54VDC 1050W AC. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum;
    - Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività
- Funzionalità Layer 2:

  - Segmentazione Vlan e Vlan tagging IEEE 802.1Q fino a 4094 Vlan ID e 2000 Vlan simultanee;
  - Spanning Tree Protocol per la prevenzione dei loop di rete a protezione delle topologie Layer 2, supporto IEEE 802.1d standard Spanning-Tree Protocol, IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) e IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP);
  - Port Mirroring per la duplicazione del traffico in ingresso e uscita da una porta verso una porta di monitoring;
  - Protocollo di tunneling VXLAN per l'implementazione di reti virtualizzate che consentono una maggiore scalabilità;
  - Internet Group Management Protocol (IGMP) per la gestione e l'inoltro del traffico Multicast all'interno di una topologia Layer 2

- Servizi Layer 3:
  - Supporto IPv4 e IPv6 con possibilità di implementazione dual-stack per consentire l'implementazione di entrambi i protocolli e facilitare la transizione dareti IPv4 a reti solo IPv6;
  - Address Resolution Protocol (ARP) per la risoluzione dei MAC address appartenenti ad un indirizzo IP presenti all'interno di una sottorete;
  - Protocolli di routing dinamici RIPv2, RIPng e OSPF per la gestione dinamiche del routing delle reti;
  - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
  - Access Control List (ACL) consentono di filtrare il traffico IP prevenendo accessi non autorizzati o implementare un controllo del traffico consentendo o bloccando l'inoltro dei pacchetti;
- Servizi di Sicurezza:
  - Servizi RADIUS e TACACS+ consentono di implementare strumenti di autenticazione per accesso ai dispositivi ed implementare controlli di accesso alla rete attraverso implementazione di meccanismi di autenticazione dei client;
  - Supporto per l'autenticazione IEEE 8092.1x e autenticazione centralizzata dei degli indirizzi MAC che controlla i permessi di accesso degli utenti alla rete secondo indirizzamento MAC e porte dello switch;

  - Management sicuro mediante implementazione di accesso CLI, GUI o MIB mediante protocolli SSHv2, HTTPS e SNMPv3;
  - Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP.

- Gestione e configurazione:
  - Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI) e Web network management per facilitare la gestione del sistema;
  - Accesso sicuro al dispositivo attraverso linea di comando (CLI) o web GUI attraverso l'implementazione di protocolli sicuri SSHv2 e HTTPS;
  - Sistema operativo modulare a microservizi a garanzia di una elevata stabilità ed una migliore ridondanza del sistema stesso;
  - Le Policy di segmentazione dinamica (Aruba Dynamic Segmentation) consentono di configurare i parametri di accesso alla rete automaticamente e consistenti su tutta l'infrastruttura per i client wired e wireless;
  - L'integrazione con Aruba Clearpass consente di riconoscere il client wired all'accesso e operare una configurazione ad-hoc della porta a cui il client è attestato, eliminando la necessità di configurare manualmente la porta per ogni client;
  - Interfaccia REST-API per la programmazione e l'automazione dei task configurativi;
- Quality of Services (QoS):
  - Gestione dei meccanismi di anti-congestione e prioritizzazione del traffico attraverso impostazione della Class of Services (CoS) mediante tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo Layer 3, port number TCP/UDP e DiffServ;
  - Meccanismi di accodamento Strict Priority (SP) e Deficit Weighted Round Robin (DWRR) e prioritizzazione del traffico per classificazione in tempo reale;
  - Tecnologia LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza la banda per le tipologie di traffico time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce;

  - Virtual Output Queing (VOQ) consente di isolare le congestioni, prevendendo situazioni di head of line blocking a garanzia dell'inoltro del traffico in uscita dalle porte dello switch;

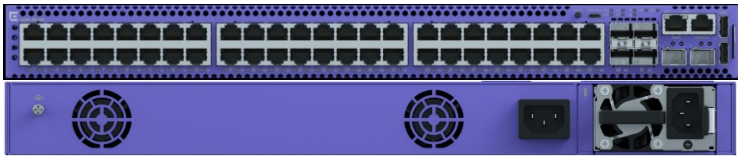
- Specifiche Tecniche:
  - 48 porte 10/100/1000 Mbps BaseT autosensing PoE Class 4 fino a 30W per porta;
  - 4 porte SFP+ 100M/1/10 Gbps;
  - Capacità di stacking fino a 8 elementi della serie Aruba CX 62xx 24/48 porte;
  - Capacità di switching 176 Gbps;
  - Supporta fino a 32768 indirizzi MAC;
  - Supporta fino a 2048 prefissi IPv4 unicast e 1024 prefissi IPv6 unicast;
  - Latenza media 2,28 microsecondi 1 Gbps e 1,46 microsecondi 10 Gbps (con pacchetti di 64 Byte);
  - Assorbimento 73W con il 100% del traffico;
  - Dissipazione 260BTU/ora;
  - Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
  - Umidità operativa da 5% a 95% a 40°C, di stoccaggio da 5% a 95% a 65°C;
  - Occupazione spazio rack: 1 Rack Unit (RU);
  - Dimensioni: 44,2cm (L) x 38,5 (P) x 4,4 (A)
  - Peso 6,15 Kg.

### 2.4.3. Extreme Networks - 5420F-48P-4XE_C

Lo switch Extreme Networks 5420F-48P-4XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 208 Gbps di capacità di switching;
- 48 porte 10/100/1000BASE-T full/half duplex ports;
- 4 porte di uplink 1/10Gb Uplink SFP+ 10Gb;
- 2 porte di uplink/stacking SFPDD 10G/20G;
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 80Gb;

- Supporto PoE da 30W (IEEE 802.3at): lo switch supporta la tecnologia Power over Ethernet (PoE) con una potenza massima di 30 watt, conforme allo standard IEEE 802.3at su tutte le porte. Supporto del PoE fast (le periferiche PoE connesse vengono immediatamente alimentate appena lo switch è acceso) e perpetuo (le periferiche PoE connesse non si spengono in caso di riavvio dello switch);
- 740watt PoE budget;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Supporto dei protocolli Fabric (sia Fabric Connect che Extreme IP Fabric) per la realizzazione di reti in tecnologia Fabric/SDN;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- Adatto ad armadi poco profondi (330 mm);
- MACsec sulle porte di accesso e uplink per garantire una crittografia sicura del collegamento;
- Supporto protocolli SPBm – Fabric Connect;
- Supporto protocolli ad anello G.8032 e EAPS;
- Lo switch può essere gestito e configurato dalla CLI, via interfaccia Web, su piattaforma Cloud ExtremeCloudIQ o da piattaforma di gestione locale;
- Secondo alimentatore hot swappable opzionale.



*Extreme Networks 5420F-48P-4XE*

Scheda Tecnica Extreme Networks 5420

### 2.4.4. Juniper - EX3400-48P-C

Gli switch ethernet della serie EX3400 sono apparati ad alte prestazioni, in grado di soddisfare i requisiti delle reti enterprise convergenti (voip, video e data), ad un costo vantaggioso. Gli switch EX3400 sono switch compatti e forniscono prestazioni di categoria superiore ed elevata' affidabilità hardware e software.

Gli EX3400 sono “cloud-ready” e supportano l’installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX3400 tra loro, come se fossero in singolo apparato logico

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo *Enhanced Limited Lifetime*; la sostituzione hardware è garantita per tutta la vita dell’apparato. L’accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall’apertura del ticket di RMA.

Per le parti software la garanzia *Limited Lifetime* prevede la possibilita’ per l’end user di accedere a tutti gli upgade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

https://support.juniper.net/support/pdf/warranty/990240.pdf

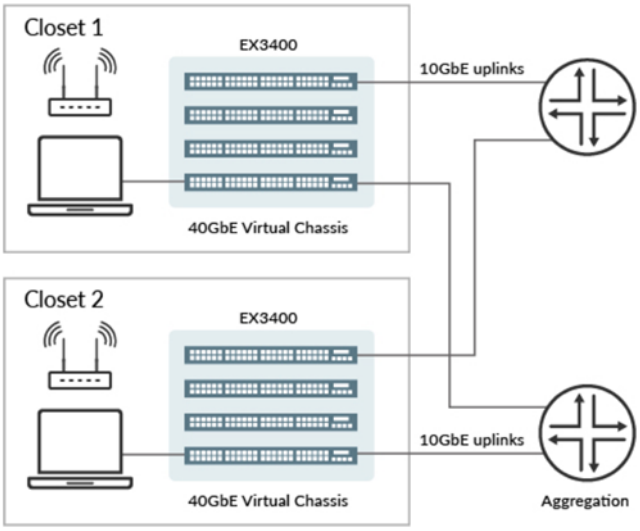
**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 48 x 1GbE + 4 x 1/10GbE SFP/SFP+ + 2 x 40GbE QSFP+ |
| Power | PSU ridondata, PoE/PoE+ fino a 30W per porta |

| | |
|---|---|
| Switch capacity | 336 Gbps |
| Fabric | Virtual Chassis fino a 10 switch |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 10 EX3400 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.




**MACsec**

Gli switch EX3400 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer. Gli switch garantiscono 88Gbps di throughput con cifratura a livello hardeware sulle porte 1/10Gbps.

***QoS con 12 code di priorità***

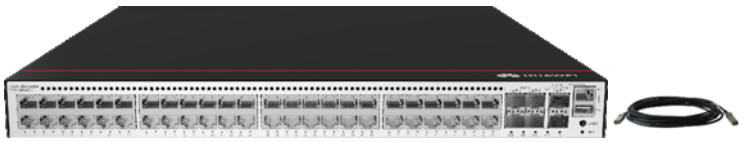
Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettono, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

### 2.4.5. Huawei - S5735-S48P4XE-V2-C

Il modello Ethernet Switch S5735-S48P4XE-V2 fa parte della series enhanced CloudEngine S5735-S-V2.

È uno switch Full Layer 3 con supporto di IP routing statico, RIP e OSPF, BGP, IS-IS, VRRP. Grazie a funzionalità avanzate di MPLS è ideale anche in contesti metropolitani per realizzare infrastrutture uniche per più VPN. Inoltre, il supporto del VxLAN e del protocollo di control-plane BGP EVPN lo rende adatto anche come elemento di Edge per la soluzione CloudCampus di Huawei o per trasportare VLAN tra un sito all'altro connesso attraverso una rete di livello 3.

Può quindi essere dispiegato sia come switch di Accesso che di Aggregazione. Installabile a rack 19", profondo 42 cm, equipaggia 48 porte 10/100/1000 PoE+ Ethernet su rame e 4 porte 10GE (operanti anche a 1GE) ottico su SFP+. In dotazione è fornito un cavo di stack da 1 metro e un modulo aggiuntivo con 8 porte 10G SFP+ da installare sul retro. È possibile instaurare lo stack con i modelli della stessa series S5731-H. In termini di alimentazione, è dotato di un alimentatore da 1000W estraibile in AC che può essere ridondato nell'opportuno slot sul retro dell'apparato.



*CloudEngine S5735-S48P4XE-V2*

L'apparato ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed grazie alla switching capacity fino a 672 Gbit/s, supporta funzionalità di multicast di livello 2 e livello 3 (IGMP, MLD, PIM) e meccanismi loop prevention di livello 2 sia per reti ad albero che ad anello (G.8032).

E' gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller della soluzione CloudCampus.

## 2.5. Switch Tipo 5

### 2.5.1. Cisco - C9300L-48UXG-4XC

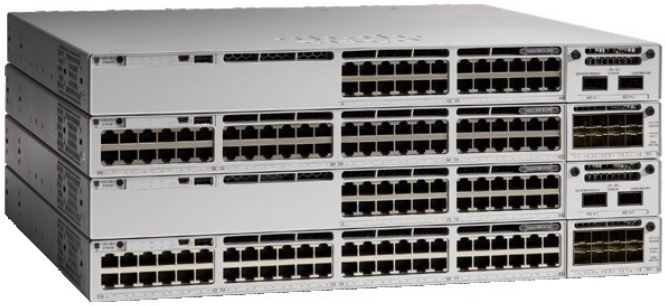
La serie Catalyst 9300 è la nuova generazione di switch stackable più diffusa del settore, premiata dalla prestigiosa rivista tecnica CRN come "Overall Network Product of the Year" nel 2018. Concepita per offrire performance, sicurezza, scalabilità e flessibilità, costituisce inoltre l'elemento fondante dell'architettura Cisco Software-Defined Access (SD-Access).

Gli switch Catalyst 9300 sono basati sull'architettura Cisco Unified Access ™ Data Plane 2.0 (UADP) 2.0, che non solo protegge il vostro investimento, ma consente anche una scalabilità più ampia e un throughput più elevato. Un sistema operativo moderno, Cisco IOS® XE ampiamente programmabile offre funzionalità di sicurezza avanzate e convergenza adeguate alle esigenze del mondo Internet of Things (IoT). Sono inoltre pronti a supportare il futuro: con un'architettura CPU x86 e più memoria, consentono di ospitare container ed eseguire applicazioni e script di terze parti in modo nativo all'interno dello switch.

I Cisco Catalyst 9300 supportano funzionalità Layer 2 e Layer 3 (Routed Access RIP, EIGRP Stub, OSPF - 1000 routes, PBR, PIM Stub Multicast 1000 routes, PVLAN, VRRP, PBR, CDP, FHS, CoPP, SXP, IP SLA Responder), a cui aggiungono ulteriori funzioni avanzate di sicurezza (Cisco Trust Anchor, Encrypted Traffic Analytics, MACSEC IEEE 802.1AE, 802.1X), scalabilità (StackWise-480 con stacking a 480Gbps), alta affidabilità (cross-stack etherchannel, NSF/SSO, port autorecovery), qualità del servizio (CoS, DSCP, CIR, SRR), visibilità (NBAR, NetFlow).

L'offerta in Convenzione prevede un modello con 48 porte rame RJ45, di cui 12 multi-gigabit da 100Mbps, 1Gbps, 2,5Gbps, 5Gbps o 10Gbps, e le rimanenti 36 porte 10/100/1000. La funzionalità IEEE 802.3bt type 3 (PoE fino a 60W) è supportata su tutte 48 le porte di accesso. Il modello prevede inoltre un modulo di uplink con 8 porte 1/10G-X.

Per maggiori informazioni, riferirsi al data sheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html



### 2.5.2. Aruba - R8Q71AC

Gli switch HPE Aruba Networking 6200M, appartenenti alla tipologia 5 in convenzione Reti Locali 8, sono switch Layer 3 Ethernet in grado di supportare diversi servizi layer 2 e layer 3, offrendo alle Amministrazioni 36porte Ethernet Base-T modulabili a 10-Mbps, 100-Mbps o 1-Gbps con supporto Power over Ethernet (PoE+) di classe 6, 12 porte di tipo smartrate 100-Mbps/1-Gbps/2,5Gbps/5-Gbps Base-T anch'esse con supporto PoE+ di classe 6, più quattro porte 1/10 Gigabit Ethernet (GbE) e power supply ridondato interno. Consentono il forwarding IPv4 e IPv6 e supportano i principali protocolli di routing dinamico quali RIPv2, RIPng e OSPF.

*HPE Aruba Networking CX 6200M 36G 12SR5 4SFP+*

La serie Aruba CX 6200M è basato su una architettura ASIC Aruba di 7° generazione ed offre un accesso fino a 1-GbE e 5GbE che può essere utilizzato nel perimetro di accesso (edge) del network o per collegare dispositivi che richiedono un assorbimento fino a 60w e una elevata banda passante.

Il sistema operativo Aruba AOS-CX, basato su microservizi, garantisce stabilità e resilienza del sistema stesso, consentendo l'integrazione dei servizi e mettendo a disposizione dell'utente finale funzionalità di programmabilità via REST-API, ma anche una migliore visibilità delle informazioni di stato della rete.

La tecnologia di clustering Aruba Virtual Stacking Framework (VSF) consente la configurazione di un virtual chassis di dimensione massima di 8 apparati attraverso le porte uplink 10-GbE presenti su questo modello di switch, consentendo una rapida scalabilità a supporto delle esigenze delle Amministrazioni. I

modelli 6200M sono dotati di alimentazione modulare e pertanto possono implementare una alimentazione ridondata di tipo N+1.

- Caratteristiche Generali:
    - Supporto 48 porte IEEE 802.3 (100Mbps/1000Mbps) con 4 uplink 1-GbE/10-GbE;
    - Auto-MDIX: adeguamento automatico per cavi dritti o crossover su tutte le porte 100/1000Mbps;
    - Configurazione Jumbo Frames per la gestione di frame di grandezza massima fino a 9198 Bytes;
    - Il supporto PoE standard IEEE 802.3bt High Power PoE di classe 6, fornisce fino a 60 W sulle singole porte Base-T per alimentazione di dispositivi IoT locali e access point;
    - Funzionalità di aggregazione dei link IEEE 802.3ad basata su protocollo LACP supportando fino a 32 interfacce aggregate con un massimo di 8 porte per interfaccia aggregata;
    - Individuazione dei link unidirezionali Uni-directional Link Detection (UDLD) consentendo di disattivare una porta qualora venga individuato traffico unidirezionale su un collegamento e prevenendo loop all'interno di una topologia Layer 2 con protocollo Spanning-Tree attivo;
    - Meccanismi di protezione contro packet storm broadcast, unknown unicast e multicast mediante la configurazione di soglie definite dall'utente;
    - Gli switch Aruba 6300M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 3 è disponibile il Power Supply Aruba X372 54VDC 1050W AC. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum;
    - Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività;
- Funzionalità Layer 2:
    - Segmentazione Vlan e Vlan tagging IEEE 802.1Q fino a 4094 Vlan ID e 2000 Vlan simultanee;

  - Spanning Tree Protocol per la prevenzione dei loop di rete a protezione delle topologie Layer 2, supporto IEEE 802.1d standard Spanning-Tree Protocol, IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) e IEE 802.1w Rapid Spanning-Tree Protocol (RSTP);
  - Port Mirroring per la duplicazione del traffico in ingresso e uscita da una porta verso una porta di monitoring;
  - Protocollo di tunneling VXLAN per l'implementazione di reti virtualizzate che consentono una maggiore scalabilità;
  - Internet Group Management Protocol (IGMP) per la gestione e l'inoltro del traffico Multicast all'interno di una topologia Layer 2;

- Servizi Layer 3:
  - Supporto IPv4 e IPv6 con possibilità di implementazione dual-stack per consentire l'introduzione di entrambi i protocolli e facilitare la transizione dareti IPv4 a reti solo IPv6;
  - Address Resolution Protocol (ARP) per la risoluzione dei MAC address appartenenti ad un indirizzo IP presenti all'interno di una sottorete;
  - Protocolli di routing dinamici RIPv2, RIPng e OSPF per la gestione dinamiche del routing delle reti;
  - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
  - Access Control List (ACL) consentono di filtrare il traffico IP prevenendo accessi non autorizzati o implementare un controllo del traffico consentendo o bloccando l'inoltro dei pacchetti;
- Servizi di Sicurezza:
  - Servizi RADIUS e TACACS+ consentono di implementare strumenti di autenticazione per accesso ai dispositivi ed implementare controlli di accesso alla rete attraverso implementazione di meccanismi di autenticazione dei client;
  - Supporto per l'autenticazione IEEE 8092.1x e autenticazione centralizzata dei degli indirizzi MAC che controlla i permessi di accesso degli utenti alla rete secondo indirizzamento MAC e porte dello switch;
  - Management sicuro mediante implementazione di accesso CLI, GUI o MIB mediante protocolli SSHv2, HTTPS e SNMPv3;

  - Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP;

- Gestione e configurazione:
  - Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema;
  - Accesso sicuro al dispositivo attraverso linea di comando (CLI) o web GUI attraverso l'implementazione di protocolli sicuri SSHv2 e HTTPS;
  - Sistema operativo modulare a microservizi a garanzia di una elevata stabilità ed una migliore ridondanza del sistema stesso;
  - Le Policy di segmentazione dinamica (Aruba Dynamic Segmentation) consentono di configurare i parametri di accesso alla rete autmaticamente e consistenti su tutta l'infrastruttura per i client wired e wireless;
  - L'integrazione con Aruba Clearpass consente di riconoscere il client wired all'accesso e operare una configurazione ad-hoc della porta a cui il client è attestato, eliminando la necessità di configurare manualmente la porta per ogni client;
  - Interfaccia REST-API per la programmazione e l'automazione dei task configurativi;
- Quality of Services (QoS):
  - Gestione dei meccanismi di anti-congestione e prioritizzazione del traffico attraverso impostazione della Class of Services (CoS) mediante tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo Layer 3, port number TCP/UDP e DiffServ;
  - Meccanismi di accodamento Strict Priority (SP) e Deficit Weighted Round Robin (DWRR) e prioritizzazione del traffico per classificazione in tempo reale;
  - Tecnologia LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza la banda per le tipologie di traffico time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce;
  - Virtual Output Queing (VOQ) consente di isolare le congestioni, prevendendo situazioni di head of line blocking a garanzia dell'inoltro del traffico in uscita dalle porte dello switch;
- Specifiche Tecniche:

- 36 porte 10/100/1000 Mbps BaseT autosensing PoE Class 6 fino a 60W per porta;
- 12 porte smartrate 100 Mbps - 1/2,5/5 Gbps BaseT autosensing PoE Class 6 fino a 60W per porta;
- 4 porte SFP+ 100 Mbps - 1/10 Gbps;
- Capacità di stacking fino a 8 elementi della serie Aruba CX 62xx 24/48 porte;
- Capacità di switching 272 Gbps;
- Supporta fino a 32768 indirizzi MAC;
- Supporta fino a 2048 prefissi IPv4 unicast e 1024 prefissi IPv6 unicast;
- Latenza media 2,28 microsecondi 1 Gbps e 1,46 microsecondi 10 Gbps (con pacchetti di 64 Byte);
- Assorbimento 96W con il 100% del traffico;
- Dissipazione 260BTU/ora;
- Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
- Umidità operativa da 5% a 95% a 40°C, di stoccaggio da 5% a 95% a 65°C;
- Occupazione spazio rack: 1 Rack Unit (RU);
- Dimensioni: 44,2cm (L) x 38,5 (P) x 4,4 (A);
- Peso 6,31 Kg.

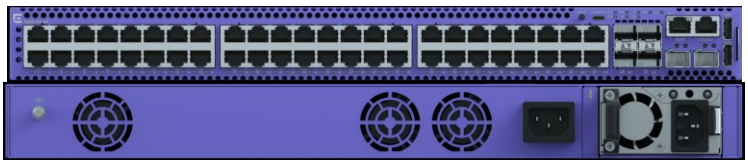
### 2.5.3. Extreme Networks - 5420F-16MW-32P-4XE_C

Lo switch Extreme Networks 5420F-16MW-32P-4XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 304 Gbps di capacità di switching;
- 16 porte 100/1000/2500BASE-T, 32 porte 10/100/1000BASE-T full/half duplex ports;
- 4 porte di uplink 1/10Gb Uplink SFP+ 10Gb;
- 2 porte di uplink/stacking SFPDD 10G/20G;
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 80Gb;
- Supporto PoE da 90W (803.3bt) disponibile su 16 porte: lo switch supporta la tecnologia Power over Ethernet (PoE) con una potenza massima di 90 watt, conforme allo standard IEEE 802.3bt su tutte

le porte. Supporto del PoE fast (le periferiche PoE connesse vengono immediatamente alimentate appena lo switch è acceso) e perpetuo (le periferiche PoE connesse non si spengono in caso di riavvio dello switch);

- Supporto PoE da 30W (IEEE 802.3at) disponibile su 32 porte: lo switch supporta la tecnologia Power over Ethernet (PoE) con una potenza massima di 30 watt, conforme allo standard IEEE 802.3at su tutte le porte. Supporto del PoE fast (le periferiche PoE connesse vengono immediatamente alimentate appena lo switch è acceso) e perpetuo (le periferiche PoE connesse non si spengono in caso di riavvio dello switch);
- 960watt PoE budget;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Supporto dei protocolli Fabric (sia Fabric Connect che Extreme IP Fabric) per la realizzazione di reti in tecnologia Fabric/SDN;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- Adatto ad armadi poco profondi (330 mm);
- MACsec sulle porte di accesso e uplink per garantire una crittografia sicura del collegamento;
- Supporto protocolli SPBm – Fabric Connect;
- Supporto protocolli ad anello G.8032 e EAPS;
- Lo switch può essere gestito e configurato dalla CLI, via interfaccia Web, su piattaforma Cloud ExtremeCloudIQ o da piattaforma di gestione locale;
- Secondo alimentatore hot swappable opzionale.



*Extreme Networks 5420F-16MW-32P-4XE*

Scheda Tecnica Extreme Networks 5420

### 2.5.4. Juniper - EX4100-48MP-C

Lo switch ethernet EX4100-48MP è un apparato ad alte prestazioni per infrastrutture LAN campus e branch che supportano servizi avanzati. Le infrastrutture moderne, infatti, devono supportare WI-FI 802.11ax (Wifi 6 e Wifi 6E) e velocità multi-gigabit 1/2.5 GbE con PoE fino a 90W per porta.

Gli EX4100 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4100 tra loro, come se fossero in singolo apparato logico.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo *Enhanced Limited Lifetime*; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia *Limited Lifetime* prevede la possibilita' per l'end user di accedere a tutti gli upgade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

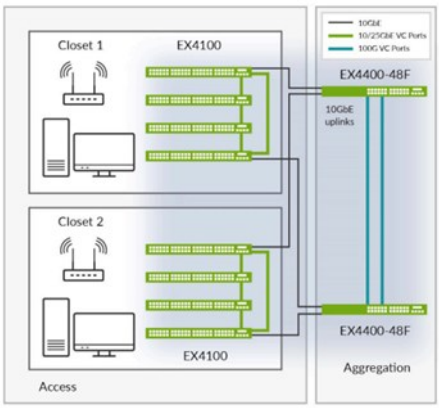
https://support.juniper.net/support/pdf/warranty/990240.pdf

**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 16x100 MB/1GbE/2.5GbE + 32x10 MB/100 MB/1GbE - 4x10GbE uplinks, 4x25GbE stacking/uplink |
| Power | PSU ridondata – PoE/PoE+/PoE++ fino a 90W per porta |
| Switch capacity | 424 Gbps |
| Fabric | Virtual Chassis fino a 10 switch, EVPN/VxLAN |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4100 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.




**MACsec AES256**

Gli switch EX4100 supportano IEEE 802.1ae MACsec AES256 e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

***PoE++***

Lo switch EX4100 Multi gigabit supporta lo standard 802.3bt e fornisce fino a 90watts per porta per dispostivi ad alto assorbimento come terminali Virtual Desktop Infrastructure (VDI), telefono IP, APs.

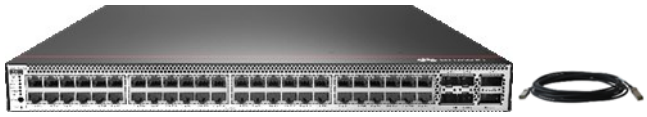
***Campus Fabric***

*Lo switch supporta fabric IP con overlay EVPN-VxLAN. La fabric può estendere la connettività tra più siti e realizzare l'estensione a livello 2 della rete (L2 stretch).*

### 2.5.5. Huawei - S5732-H48UM4Y2CZV2-C

Il modello Ethernet Switch CloudEngineS5732-H48UM4Y2CZ-V2 fa parte della series enhanced CloudEngine S5732-H-V2.

È uno switch Full Layer 3 con supporto di IP routing statico, RIP e OSPF, BGP, IS-IS, VRRP. Grazie a funzionalità avanzate di MPLS è ideale anche in contesti metropolitani per realizzare infrastrutture uniche per più VPN. Inoltre il supporto del VxLAN e del protocollo di control-plane BGP EVPN lo rende adatto anche come elemento di Edge per la soluzione CloudCampus di Huawei o per trasportare VLAN tra un sito all'altro connessi attraverso una rete di livello 3.



*CloudEngine S5732-H48UM4Y2CZ-V2*

Può essere dispiegato sia come switch di Accesso per le interfacce Multigigabit Ethernet (2.5/5G/10G) che di Aggregazione. Installabile a rack 19", equipaggia 48 × 100M/1000M/2.5G/5G/10G Base-T Ethernet ports PoE++, in uplink 4 x 10/25GE SFP28 +,2 x 40/100GE QSFP28. In dotazione è fornito un cavo di stack da 1 metro. In termini di alimentazione, è dotato e fornito con un alimentatore da 1000W estraibile in AC che può essere ridondato nell'opportuno slot sul retro dell'apparato.

Ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed grazie alla switching capacity di 2.4 Tbit/s, supporta funzionalità avanzate proprie delle famiglie S5732-H-V2.

È gestibile (configurazione, monitoraggio e allaramistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller della soluzione CloudCampus.

## 2.6. Switch Tipo 6

### 2.6.1. Cisco - C9300-48UC

La serie Catalyst 9300 è la nuova generazione di switch stackable più diffusa del settore, premiata dalla prestigiosa rivista tecnica CRN come "Overall Network Product of the Year" nel 2018. Concepita per offrire performance, sicurezza, scalabilità e flessibilità, costituisce inoltre l'elemento fondante dell'architettura Cisco Software-Defined Access (SD-Access).

Gli switch Catalyst 9300 sono basati sull'architettura Cisco Unified Access ™ Data Plane 2.0 (UADP) 2.0, che non solo protegge il vostro investimento, ma consente anche una scalabilità più ampia e un throughput più elevato. Un sistema operativo moderno, Cisco IOS® XE ampiamente programmabile offre funzionalità di sicurezza avanzate e convergenza adeguate alle esigenze del mondo Internet of Things (IoT). Sono inoltre pronti a supportare il futuro: con un'architettura CPU x86 e più memoria, consentono di ospitare container ed eseguire applicazioni e script di terze parti in modo nativo all'interno dello switch.

I Cisco Catalyst 9300 supportano funzionalità Layer 2 e Layer 3 (Routed Access RIP, EIGRP Stub, OSPF - 1000 routes, PBR, PIM Stub Multicast 1000 routes, PVLAN, VRRP, PBR, CDP, FHS, CoPP, SXP, IP SLA Responder), a cui aggiungono ulteriori funzioni avanzate di sicurezza (Cisco Trust Anchor, Encrypted Traffic Analytics, MACSEC IEEE 802.1AE, 802.1X), scalabilità (StackWise-480 con stacking a 480Gbps), alta affidabilità (cross-stack etherchannel, NSF/SSO, port autorecovery), qualità del servizio (CoS, DSCP, CIR, SRR), visibilità (NBAR, NetFlow).

L'offerta in Convenzione prevede un modello con 48 porte rame RJ45 10/100/1000, con funzionalità IEEE 802.2at (PoE fino a 30W su tutte le porte, fino a 60W su un massimo di 30 porte) e un modulo di uplink con 8 porte 1/10G-X. Supporta inoltre funzionalità di routing dinamico Layer 3 (BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM-BIDIR, IP SLA, OSPF).

Per maggiori informazioni, riferirsi al datasheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

### 2.6.2. Aruba - JL661AC

Gli HPE Aruba Networking CX 6300M, appartenenti alla tipologia 6 in convenzione Reti Locali 8, sono switch Layer 3 Ethernet in grado di supportare diversi servizi layer 2 e layer 3 avanzati, offrendo alle Amministrazioni 48 porte Ethernet Base-T modulabili a 10-Mbps, 100-Mbps o 1-Gbps con supporto Power over Ethernet (PoE) di classe 4, più quattro porte 1/10/25/50 Gigabit Ethernet (GbE) e power supply ridondato interno. Consentono il forwarding IPv4 e IPv6 e supportano i principali protocolli di routing dinamico quali RIPv2, RIPng, OSPF e BGP, ma anche supporto di costrutti di virtualizzazione avanzata quali EVPN e VXLAN per offrire una elevata scalabilità.

*HPE Aruba Networking CX 6300M 48G Class 4 PoE 4 SFP56*

La serie Aruba CX 6300M è basato su una architettura ASIC Aruba di 7° generazione ed offre un accesso da 1-GbE e può essere utilizzata nel perimetro di accesso (edge) del network o per collegare i cluster dei server nei data center in una implementazione di tipo Top of Rack (ToR).

Il sistema operativo Aruba AOS-CX, basato su microservizi, garantisce stabilità e resilienza del sistema stesso, consentendo l'integrazione dei servizi e mettendo a disposizione dell'utente finale funzionalità di programmabilità via REST-API, ma anche una migliore visibilità delle informazioni di stato della rete.

La tecnologia di clustering Aruba Virtual Stacking Framework (VSF) permette la configurazione di un virtual chassis di dimensione massima di 10 apparati attraverso le porte uplink che supportano fino a 50-GbE presenti su questo modello di switch, consentendo una rapida scalabilità a supporto delle esigenze delle Amministrazioni. I modelli 6300M possono essere dotati di alimentazione ridondata di tipo N+1 con alimentatori doppi hot-swap.

- Caratteristiche Generali:
    - Supporto 48 porte IEEE 802.3 (100Mbps/1000Mbps) con 4 uplink 1-GbE/10-GbE/25-GbE/50-GbE (Il supporto 50-GbE è inteso con utilizzo cavo DAC per realizzare uno stack VSF, il supporto dei transceiver 50G SR è stato introdotto nella release 10.09.1010);
    - Auto-MDIX: adeguamento automatico per cavi dritti o crossover su tutte le porte 100/1000Mbps;
    - Configurazione Jumbo Frames per la gestione di frame di grandezza massima fino a 9198 Bytes;
    - Il supporto PoE standard IEEE 802.3at e 802.3af fornisce fino a 30 W sulle single porte per alimentazione di dispositivi locali;
    - Funzionalità di aggregazione dei link IEEE 802.3ad basata su protocollo LACP supportando fino a 32 interfacce aggregate con un massimo di 8 porte per interfaccia aggregata;
    - Individuazione dei link unidirezionali Uni-directional Link Detection (UDLD) consentendo di disattivare una porta qualora venga individuato traffico unidirezionale su un collegamento e prevenendo loop all'interno di una topologia Layer 2 con protocollo Spanning-Tree attivo;
    - Meccanismi di protezione contro packet storm broadcast, unknown unicast e multicast mediante la configurazione di soglie definite dall'utente;
    - Gli switch Aruba 6300M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 3 è disponibile il Power Supply Aruba X372 54VDC 1050W AC. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum;
    - Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività;
- Funzionalità Layer 2:

  - Segmentazione Vlan e Vlan tagging IEEE 802.1Q fino a 4094 Vlan ID;
  - Spanning Tree Protocol per la prevenzione dei loop di rete a protezione delle topologie Layer 2, supporto IEEE 802.1d standard Spanning-Tree Protocol, IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) e IEE 802.1w Rapid Spanning-Tree Protocol (RSTP);
  - Port Mirroring per la duplicazione del traffico in ingresso e uscita da una porta verso una porta di monitoring;
  - Protocollo di tunneling VXLAN per l'implementazione di reti virtualizzate che consentono una maggiore scalabilità;
  - Internet Group Management Protocol (IGMP) per la gestione e l'inoltro del traffico Multicast all'interno di una topologia Layer 2;

- Servizi Layer 3:
  - Supporto IPv4 e IPv6 con possibilità di implementare dual-stack per consentire l'adozione di entrambi i protocolli e facilitare la transizione da reti IPv4 a reti solo IPv6;
  - Address Resolution Protocol (ARP) per la risoluzione dei MAC address appartenenti ad un indirizzo IP presenti all'interno di una sottorete;
  - Protocolli di routing dinamici RIPv2, RIPng e OSPF per la gestione dinamiche del routing delle reti;
  - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
  - Access Control List (ACL) consentono di filtrare il traffico IP prevenendo accessi non autorizzati o implementare un controllo del traffico consentendo o bloccando l'inoltro dei pacchetti.
- Servizi di Sicurezza:
  - Servizi RADIUS e TACACS+ consentono di implementare strumenti di autenticazione per accesso ai dispositivi ed implementare controlli di accesso alla rete attraverso implementazione di meccanismi di autenticazione dei client;
  - Supporto per l'autenticazione IEEE 8092.1x e autenticazione centralizzata dei degli indirizzi MAC che controlla i permessi di accesso degli utenti alla rete secondo indirizzamento MAC e porte dello switch;
  - Management sicuro mediante implementazione di accesso CLI, GUI o MIB mediante protocolli SSHv2, HTTPS e SNMPv3;

  - Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP;

- Gestione e configurazione:
  - Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI) e Web network management per facilitare la gestione del sistema;
  - Accesso sicuro al dispositivo attraverso linea di comando (CLI) o web GUI attraverso l'implementazione di protocolli sicuri SSHv2 e HTTPS;
  - Le Policy di segmentazione dinamica (Aruba Dynamic Segmentation) consentono di configurare i parametri di accesso alla rete automaticamente e consistenti su tutta l'infrastruttura per i client wired e wireless;
  - L'integrazione con Aruba Clearpass consente di riconoscere il client wired all'accesso e operare una configurazione ad-hoc della porta a cui il client è attestato, eliminando la necessità di configurare manualmente la porta per ogni client;
  - Interfaccia REST-API per la programmazione e l'automazione dei task configurativi.
- Quality of Services (QoS):
  - Gestione dei meccanismi di anti-congestione e prioritizzazione del traffico attraverso impostazione della Class of Services (CoS) mediante tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo Layer 3, port number TCP/UDP e DiffServ;
  - Meccanismi di accodamento Strict Priority (SP) e Deficit Weighted Round Robin (DWRR) e prioritizzazione del traffico per classificazione in tempo reale;
  - Tecnologia LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza la banda per le tipologie di traffico time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce;
  - Virtual Output Queing (VOQ) consente di isolare le congestioni, prevendendo situazioni di head of line blocking a garanzia dell'inoltro del traffico in uscita dalle porte dello switch;
- Specifiche Tecniche:
  - 48 porte 10/100/1000 Mbps BaseT autosensing PoE Class 4 fino a 30W per porta;
  - 4 porte SFP+ 1/10/25/50 Gbps;

- Capacità di stacking fino a 10 elementi della serie Aruba CX 63xx;
- Capacità di switching 880 Gbps;
- Supporta fino a 32768 indirizzi MAC;
- Supporta fino a 61000 prefissi IPv4 unicast e 61000 prefissi IPv6 unicast;
- Latenza media 2,28 microsecondi 1 Gbps, 1,46 microsecondi 10 Gbps, 1,9 microsecondi 25 Gbps e 3,59 microsecondi 50 Gbps (con pacchetti di 64 Byte);
- Assorbimento 96W con il 100% del traffico;
- Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
- Umidità operativa da 5% a 95% a 40°C, di stoccaggio da 5% a 95% a 65°C;
- Occupazione spazio rack: 1 Rack Unit (RU);
- Dimensioni: 44,2cm (L) x 38,5 (P) x 4,4 (A);
- Peso 5,72 Kg.

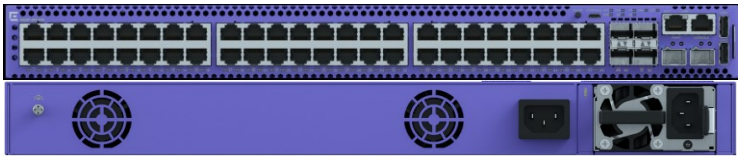
### 2.6.3. Extreme Networks - 5420F-48P-4XE_CP

Lo switch Extreme Networks 5420F-16MW-32P-4XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

Lo switch Extreme Networks 5420F-48P-4XE è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 208 Gbps di capacità di switching;
- 48 porte 10/100/1000BASE-T full/half duplex ports;
- 4 porte di uplink 1/10Gb Uplink SFP+ 10Gb;
- 2 porte di uplink/stacking SFPDD 10G/20G;
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 80Gb;
- Supporto PoE da 30W (IEEE 802.3at): lo switch supporta la tecnologia Power over Ethernet (PoE) con una potenza massima di 30 watt, conforme allo standard IEEE 802.3at su tutte le porte. Supporto del PoE fast (le periferiche PoE connesse vengono immediatamente alimentate appena lo switch è acceso) e perpetuo (le periferiche PoE connesse non si spengono in caso di riavvio dello switch);

- 740watt PoE budget;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Supporto dei protocolli Fabric (sia Fabric Connect che Extreme IP Fabric) per la realizzazione di reti in tecnologia Fabric/SDN;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- Adatto ad armadi poco profondi (330 mm);
- MACsec sulle porte di accesso e uplink per garantire una crittografia sicura del collegamento;
- Supporto Routing avanzato BGP, OSPF, ISIS;
- Supporto protocolli VXLAN EVPN – IP Fabric;
- Supporto protocolli SPBm – Fabric Connect;
- Supporto protocolli ad anello G.8032 e EAPS;
- Lo switch può essere gestito e configurato dalla CLI, via interfaccia Web, su piattaforma Cloud ExtremeCloudIQ o da piattaforma di gestione locale;
- Secondo alimentatore hot swappable opzionale.



*Extreme Networks 5420F-48P-4XE*

Scheda Tecnica Extreme Networks 5420

### 2.6.4. Juniper - EX4100-48P-C

Lo switch ethernet EX4100-48P è un apparato ad alte prestazioni per infrastrutture LAN campus e branch che supportano servizi avanzati. Supporta IEEE 802.3af Power over Ethernet e 802.3at PoE+ fino a 30W per porta.

Gli EX4100 sono “cloud-ready” e supportano l’installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4100 tra loro.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo *Enhanced Limited Lifetime*; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia *Limited Lifetime* prevede la possibilita' per l'end user di accedere a tutti gli upgade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

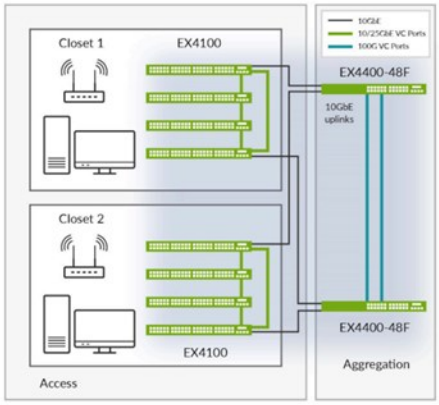
https://support.juniper.net/support/pdf/warranty/990240.pdf

**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 48 x 1GbE - 4x10GbE uplinks, 4x25GbE stacking/uplink |
| Power | PSU ridondata – PoE/PoE+ fino a 30W per porta |
| Switch capacity | 376 Gbps (bidirectional) |
| Fabric | Virtual Chassis fino a 10 switch |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4100 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.




**MACsec**

Gli switch EX4100 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

***QoS con 12 code di priorità***

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

### 2.6.5. Huawei - S5731-H48P4XC-C

Il modello Ethernet Switch S5731-H48P4XC fa parte della series S5731-H. È uno switch Full Layer 3 con supporto di IP routing avanzato (statico, RIP e OSPF, IS-IS, BGP4+), ECMP, di protocolli di affidabilità (VRRP) e migliori specifiche tecniche per essere dispiegato come switch di Aggregazione in un Campus o, grazie a funzionalità avanzate di MPLS anche in contesti metropolitani per realizzare infrastrutture uniche per più VPN. Inoltre, il supporto del VxLAN e del protocollo di control-plane BGP EVPN lo rende adatto anche come elemento di Edge per la soluzione CloudCampus di Huawei o per trasportare VLAN tra un sito all'altro connesso attraverso una rete di livello 3.

Installabile a rack 19" e profondo 42 cm, equipaggia 48 porte 10/100/1000 PoE++ Ethernet su rame e 4 porte 10GE (autosensing @1GE) ottico su SFP+. In dotazione è fornito un modulo di espansione alloggiato posteriormente che permette di alloggiare ulteriori 2 porte 40GE QSFP+ in rame utilizzabili per Stack o traffico. In termini di alimentazione, è dotato e fornito con un un alimentatore 1000W estraibile in AC che può essere ridondato nell'opportuno slot sul retro dell'apparato.

*CloudEngineS5731-H48P4XC e S7X08000*

La famiglia S5731-H fornisce la funzionalità di WLAN AC Controller integrate (già licenziato per gestire 16 AP) che permette di gestire fino a 1024 AP ed evitando di utilizzare un appliance WLAN AC dedicato esterno, funzionalità particolarmente utile in realtà aziendali piccole/medie. Gestisce una capacità di switching per la componente Wireless fino a 543 Gbit/s e permette di gestire in maniera unificata l'autenticazione (supporta 802.1x, MAC e Portal) degli utenti wired e wireless semplificando la user experience di accesso dei terminali.

E' gestibile (configurazione, monitoraggio e allaramistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller della soluzione CloudCampus.

## 2.7. Switch Tipo 7

### 2.7.1. Cisco - C9300-24SC

La serie Catalyst 9300 è la nuova generazione di switch stackable più diffusa del settore, premiata dalla prestigiosa rivista tecnica CRN come "Overall Network Product of the Year" nel 2018. Concepita per offrire performance, sicurezza, scalabilità e flessibilità, costituisce inoltre l'elemento fondante dell'architettura Cisco Software-Defined Access (SD-Access).

Gli switch Catalyst 9300 sono basati sull'architettura Cisco Unified Access ™ Data Plane 2.0 (UADP) 2.0, che non solo protegge il vostro investimento, ma consente anche una scalabilità più ampia e un throughput più elevato. Un sistema operativo moderno, Cisco IOS® XE ampiamente programmabile

offre funzionalità di sicurezza avanzate e convergenza adeguate alle esigenze del mondo Internet of Things (IoT). Sono inoltre pronti a supportare il futuro: con un'architettura CPU x86 e più memoria, consentono di ospitare container ed eseguire applicazioni e script di terze parti in modo nativo all'interno dello switch.

I Cisco Catalyst 9300 supportano funzionalità Layer 2 e Layer 3 (Routed Access RIP, EIGRP Stub, OSPF - 1000 routes, PBR, PIM Stub Multicast 1000 routes, PVLAN, VRRP, PBR, CDP, FHS, CoPP, SXP, IP SLA Responder), a cui aggiungono ulteriori funzioni avanzate di sicurezza (Cisco Trust Anchor, Encrypted Traffic Analytics, MACSEC IEEE 802.1AE, 802.1X), scalabilità (StackWise-480 con stacking a 480Gbps), alta affidabilità (cross-stack etherchannel, NSF/SSO, port autorecovery), qualità del servizio (CoS, DSCP, CIR, SRR), visibilità (NBAR, NetFlow).

L'offerta in Convenzione prevede un modello con 24 porte 1G SFP e un modulo di uplink con 8 porte 1/10G-X. Supporta inoltre funzionalità di routing dinamico Layer 3 (BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM-BIDIR, IP SLA, OSPF).

Per maggiori informazioni, riferirsi al data sheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

### 2.7.2. Aruba - R8S92AC

Gli HPE Aruba Networking CX 6300M, appartenenti alla tipologia 7 in convenzione Reti Locali 8, sono switch Layer 3 Ethernet in grado di supportare diversi servizi layer 2 e layer 3 avanzati, offrendo alle Amministrazioni 24 porte Ethernet modulabili a 1-Gbps o 10-Gbps mediante appositi transceiver, più quattro porte 10/25/50 Gigabit Ethernet (GbE) SFP+ Lo chassis offre la possibilità di utilizzare moduli di

alimentazioni ridondati. Consentono il forwarding IPv4 e IPv6 e supportano i principali protocolli di routing dinamico quali RIPv2, RIPng, OSPF e BGP, ma anche supporto di costrutti di virtualizzazione avanzata quali EVPN e VXLAN per offrire una elevata scalabilità. Questo modello implementa il supporto MACSec per la cifratura del traffico switch-to-switch e switch-to-host.

*HPE Aruba Networking CX 6300M 24G SFP+ 2SFP56*

La serie HPE Aruba Networking CX 6300M è basato su una architettura ASIC Aruba di 7° generazione ed offre un accesso da 1/10GbE e può essere utilizzata nel perimetro di aggregazione del network o per collegare i cluster dei server nei data center in una implementazione di tipo ToR of Rack (ToR).

Il sistema operativo Aruba AOS-CX, basato su microservizi, garantisce stabilità e resilienza del sistema stesso, consentendo l'integrazione dei servizi e mettendo a disposizione dell'utente finale funzionalità di programmabilità via REST-API, ma anche una migliore visibilità delle informazioni di stato della rete.

La tecnologia di clustering Aruba Virtual Stacking Framework (VSF) permette la configurazione di un virtual chassis di dimensione massima di 10 apparati attraverso le porte uplink che supportano fino a 50-GbE presenti su questo modello di switch, consentendo una rapida scalabilità a supporto delle esigenze delle Amministrazioni. I modelli 6300M possono essere dotati di alimentazione ridondata di tipo N+1 con alimentatori doppi hot-swap.

- Caratteristiche Generali:
    - Supporto 24 porte IEEE 802.3 (1 GbE/10 GbE) con 4 uplink 1-GbE/10-GbE/25-GbE/50-GbE;
    - Auto-MDIX: adeguamento automatico per cavi dritti o crossover su tutte le porte 100/1000Mbps;
    - Configurazione Jumbo Frames per la gestione di frame di grandezza massima fino a 9198 Bytes;
    - Il supporto PoE standard IEEE 802.3at e 802.3af fornisce fino a 30 W sulle single porte per alimentazione di dispositivi locali;

- Funzionalità di aggregazione dei link IEEE 802.3ad basata su protocollo LACP supportando fino a 32 interfacce aggregate con un massimo di 8 porte per interfaccia aggregata;
- Individuazione dei link unidirezionali Uni-directional Link Detection (UDLD) consentendo di disattivare una porta qualora venga individuato traffico unidirezionale su un collegamento e prevenendo loop all'interno di una topologia Layer 2 con protocollo Spanning-Tree attivo;
- Meccanismi di protezione contro packet storm broadcast, unknown unicast e multicast mediante la configurazione di soglie definite dall'utente;
- Gli switch Aruba 6300M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 3 è disponibile il Power Supply Aruba X371 12VDC 250W AC. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum;
- Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività;

- Funzionalità Layer 2:
  - Segmentazione Vlan e Vlan tagging IEEE 802.1Q fino a 4094 Vlan ID;
  - Spanning Tree Protocol per la prevenzione dei loop di rete a protezione delle topologie Layer 2, supporto IEEE 802.1d standard Spanning-Tree Protocol, IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) e IEE 802.1w Rapid Spanning-Tree Protocol (RSTP);
  - Port Mirroring per la duplicazione del traffico in ingresso e uscita da una porta verso una porta di monitoring;
  - Protocollo di tunneling VXLAN per l'implementazione di reti virtualizzate che consentono una maggiore scalabilità;
  - Internet Group Management Protocol (IGMP) per la gestione e l'inoltro del traffico Multicast all'interno di una topologia Layer 2;
  - Supporto per l'inoltro del traffico PIM-SM/IGMP snooping IPv4 Multicast all'interno dei tunnel VXLAN;
  - Supporto per l'inoltro del traffico IPv6 all'interno dei tunnel VXLAN;

  - Il meccanismo per la soppressione del traffico VXLAN ARP/ND consente di minimizzare il traffico ARP e ND all'interno dei segmenti VXLAN con conseguente ottimizzazione del traffico di rete VXLAN;
  - L'incapsulamento QinQ consente di migliorare l'utilizzo delle Vlan mediante l'aggiunta di tag IEEE 802.1Q alla frame ethernet;

- Servizi Layer 3:
  - Supporto IPv4 e IPv6 con possibilità di implementare dual-stack per consentire l'implementazione di entrambi i protocolli e facilitare la transizione da reti IPv4 a reti solo IPv6;
  - Address Resolution Protocol (ARP) per la risoluzione dei MAC address appartenenti ad un indirizzo IP presenti all'interno di una sottorete;
  - Protocolli di routing dinamici RIPv2, RIPng, OSPF e BGP per la gestione dinamiche del routing delle reti;
  - Supporto Multi-protocol BGP (MP-BGP) a supporto della segnalazione dei prefissi IPv6 e per la realizzazione piano di controllo su Ethernet VPN (EVPN);
  - Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
  - Access Control List (ACL) consentono di filtrare il traffico IP prevenendo accessi non autorizzati o implementare un controllo del traffico consentendo o bloccando l'inoltro dei pacchetti;
  - Il Bidirectional Forwarding Detection (BFD) consente di monitorare la connettività sui collegamenti fisici e logici e ridurre i tempi di convergenza del routing statico, dinamico e VRRP;
  - Il Dynamic Host Configuration Protocol (DHCP) semplifica la gestione di reti IP di large dimensioni, supportando l'indirizzamento dinamico dei client;
  - Le sub-interface consentono, tramite la configurazione di interfacce virtuali, di suddividere le interfacce fisiche in multiple interfacce logiche con tag 802.1Q ed utilizzare differenti Vlan-ID, utilizzabili in differenti scenari come VRF-lite o inter-vlan routing (router on a stick);

- Servizi di Sicurezza:

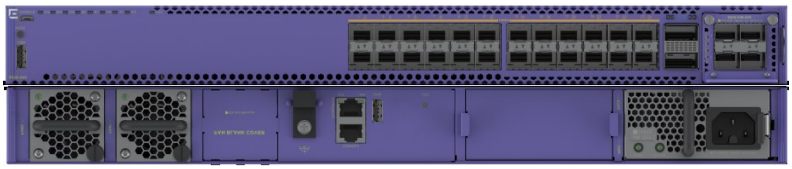
  - Servizi RADIUS e TACACS+ consentono di implementare strumenti di autenticazione per accesso ai dispositivi ed implementare controlli di accesso alla rete attraverso implementazione di meccanismi di autenticazione dei client;
  - Supporto per l'autenticazione IEEE 8092.1x e autenticazione centralizzata dei degli indirizzi MAC che controlla i permessi di accesso degli utenti alla rete secondo indirizzamento MAC e porte dello switch;
  - Management sicuro mediante implementazione di accesso CLI, GUI o MIB mediante protocolli SSHv2, HTTPS e SNMPv3;
  - Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP;
  - Il protocollo MACSec IEEE 802.1AE consente l'implementazione di autenticazione e cifratura del traffico sia sui link switch-to-switch (uplink) che i link switch-to-host (downlink);
- Gestione e configurazione:
  - Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI) e Web network management per facilitare la gestione del sistema;
  - Accesso sicuro al dispositivo attraverso linea di comando (CLI) o web GUI attraverso l'implementazione di protocolli sicuri SSHv2 e HTTPS;
  - Le Policy di segmentazione dinamica (Aruba Dynamic Segmentation) consentono di configurare i parametri di accesso alla rete automaticamente e consistenti su tutta l'infrastruttura per i client wired e wireless;
  - L'integrazione con Aruba Clearpass consente di riconoscere il client wired all'accesso e operare una configurazione ad-hoc della porta a cui il client è attestato, eliminando la necessità di configurare manualmente la porta per ogni client;
  - Interfaccia REST-API per la programmazione e l'automazione dei task configurativi;
- Quality of Services (QoS):
  - Gestione dei meccanismi di anti-congestione e prioritizzazione del traffico attraverso impostazione della Class of Services (CoS) mediante tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo Layer 3, port number TCP/UDP e DiffServ;

  - Meccanismi di accodamento Strict Priority (SP) e Deficit Weighted Round Robin (DWRR) e prioritizzazione del traffico per classificazione in tempo reale;
  - Tecnologia LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza la banda per le tipologie di traffico time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce;
  - Virtual Output Queing (VOQ) consente di isolare le congestioni, prevendendo situazioni di head of line blocking a garanzia dell'inoltro del traffico in uscita dalle porte dello switch;
- Specifiche Tecniche:
  - 24 porte SFP+ 1/10 Gbps con supporto MACSec;
  - 2 porte SFP+ 10/25/50 Gbps;
  - 2 porte SFP+ 10/25/50 Gbps con supporto MACSec;
  - Capacità di stacking fino a 10 elementi della serie Aruba CX 63xx;
  - Capacità di switching 880 Gbps;
  - Supporta fino a 32768 indirizzi MAC;
  - Supporta fino a 61000 prefissi IPv4 unicast e 61000 prefissi IPv6 unicast;
  - Latenza media 4,24 microsecondi 1 Gbps, 1,5 microsecondi 10 Gbps, 2,9 microsecondi 25 Gbps e 3,49 microsecondi 50 Gbps (con pacchetti di 64 Byte);
  - Assorbimento 131W con il 100% del traffico;
  - Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
  - Umidità operativa da 5% a 95% a 40°C, di stoccaggio da 5% a 95% a 65°C;
  - Occupazione spazio rack: 1 Rack Unit (RU);
  - Dimensioni: 44,2cm (L) x 38,5 (P) x 4,4 (A);
  - Peso 4,85 Kg.

### 2.7.3. Extreme Networks - 5520-24X_CP

Lo switch Extreme Networks 5520-24X è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 1080 Gbps di capacità di switching;
- 28 porte SFP+ 10G di cui 24 porte 100/1000/10000 SFP+ e 4 porte 1000/10000 SFP+;
- 2 porte uplink/stacking 50G QSFP28;
- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 200Gb;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Supporto dei protocolli Fabric (sia Fabric Connect che Extreme IP Fabric) per la realizzazione di reti in tecnologia Fabric/SDN;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- MACsec sulle porte uplink 10G per garantire una crittografia sicura del collegamento;
- Supporto Routing avanzato BGP, OSPF, ISIS;
- Supporto protocolli VXLAN EVPN – IP Fabric;
- Supporto protocolli SPBm – Fabric Connect;
- Supporto protocolli ad anello G.8032 e EAPS;
- Supporto protocolli MPLS (VPLS e L3VPN) incluso (non sono necessarie licenze aggiuntive);
- Supporto protocollo PTP 1588v2 incluso;
- Lo switch può essere gestito e configurato dalla CLI, via interfaccia Web, su piattaforma Cloud ExtremeCloudIQ o da piattaforma di gestione locale;
- Dotato di alimentatore hot swappable;
- Secondo alimentatore hot swappable opzionale.



*Extreme Networks 5520-24X*

Scheda Tecnica Extreme Networks 5520

### 2.7.4. Juniper - EX4400-48F-C

Lo switch ethernet EX4400-48F è un apparato ad alte prestazioni per infrastrutture LAN campus e branch che supportano servizi avanzati. Il sistema operativo dello switch, Junos OS, supporta funzionalità di switching L2 e L3, routing e servizi di security e, grazie alla sua architettura modulare, l'interruzione di un singolo processo non impatta il complessivo funzionamento dello switch. Anche le caratteristiche hardware garantiscono l'alta affidabilità, grazie ad alimentatori e ventole ridondate e hot-swappable.

Gli EX4400 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4400 tra loro come se fossero in singolo apparato logico.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo Enhanced Limited Lifetime; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia Limited Lifetime prevede la possibilità per l'end user di accedere a tutti gli upgade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

https://support.juniper.net/support/pdf/warranty/990240.pdf

**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 12 x 10 GbE SFP+ e 36 x 1GbE SFP porte di accesso in fibra |
| Power | PSU ridondata e hot-swappable |
| Switch capacity | 912 Gbps |
| Fabric | Virtual Chassis fino a 10 switch |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4400 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

**MACsec**

Gli switch EX4400 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

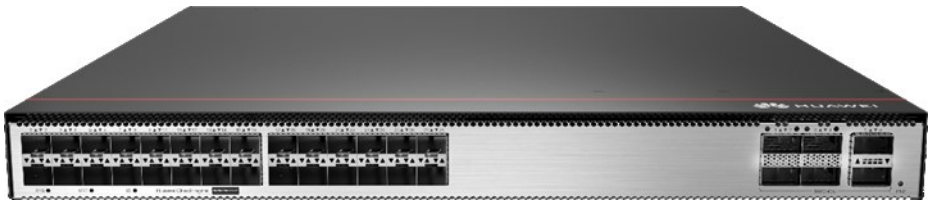
***QoS con 12 code di priorità***

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

### 2.7.5. Huawei - S6730-H28X6CZ-V2-C

Il modello Ethernet Switch CloudEngine S6730-H28X6CZ-V2 fa parte della series S6730-H-V2. E' uno switch Full Layer 3 con supporto di IP routing avanzato (statico, RIP e OSPF, IS-IS, BGP4+), ECMP, di protocolli di affidabilità (VRRP) e migliori specifiche tecniche per essere dispiegato come switch di Aggregazione in un Campus o, grazie a funzionalità avanzate di MPLS anche in contesti metropolitani per realizzare infrastrutture uniche per più VPN. Inoltre, il supporto del VxLAN e del protocollo di control-plane BGP EVPN lo rende adatto anche come elemento di Edge per la soluzione CloudCampus di Huawei o per trasportare VLAN tra un sito all'altro connesso attraverso una rete di livello 3. Installabile a rack 19" e profondo 42 cm, equipaggia 28 x 10 Gig SFP+, ottico su SFP+. Inoltre, in uplink sono previsti 6x40/100 Gig QSFP28 porte.

Ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e che consente di raggiungere un throughput di 1.76Tbps.



*CloudEngine S6730-H28X6CZ-V2*

E' gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 9) incluso all'interno della convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller della soluzione CloudCampus.

## 2.8. Switch Tipo 8

### 2.8.1. Cisco - C9500-48Y4CC

Gli switch Cisco® Catalyst® serie 9500 sono la nuova generazione di switch a livello di aggregazione e core di classe enterprise, che supportano la piena programmabilità e facilità di manutenzione. Basata su una CPU x86, la serie Cisco Catalyst 9500 è la piattaforma di switching aziendale di aggregazione e core fissa sviluppata appositamente da Cisco, creata per la sicurezza, IoT e cloud. Gli switch sono dotati di 4 core x86, CPU da 2,4 GHz, memoria DDR4 da 16 GB e memoria interna da 16 GB.

Gli switch Catalyst 9500 supportano servizi di infrastruttura e routing avanzati (come Multiprotocol Label Switching [MPLS] Layer 2 e Layer 3 VPN, Multicast VPN [MVPN] e Network Address Translation [NAT]); Funzionalità Cisco Software-Defined Access (come un database di tracciamento host, connettività tra domini e Routing e inoltro VPN [VRF] -aware Locator / ID Separation Protocol [LISP]). Lo switch supporta inoltre Cisco StackWise Virtual, una tecnologia di stacking avanzata che supporta stacking senza necessità di connettere fisicamente gli elementi tra loro: uno "stack virtuale" comprende due apparati.

L'offerta in Convenzione prevede un modello Cisco Catalyst 9500 offerto, adatto a funzioni di aggregazione e core compatto, che presenta 48 porte 1/10/25G SFP/SFP+/SFP28 e 4 porte di uplink a 40/100G QSFP+.

Per maggiori informazioni, riferirsi al data sheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html

### 2.8.2. Aruba - JL704CC

Gli switch HPE Aruba Networking CX 8360v2, appartenenti alla tipologia 8 in convenzione Reti Locali 8, sono dispositivi Layer 3 Ethernet in grado di operare a velocità wire su tutte le porte per implementazioni come Top of Rack switch (ToR) all'interno di infrastrutture di grandi dimensioni dove sono richieste basse latenze ed elevate velocità. Lo switch è in grado di supportare diversi servizi layer 2 e layer 3 avanzati, offrendo alle Amministrazioni 48 porte Ethernet modulabili a 1-GbE, 10-GbE o 25-GbE mediante appositi transceiver, più sei porte porte 40/100 Gigabit Ethernet (GbE) con moduli transceiver QFSP/QSFP28. Lo chassis offre la possibilità di utilizzare moduli di alimentazioni ridondati. Consentono il forwarding IPv4 e IPv6 e supportano i principali protocolli di routing dinamico quali RIPv2, RIPng, OSPF e BGP, ma anche supporto di costrutti di virtualizzazione avanzata quali EVPN e VXLAN per offrire una elevata scalabilità.

*HPE Aruba Networking CX 8360v2 48G SFP+ 6 40/100G QSFP*

La serie HPE Aruba Networking CX 8360v2 può essere utilizzata nel perimetro di aggregazione dei data center come Spine o come nodo Leaf di accesso per collegare i cluster dei server nei data center in una implementazione di tipo ToR of Rack (ToR).

Il sistema operativo Aruba AOS-CX, basato su microservizi, garantisce stabilità e resilienza del sistema stesso, consentendo l'integrazione dei servizi e mettendo a disposizione dell'utente finale funzionalità di programmabilità via REST-API, ma anche una migliore visibilità delle informazioni di stato della rete attraverso funzionalità di telemetria offerte dal motore di analisi Network Analytics Engine (NAE).

La tecnologia Aruba Virtual Stacking Extension (VSX) permette la realizzazione di collegamenti di tipo Multichassis Link Aggregation (MC-LAG) garantendo l'alta affidabilità dei collegamenti attraverso una interconnessione tra i 2 chassis mediante un inter-switch link, mantenendo il controllo indipendente di ogni chassis. I modelli CX 8360v2 possono essere dotati di alimentazione ridondata di tipo N+1 mediante doppia alimentazione hot-swap.

- Caratteristiche Generali:
    - Supporto 48 porte 1 GbE/10 GbE/25 GbE con 6 uplink 40-GbE/100-GbE;
    - Elevato throughput di switching fino a 4,8 Tbps full duplex con supporto wire-speed su tutte le porte;
    - Configurazione Jumbo Frames per la gestione di frame di grandezza massima fino a 9000 Bytes;
    - Funzionalità di aggregazione dei link IEEE 802.3ad basata su protocollo LACP supportando fino a 54 interfacce aggregate con un massimo di 16 porte per interfaccia aggregata (32 per coppia VSX);
    - Individuazione dei link unidirezionali Uni-directional Link Detection (UDLD) consentendo di disattivare una porta qualora venga individuato traffico unidirezionale su un

collegamento e prevenendo loop all'interno di una topologia Layer 2 con protocollo Spanning-Tree attivo;

- Meccanismi di protezione contro packet storm broadcast, unknown unicast e multicast mediante la configurazione di soglie definite dall'utente;
- Gli switch Aruba 8360v2 vengono forniti con modulo di alimentazione ridondato a garanzia di una maggiore alta affidabilità.

- Funzionalità Layer 2:
  - Segmentazione Vlan e Vlan tagging IEEE 802.1Q fino a 4094 Vlan ID;
  - Spanning Tree Protocol per la prevenzione dei loop di rete a protezione delle topologie Layer 2, supporto IEEE 802.1d standard Spanning-Tree Protocol, IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) e IEE 802.1w Rapid Spanning-Tree Protocol (RSTP);
  - Port Mirroring per la duplicazione del traffico in ingresso e uscita da una porta verso una porta di monitoring;
  - Internet Group Management Protocol (IGMP) per la gestione e l'inoltro del traffico Multicast all'interno di una topologia Layer 2;
  - Protocollo di tunneling VXLAN per l'implementazione di reti virtualizzate che consentono una maggiore scalabilità;
  - Segmentazione avanzata attraverso l'implementazione di tunnel VXLAN su architetture data center di tipo Spine/Leaf o infrastrutture campus con gateway Layer 3 centralizzato e Symmetric Integrated Routing and Bridging (IRB) basato su gateway VXLAN distribuiti;
  - Supporto per l'inoltro del traffico PIM-SM/IGMP snooping IPv4 Multicast all'interno dei tunnel VXLAN;
  - Supporto per l'inoltro del traffico IPv6 all'interno dei tunnel VXLAN;
  - Il meccanismo per la soppressione del traffico VXLAN ARP/ND consente di minimizzare il traffico ARP e ND all'interno dei segmenti VXLAN con conseguente ottimizzazione del traffico di rete VXLAN;
  - L'incapsulamento QinQ consente di migliorare l'utilizzo delle Vlan mediante l'aggiunta di tag IEEE 802.1Q alla frame ethernet;
- Servizi Layer 3:
  - Supporto IPv4 e IPv6 con possibilità di implementare dual-stack per consentire l'implementazione di entrambi i protocolli e facilitare la transizione dareti IPv4 a reti solo IPv6;

- Address Resolution Protocol (ARP) per la risoluzione dei MAC address appartenenti ad un indirizzo IP presenti all'interno di una sottorete;
- Protocolli di routing dinamici RIPv2, RIPng, OSPF e BGP per la gestione dinamiche del routing delle reti;
- Supporto Multi-protocol BGP (MP-BGP) a supporto della segnalazione dei prefissi IPv6 e per la realizzazione piano di controllo su Ethernet VPN (EVPN);
- Gestione dei meccanismi di alta affidabilità Layer 3 attraverso l'implementazione di First Hop Redundancy Protocol quale Virtual Router Redundancy Protocol (VRRP);
- Access Control List (ACL) consentono di filtrare il traffico IP prevenendo accessi non autorizzati o implementare un controllo del traffico consentendo o bloccando l'inoltro dei pacchetti;
- Il Bidirectional Forwarding Detection (BFD) consente di monitorare la connettività sui collegamenti fisici e logici e ridurre i tempi di convergenza del routing statico, dinamico e VRRP;
- Il Dynamic Host Configuration Protocol (DHCP) semplifica la gestione di reti IP di large dimensioni, supportando l'indirizzamento dinamico dei client sia in IPv4 che IPv6;
- Il tunneling 6in4 consente di configurare un trasporto del traffico IPv6 all'interno di una rete IPv4;
- Possibilità di ottimizzare i percorsi di traffico attraverso collegamenti Equal-Cost Multipath (ECMP) in grado di ottimizzare l'utilizzo della banda, nonché migliorare l'affidabilità dei percorsi;
- Le sub-interface consentono, tramite la configurazione di interfacce virtuali, di suddividere le interfacce fisiche in multiple interfacce logiche con tag 802.1Q ed utilizzare differenti Vlan-ID, utilizzabili in differenti scenari come VRF-lite o inter-vlan routing (router on a stick);
- Il Policy Based Routing consente la configurazione di politiche di inoltro dei pacchetti IP ad-hoc secondo definizione dell'amministratore di rete;

- Servizi di Sicurezza:
  - Gli switch HPE Aruba Networking serie 8360v2 con sistema operativo AOS-CX sono prodotti conformi allo standard TAA ed utilizzano cifratura FIPS 140-2 per la protezione dei dati sensibili;

  - Servizi RADIUS e TACACS+ consentono di implementare strumenti di autenticazione per accesso ai dispositivi ed implementare controlli di accesso alla rete attraverso implementazione di meccanismi di autenticazione dei client;
  - Supporto per l'autenticazione IEEE 8092.1x e autenticazione centralizzata dei degli indirizzi MAC che controlla i permessi di accesso degli utenti alla rete secondo indirizzamento MAC e porte dello switch;
  - Management sicuro mediante implementazione di accesso CLI, GUI o MIB mediante protocolli SSHv2, HTTPS e SNMPv3;
  - Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP;
  - Il protocollo MACSec IEEE 802.1AE consente l'implementazione di autenticazione e cifratura del traffico su 2 link 40/100 GbE per collegamento switch-to-switch (uplink), con supporto cifratura AES128 e AES256;
- Gestione e configurazione:
  - Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba AirWave. Supportano anche command-line interface (CLI) e Web network management per facilitare la gestione del sistema;
  - Accesso sicuro al dispositivo attraverso linea di comando (CLI) o web GUI attraverso l'implementazione di protocolli sicuri SSHv2 e HTTPS;
  - Le Policy di segmentazione dinamica (Aruba Dynamic Segmentation) consentono di configurare i parametri di accesso alla rete automaticamente e consistenti su tutta l'infrastruttura per i client wired e wireless;
  - L'integrazione con Aruba Clearpass consente di riconoscere il client wired all'accesso e operare una configurazione ad-hoc della porta a cui il client è attestato, eliminando la necessità di configurare manualmente la porta per ogni client;
  - Interfaccia REST-API per la programmazione e l'automazione dei task configurativi;
- Quality of Services (QoS):
  - Gestione dei meccanismi di anti-congestione mediante implementazione dello strict priority sulle code e del Deficit Weighted Round Robin per la prioritizzazione del traffico in tempo reale;

  - Meccanismi Data Center Bridging (DCB) per il supporto degli standard di rete quali lossless Ethernet per eliminare la perdita di pacchetti accodati in eccesso e Priority Flow Control configurabile per porta;
  - Protezione del controllo di flussi per prevenire l'accumulo di congestione ed evitare la bufferizzazione dei pacchetti per periodi di tempo eccessivi;
  - Supporto dei protocolli di storage quali iSCSI, Lossless iSCSI, RDMA over converged Ethernet versione 2 (RoCEv2) e Non-Volatile Memory Express (NVMoOF) per il controllo del traffico in lettura e scrittura verso gli storage;
- Specifiche Tecniche:
  - 44 porte SFP+/SFP28 1/10/25 Gbps (fino a 22 porte SFP56 50 Gbps);
  - 4 porte SFP+/SFP28 10/25 Gbps con supporto MACSec;
  - 4 porte QSFP+/QSPF28 40/100 Gbps;
  - 2 porte QSFP+/QSPF28 40/100 Gbps con supporto MACSec;
  - Capacità di switching 4,8 Tbps;
  - Supporta fino a 212992 indirizzi MAC e 4094 Vlan 802.1Q;
  - Supporta fino a 606997 prefissi IPv4 unicast e 630784 prefissi IPv6 unicast;
  - Assorbimento 725W;
  - Dissipazione 1459 BTU/ora;
  - Temperatura operativa 0°C a 45°C, di stoccaggio -40°C a 70°C;
  - Umidità operativa da 15% a 95% a 45°C, di stoccaggio da 15% a 95% a 65°C;
  - Occupazione spazio rack: 1 Rack Unit (RU);
  - Dimensioni: 44,2cm (L) x 40,64 (P) x 4,4 (A);
  - Peso 10,73 Kg.

Per maggiori Informazioni e per una documentazione esaustiva in merito ai prodotti e la guida utile alla configurazione, si rimanda al seguente link: Network Architetture With Aruba HPE

**Porta Aggiuntive - HPE Aruba Networking Transceiver SFP/SFP+/QSFP**

Gli switch HPE Aruba Networking proposti alle Amministrazioni in convenzione Reti Locali 8 dispongono di porte modulabili che possono variare a seconda della tipologia proposta. Si riporta di seguito una

tabella che riassume i modelli di transceiver proposti in convenzione, le caratteristiche principali del transceiver, la tipologia di media supportato, nonché la tipologia di switch dove il transceiver può essere alloggiato.

| Transceiver | Tipologia | Descrizione | Codice Prodotto | Tipologia di switch |
|---|---|---|---|---|
|  | Porta aggiuntiva 1000 Base-T | 1G SFP RJ45 T 100m Cat5e Transceiver | J8177D | **Tipo 1, 2, 3, 4, 5, 6, 7, 8** |
|  | Porta aggiuntiva 1000 Base-LX | 1G SFP LC LX 10Km SMF Transceiver | J4859D | **Tipo 1, 2, 3, 4, 5, 6, 7, 8** |
|  | Porta aggiuntiva 1000 Base-SX | 1G SFP LC SX 500m MMF Transceiver | J4858D | **Tipo 1, 2, 3, 4, 5, 6, 7, 8** |
|  | Porta aggiuntiva 10G Base-SR | 10G SFP+ LC SR 300m MMF Transceiver | J9150D | **Tipo 3, 4, 5, 6, 7, 8** |
|  | Porta aggiuntiva 10G Base-LR | 10G SFP+ LC LR 10Km SMF Transceiver | J9151E | **Tipo 3, 4, 5, 6, 7, 8** |

| | | | | |
|---|---|---|---|---|
|  | Porta aggiuntiva 10G Base-ER | 10G SFP+ LC ER 40Km SMF Transceiver | J9153D | **Tipo 3, 4, 5, 6, 7, 8** |
|  | Porta aggiuntiva 40G Base-SR | 40G QSFP+ LC BiDi 150m SMF Transceiver | JL308A | **Tipo 8** |
|  | Porta aggiuntiva 40G Base-LR | 40G QSFP+ LC LR4 10Km SMF Transceiver | JH232A | **Tipo 8** |

*Porte aggiuntive HPE Aruba Networking*

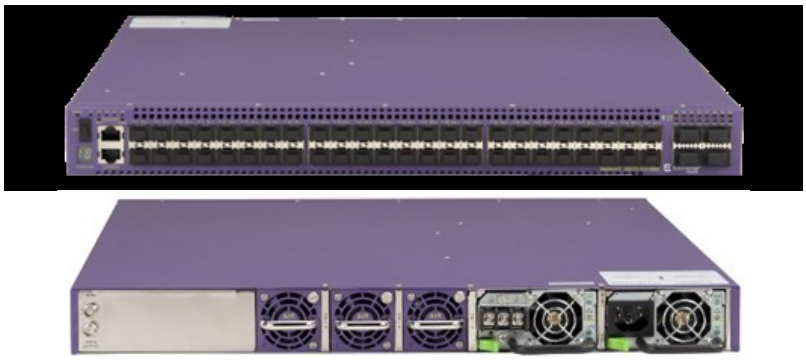
Per ulteriori esigenze di connettività, si rimanda al documento "AOS-S and AOS-CX Transceiver Guide" dove vengono riportate le informazioni sulle tipologie di transceiver supportate dagli switch HPE Aruba Networking che potranno essere acquisiti fuori convenzione, Extra Consip, secondo l'articolo 63.

### 2.8.3. Extreme Networks - 17310_C

Lo switch Extreme Networks X670G2-48x-4q è uno switch di ultima generazione che ha le seguenti caratteristiche:

- WireSpeed Design: Lo switch è progettato senza blocchi, garantendo una velocità di rete alla massima capacità del collegamento;
- 1280 Gbps di capacità di switching;
- 48 porte SFP+ 1G/10G e 4 porte 40GBase-X QSFP+;
- Le porte 40G possono essere usate per funzionalità di stacking;

- Fino a 8 Unità configurabili in modalità Stack/Virtual Chassis con capacità del bus di stacking a 320Gb;
- Supporto trasporto protocolli Audio e Video (AVB) in maniera nativa;
- Supporto dei protocolli Fabric (Extreme IP Fabric) per la realizzazione di reti in tecnologia Fabric/SDN;
- Sistema operativo basato su kernel Linux, robusto ai fenomeni di riavvio dello switch non pianificato con la possibilità di effettuare il controllo, gestione e riavvio dei singoli processi;
- Disponibilità di eseguire codice Python 3.x direttamente dalla CLI dello switch;
- MACsec sulle porte uplink 10G per garantire una crittografia sicura del collegamento;
- Supporto Routing avanzato BGP, OSPF, ISIS;
- Supporto protocolli VXLAN EVPN – IP Fabric;
- Supporto protocolli ad anello G.8032 e EAPS;
- Supporto protocolli MPLS (VPLS e L3VPN) con licenza opzionale;
- Supporto protocolli PTP 1588v2 con licenza opzionale;
- Lo switch può essere gestito e configurato dalla CLI, via interfaccia Web o da piattaforma di gestione locale;
- Dotato di alimentatore hot swappable;
- Secondo alimentatore hot swappable opzionale.



*Extreme Networks X670G2-48x-4q*

Scheda Tecnica Extreme Networks x670G2-48x

### 2.8.4. Juniper - EX4650-48Y-AFO-C

Lo switch EX4650 è un apparato compatto ad alte prestazioni adatto sia alla distribuzione/core in ambito campus che, come top-of-rack, in ambito data center. Il sistema operativo dello switch, Junos OS, supporta funzionalità di switching L2 e L3, routing e servizi di security e, grazie alla sua architettura modulare, l'interruzione di un singolo processo non impatta il complessivo funzionamento dello switch. Anche le caratteristiche hardware garantiscono l'alta affidabilità, grazie ad alimentatori e ventole ridondate e hot-swappable.

Gli EX4650 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 4 switch EX4650 tra loro come se fossero in singolo apparato logico.

**Garanzia**

La garanzia inclusa con questa classe di apparato è di tipo Enhanced Limited Lifetime; la sostituzione hardware è garantita per tutta la vita dell'apparato. L'accesso al servizio di sostituzione hardware avviene via RMA; Juniper Networks si impegna a spedire lo switch sostitutivo entro 1 Business Day dall'apertura del ticket di RMA.

Per le parti software la garanzia Limited Lifetime prevede la possibilita' per l'end user di accedere a tutti gli upgade e/o software fixes rilasciati in general availability.

Per ulteriori chiarimenti si rimanda alla documentazione presente sul portale Juniper:

https://support.juniper.net/support/pdf/warranty/990240.pdf

**Funzionalità in evidenza**

| | |
|---|---|
| Porte | 48 x 10/25 GbE SFP28/SFP+/SFP + 8 x 40/100 GbE QSFP28/QSFP+ |
| Power | PSU ridondata e hot-swappable, consumo 0.9 W/Gb |
| Switch capacity | 4 Tbps |
| Fabric | Virtual Chassis fino a 4 switch – MC-LAG |

***Virtual Chassis***

La tecnologia Virtual Chassis permette di collegare fino a 4 EX4650 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

***Campus Fabric***

Lo switch supporta fabric IP con overlay EVPN-VxLAN. La fabric può estendere la connettività tra più siti e realizzare l'estensione a livello 2 della rete (L2 stretch).

***MPLS***

EX4650, unico switch compatto nel mercato, supporta un ampio ventaglio di funzionalità MPLS, tra cui L2VPN e L3VPN, e Metro Ethernet.

### 2.8.5. Huawei - S6730-H48X6CZ-V2-C

Il modello Ethernet Switch S6730-H48X6CZ-V2 fa parte della series S6730-H-V2. È uno switch MPLS Full Layer 3 con supporto di IP routing avanzato (statico, RIP e OSPF, IS-IS, BGP4+), framework MPLS e relative

applicazioni (L2 VPN VLL/PWE3/VPLS, L3VPN, TE), funzionalità di Virtual eXtensible Local Area Network (VXLAN) L2/L3 gateways con protocollo di segnalazione BGP EVPN e configurabile via NETCONF/Yang model. È adatto quindi sia come switch di accesso server in un Data Center che apparato di aggregazione in una LAN, di raccolta in una MAN e/o di terminatore VTEP per realizzare una fabric VxLAN con cui trasportare reti di livello 2.

Installabile a rack 19", equipaggia 48 porte 10GE (autosensing @1GE) ottico su SFP+, 6 porte 40GE QSFP+ Upgradabili a 100G mediante acquisto di licenza e relativo transceiver. In aggiunta dispone di una porta seriale, una ethernet di management e di una porta USB per la gestione locale e doppia alimentazione sul retro. In dotazione è fornito un cavo di stack da 1 metro da usare sulle porte ottiche 40GE e con cui è possibile metterlo in stack.

Ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e on throughput fino a 2.4 Tbps.

E' gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 9) incluso all'interno della Convenzione e dalla piattaforma iMaster NCE-Campus, SDN Controller della soluzione CloudCampus.

*CloudEngine S6730-H48X6CZ-V2*

## 2.9. Software di gestione

### 2.9.1. Cisco – DNA Center DNAC_VM_x00

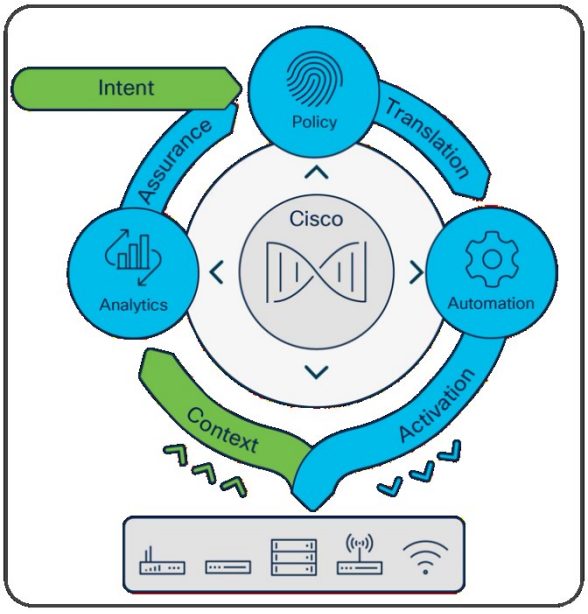
Cisco DNA Center è uno strumento aperto ed integrabile con soluzioni di terze parti che permette e facilita la gestione della rete (sia cablata che wireless). Cisco DNA Center supporta la gestione del ciclo di vita dell'intera infrastruttura di rete (cablata e wireless) da un'unica interfaccia grafica, fornendo agli amministratori di rete un'unica soluzione per il provisioning, gestione, configurazione, monitoraggio, ottimizzazione, automazione, policy-management e risoluzione di problemi. Interfacce grafiche robuste

rendono l'implementazione e le operazioni dei dispositivi semplici ed economiche. Cisco DNAC permette di tracciare e localizzare a quale dispositivo di rete (switch o AP) gli utenti sono collegati.

Cisco DNA Center sfrutta AI ed algoritmi di Machine Learning per migliorare le performance della rete e suggerire azioni di ottimizzazione o risolutive in casi di problematiche in maniera accurata ed efficace.

L'offerta in Convenzione comprende il Software DNA Center sotto forma di Virtual Machine Appliance in formato VMware (OVA). Il software in Convenzione non comprende server HW: si suggerisce di mettere a disposizione un server dedicato, equipaggiato con HW e SW secondo le specifiche consultabili al link seguente:
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/dna-center-va/esxi/2-3-7/deployment-guide/b_cisco_dna_center_virtual_appliance_esxi_deployment_guide.html#deployment-requirements

Per maggiori informazioni, riferirsi al datasheet ufficiale online: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html



### 2.9.2. Aruba – AirWave AW-AEDL-x00C

Aruba AirWave è un sistema di gestione di rete potente e di facile utilizzo, che non solo supporta solo l'infrastruttura cablata e wireless di Aruba, ma anche di una vasta gamma di altri produttori. Fornisce una visibilità granulare su dispositivi, utenti e applicazioni della rete. Con un'introspezione senza precedenti e un controllo centralizzato per gestire in modo efficace le infrastrutture aziendali globali, AirWave consente alle organizzazioni IT di ottimizzare in modo proattivo le prestazioni della rete, rafforzare la sicurezza wireless, e migliorare l'esperienza dell'utente finale.

Attraverso un'interfaccia utente centralizzata e intuitiva, AirWave fornisce monitoraggio in tempo reale, avvisi proattivi, report storici e risoluzione dei problemi rapida ed efficiente. Le visualizzazioni di pannelli dedicati consentono di visualizzare rapidamente potenziali problemi di copertura radiofrequenza (RF), traffico di comunicazioni unificate e di collaborazione (UCC), prestazioni delle applicazioni e integrità dei servizi di rete.

Il modulo Connectivity Health analizza in modo proattivo la qualità dell'esperienza degli utenti finali fornendo funzionalità di monitoraggio avanzate per servizi di rete critici, come guasti e tempo di risposta per un dispositivo mobile nell'associazione a una componente radio Wi-Fi. Altri servizi monitorati includono il tempo di autenticazione attraverso un server RADIUS, la raccolta di un indirizzo IP tramite server DHCP, e la risoluzione dei nomi per i servizi DNS. Ciò consente alle organizzazioni IT di visualizzare la visibilità end-to-end dei problemi prima che scalino, mentre le metriche vengono monitorate in tempo reale e acquisite anche tramite test opzionali a richiesta, o pianificati per analisi predittiva.

AppRF fornisce una visibilità approfondita sulle applicazioni e sul traffico Web in rete, per garantire che le app mission-critical ottengano priorità, che gli utenti non visitino siti rischiosi, o anche solo misurare i modelli di utilizzo. Un pannello UCC dedicato offre una visibilità granulare delle applicazioni di Unified Communications come Skype for Business e tutte le chiamate Wi-Fi che attraversano la rete.

La posizione e la mappatura di VisualRF offrono viste a livello di rete dell'intero ambiente RF. Le mappe della copertura Wi-Fi e la sottostante topologia cablata mostrano un'immagine chiara e precisa di chi si trova sulla rete, posizione e rendimento dei componenti. Inoltre, gli overlay dello stato dei client, e le prestazioni delle applicazioni, possono aiutare a diagnosticare rapidamente problemi specifici per un client, una planimetria, o un percorso specifico. Il rilevamento rogue AirWave RAPIDS funziona attraverso un modulo software di protezione dalle intrusioni wireless denominato RFProtect, per raccogliere dati e

mitigare i problemi con AP rogue, client non autorizzati e eventi di intrusione wireless su reti cablate e wireless. I dati wireless raccolti da RAPIDS sono correlati con i dati della rete cablata per identificare le minacce più significative e rilevanti, riducendo al contempo i falsi positivi e rafforzando la sicurezza della rete.

Disponibile come software o dispositivo hardware e software combinato, AirWave offre all'IT la possibilità di prendere decisioni intelligenti e ben informate sulla rete, riducendo al tempo stesso i costi e la complessità del miglioramento della qualità del servizio.

In convenzione sono disponibili i seguenti pacchetti di licenze, che sarà possibile acquistare in base alle proprie esigenze:

| | | |
|---|---|---|
| Software per la gestione fino a **100 nodi** | Aruba AirWave include RAPIDS, VisualRF, NetEdit (100 Nodi) | **AW-AEDL-100C** |
| Software per la gestione fino a **500 nodi** | Aruba AirWave include RAPIDS, VisualRF, NetEdit (500 Nodi) | **AW-AEDL-500C** |
| Software per la gestione fino a **1000 nodi** | Aruba AirWave include RAPIDS, VisualRF, NetEdit (1000 Nodi) | **AW-AEDL-1000C** |

*Modello licenze Aruba AirWave*

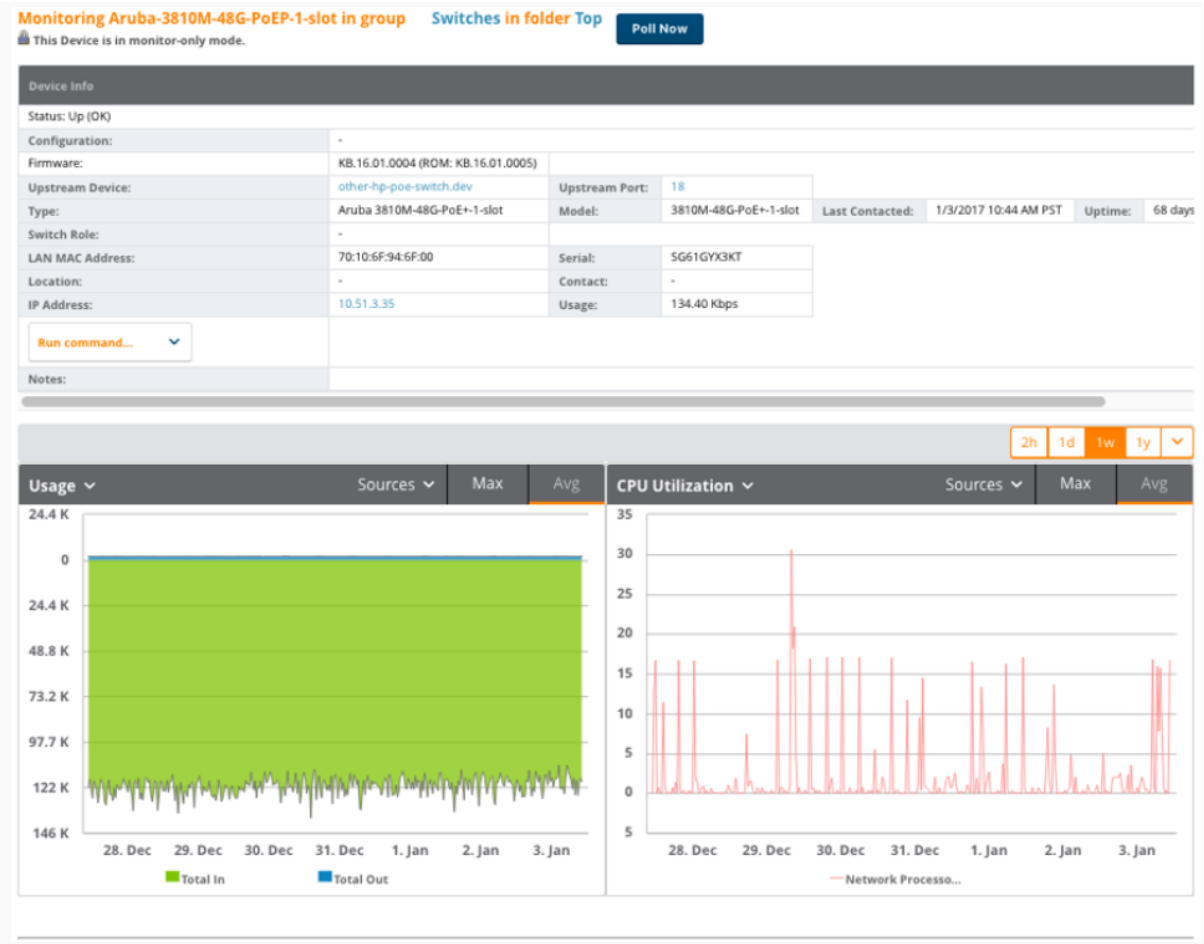
**RISOLVI I POBLEMI DI CONNETTIVITA' PRIMA CHE SI VERIFICHINO**

Con il Connectivity Health monitora proattivamente le metriche critiche non RF: il tempo necessario a un dispositivo mobile per associarsi a una radio Wi-Fi, autenticarsi su un server RADIUS, raccogliere un indirizzo IP tramite DHCP o risolvere nomi per Servizi DNS. Con avvisi personalizzati e test del cliente

simulati, Connectivity Health consente all'IT di intraprendere azioni proattive contro i problemi di prestazioni futuri.

**MONITORAGGIO E VISIBILITÀ IN TEMPO REALE**

- Visualizzare automaticamente tutti gli utenti e i dispositivi: wireless e remoti - sulla rete.
- Misurare i tempi di risposta e i tassi di errore per client, associazione con radio Wi-Fi, autenticazione con Server RADIUS, tempi di risposta DHCP, e risoluzione DNS.
- Monitorare l'infrastruttura cablata che collega il wireless controller e AP.
- Visualizza errori radio, tra cui rumore di fondo e informazioni sull'utilizzo del canale, cause frequenti di problemi di connettività.
- Analizza da livello di rete a livello di dispositivo monitoraggio delle visualizzazioni.
- Memorizza e visualizza le prestazioni, la capacità e statistiche a livello di applicazione, traffico Web e rete deviazioni per un periodo di 40 settimane.

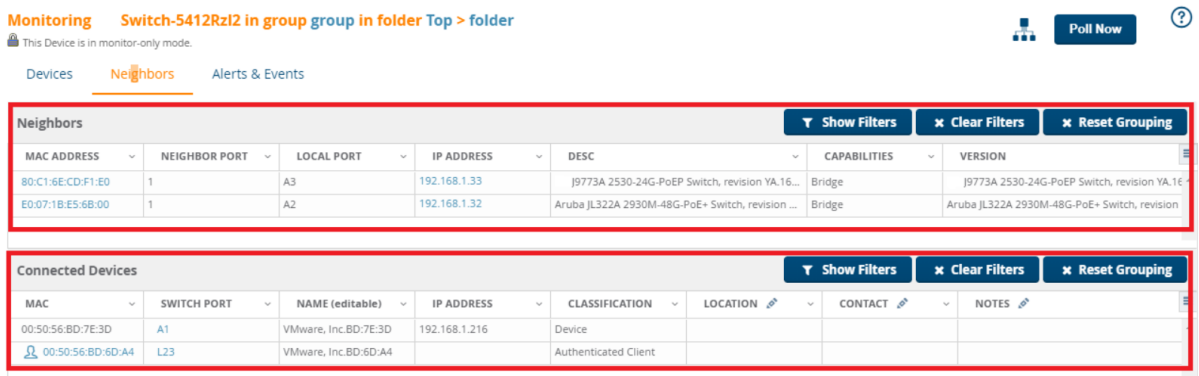



*Aruba Airware monitor device*

Gli avvisi sui dispositivi aiutano gli amministratori a tenere traccia degli eventi principali come il mancato collegamento, il riavvio dei dispositivi, il mancato funzionamento dell'alimentazione o altri eventi che possono avere un effetto significativo non solo sul dispositivo stesso ma anche sulla rete.

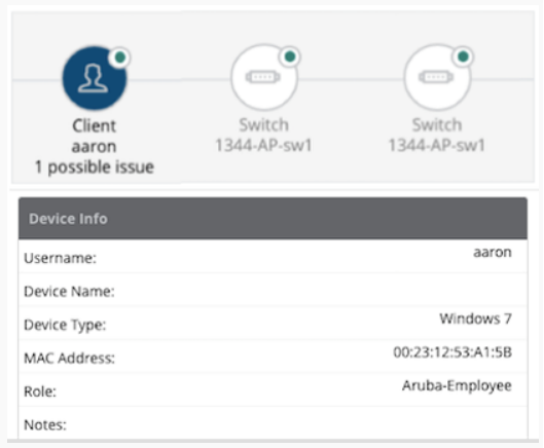
**Visibilità dei client connessi alla rete cablata**

AirWave fornisce i dati per aiutare gli amministratori di rete ad identificare gli switch adiacenti, nonché i client autenticati e non autenticati collegati a uno switch. Ciò è di grande aiuto per comprendere i peer dello switch nonché i client che dipendono da un particolare switch. La mappatura dei client collegati allo stato della porta, alla potenza consumata e alla priorità PoE è utile per identificare potenziali problemi prima che si verifichino.




*Aruba AirWave client autenticati*

Inoltre, per i client autenticati, sono disponibili dettagli come nome utente, VLAN, indirizzo IP e ruolo utente:



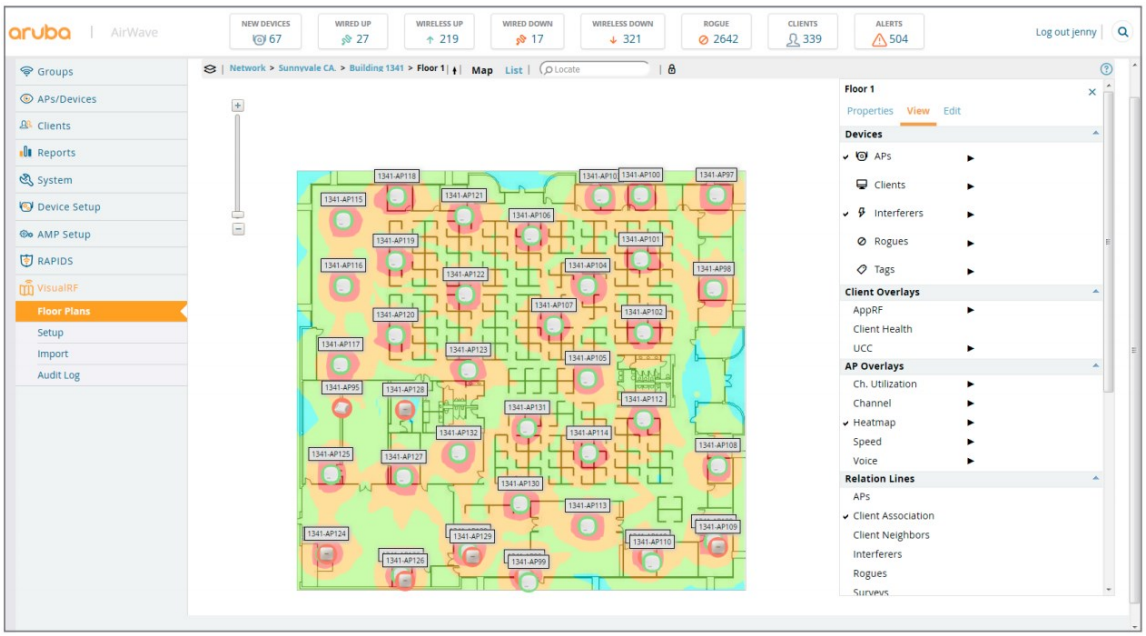

*Aruba AirWave client issue analysis*

**APPRF**

Per una visibilità approfondita delle applicazioni e del traffico web, AppRF assicura che le app mission-critical abbiano la priorità. È possibile valutare l'utilizzo complessivo delle applicazioni, e avere visibilità sugli utenti che inducono le maggiori quote di traffico. Una dashboard UCC dedicata offre una visibilità granulare per applicazioni di comunicazioni unificate come Skype per Business e tutte le chiamate Wi-Fi che attraversano la rete.

**VISUALRF**

I servizi di localizzazione e mappatura delle posizioni offrono viste dell'intero ambiente RF. Mappe di copertura Wi-Fi, e della sottostante topologia cablata, mostrano un'immagine chiara e accurata di chi è sulla rete, posizione, e comportamento generale della rete. Le sovrapposizioni configurabili mostrano lo stato e delle applicazioni dei client con relative prestazioni, per diagnosticare rapidamente problemi specifici per ogni client, per una mappa specifica, per un intero piano, o posizione specifica.

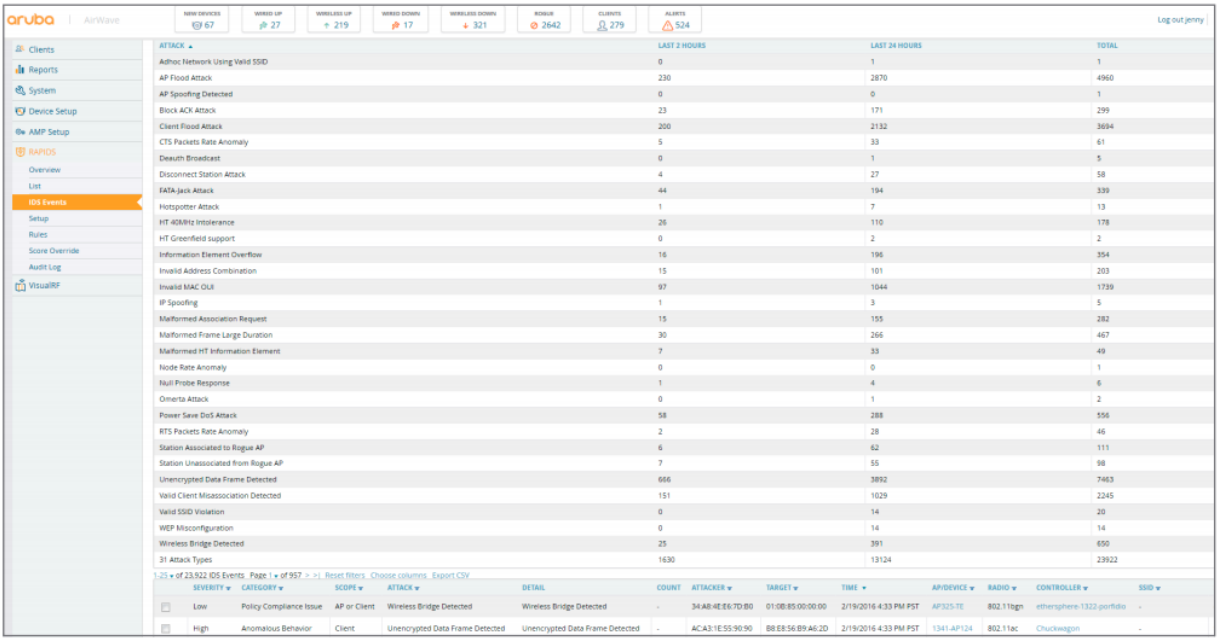



*Aruba Airware copertura area Wi-Fi*

**RAPIDS**

Il rilevamento rogue AP di AirWave funziona con il modulo Aruba RFProtect, con protezione dalle intrusioni wireless e raccolta dati per attenuare i problemi dovuti a rogue AP e client, eventi di intrusione

wireless e wired. I dati wireless raccolti sono correlati con la rete dati per identificare le minacce più significative e rilevanti, riducendo notevolmente i falsi positivi e aumentando significativamente il rafforzamento complessivo della sicurezza della rete.



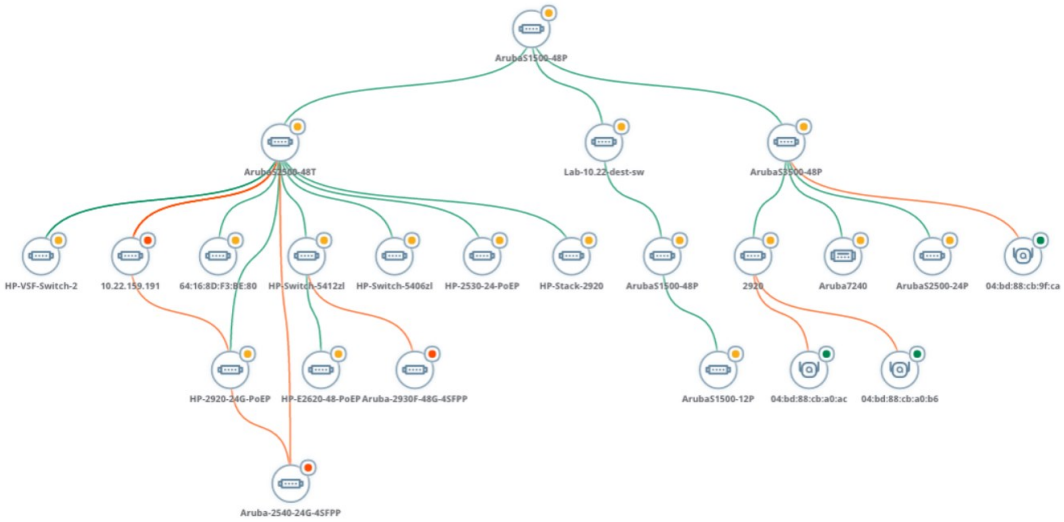

*Aruba AirWave analisi eventi*

**DISCOVERY DISPOSITIVI**

- Rileva automaticamente e mappa i dispositivi dell'intera infrastruttura, sia essa infrastruttura WLAN o Wired
- Funziona in qualsiasi ambiente di rete, inclusi quelli di grandi dimensioni e su reti distribuite multi-sito.
- Mostra la relazione tra AP, controller e switch al fine di produrre una topologia della rete

**Vista della Topologia**

AirWave rileva, identifica e crea automaticamente una topologia in tempo reale dell'intera rete; in particolare, in una rete mista wired e wireless, la piattaforma è in grado di creare una mappa dell'ambiente RF e della topologia cablata sottostante. La topologia può anche includere dispositivi di altri fornitori, purché gli altri dispositivi utilizzino un protocollo basato su standard come LLDP per annunciarsi.



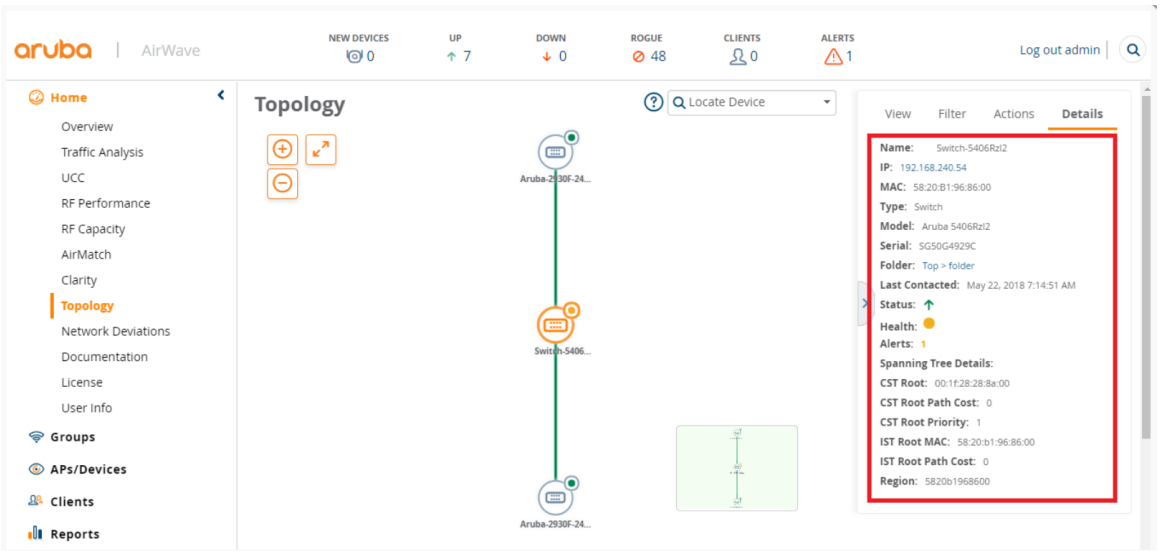

*Aruba AirWave vista topologica*

La topologia mostra:

- la connettività L2;
- l'integrità dei dispositivi;
- i collegamenti che li interconnettono e consente inoltre di individuare un dispositivo tramite il numero di modello;
- il tipo di dispositivo;
- la cartella in cui è stato configurato.

Facendo clic su di un determinato dispositivo nella topologia vengono inoltre forniti i dettagli di quel particolare dispositivo (inclusi modello, numero di serie, stato di salute, avvisi e dettagli STP).

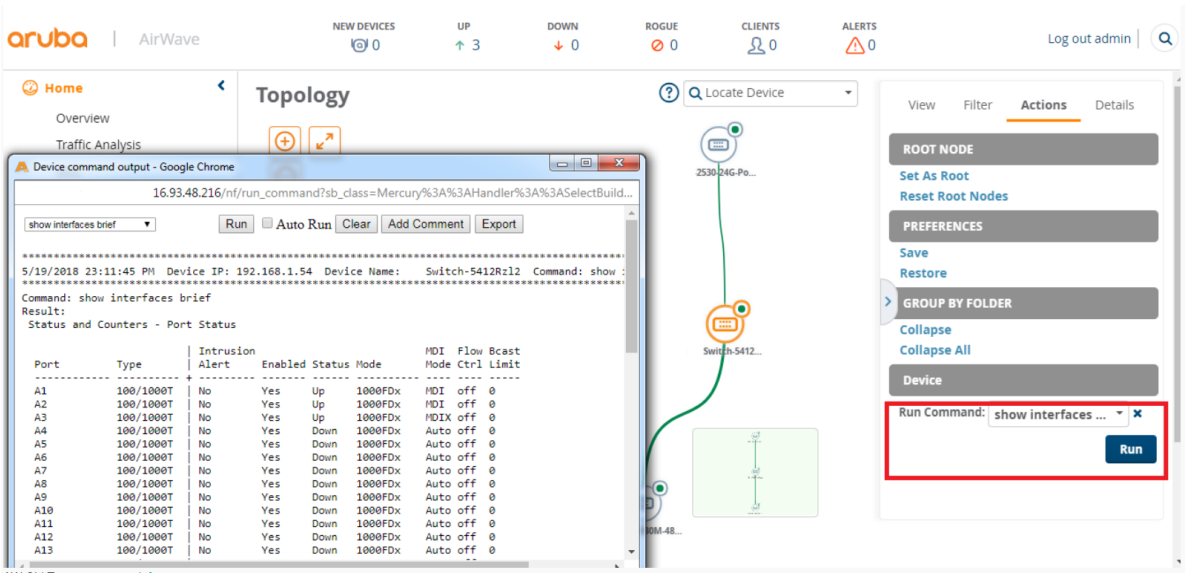
Facendo clic invece su un collegamento nella topologia vengono forniti dettagli sullo stato di salute, la velocità e il tipo di collegamento, compreso il suo stato di aggregazione (LACP).




*Aruba Airware topologia di rete*

La vista “Topologia” consente inoltre agli amministratori di cercare ed evidenziare una parte della rete per VLAN e per Spanning Tree. Questo può essere utile per restringere il campo a una particolare porzione della rete senza distrarsi, specialmente nelle reti di grandi dimensioni.

Per comodità, i comandi CLI possono essere eseguiti anche direttamente dalla vista “Topologia”. Ad esempio, l'esecuzione di "show interfaces brief" può mostrare i dettagli della porta e quindi un amministratore può comprendere meglio il motivo di un eventuale avviso.




*Aruba AirWave Browser CLI*

**RISOLUZIONE DEI PROBLEMI E DIAGNOSTICA**

- Visualizza i dati di dispositivi client ArubaOS, Instant e ClearPass Policy Manager; comprendendo incluso il tipo di dispositivo, il sistema operativo, dettagli del sistema operativo, produttore e modello.
- Ricerca di client per nome utente o indirizzo MAC, visualizzazione diagnostica delle statistiche dei dispositivi di rete, unitamente ad indicatori per valutare lo stato di salute e le prestazioni complessive.
- Sovrapposizione dello stato dei client su planimetria per diagnosticare problemi specifici per client o su un'area della mappa.
- Diagnostica facilmente problemi di radiofrequenza

**ANALISI DELLA CAUSA E CORRELAZIONE EVENTI**

- Mappa le relazioni tra gli AP controller e switch per identificare principali cause dei tempi di inattività e problemi di prestazioni;
- Correla i problemi di prestazioni e tempi di inattività in modo tale da inviare singoli avvisi di allarme.

**GESTIONE DELLE CONFIGURAZIONI**

- Configura automaticamente AP, controller, Aruba Instant, e Aruba Switches;
- Permette di definire le politiche di configurazione attraverso un'interfaccia utente web, o importando una configurazione nota da un dispositivo esistente;
- Configura gli AP Instant Aruba facilmente in ambienti multi-sito;
- Permette di eliminare dispendiosi ed inclini ad errori operazioni ed aggiornamenti manuali per mezzo di una efficiente distribuzione del software remoto;
- Supporta aggiornamenti avanzati del firmware con possibilità di scelta ed imposizione versioni certificate, con download differiti di immagini e processi di riavvio, nonché supporto per la programmazione posticipata degli aggiornamenti o delle modifiche del firmware;
- Archivia configurazioni dei dispositivi ed esegue e backup dei flash per ripristinare le statistiche e le configurazioni precedenti dei controller Aruba;
- Mantiene registri di verifica dettagliati delle modifiche apportate da tutti gli operatori di AirWave.

La modifica della configurazione è un evento importante e deve essere monitorata attentamente per correlare la modifica del comportamento della rete alla modifica della configurazione stessa. AirWave può eseguire backup periodici dei dispositivi, eseguire automaticamente controlli di configurazione e avvisare gli amministratori nel caso in cui la configurazione del dispositivo sia diversa da quella che AirWave si aspetta che sia.


*Aruba AirWave backup configurazioni*

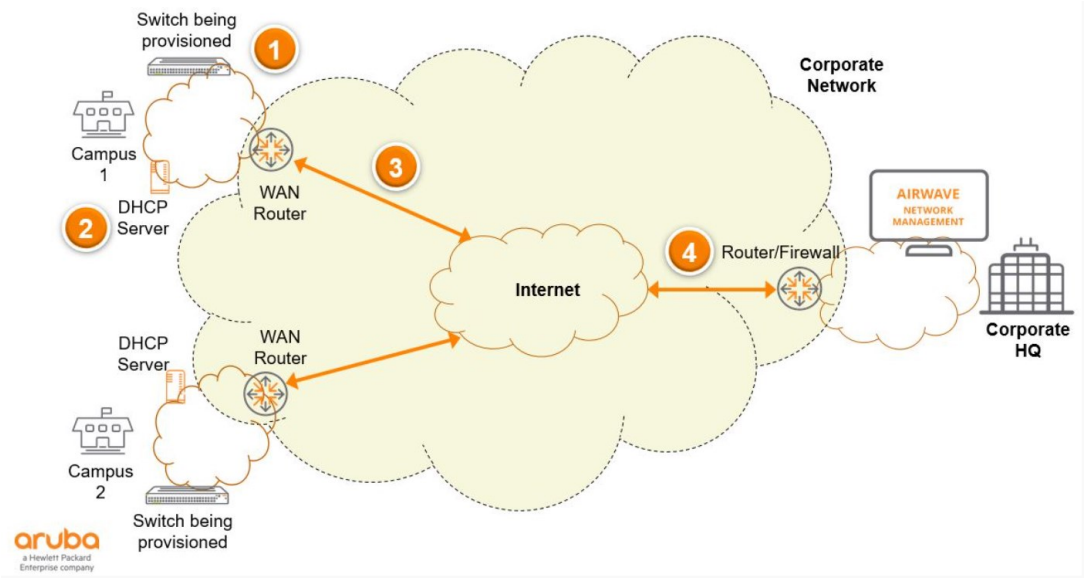
Per questo motivo, AirWave esegue backup periodici dei dispositivi in modo che l'amministratore possa scegliere di ripristinare l'ultima configurazione funzionante nota nel caso in cui lo stato della rete non sia quello previsto oppure se qualcuno modifica accidentalmente la configurazione all'insaputa dell'amministratore.

**Zero Touch Provisioning**

La funzionalità di Zero Touch Provisioning utilizza template di configurazione che permettono di automatizzare tutto il processo di configurazione e di deployment per aziende distribuite che devono gestire anche gli uffici e le sedi remote.

Lo ZTP garantisce che, una volta che la configurazione per un tipo di dispositivo è resa disponibile su AirWave, la configurazione dello switch possa avvenire in modo asincrono senza la necessità che un amministratore di rete sia presente presso la sede centrale o il campus al momento del deployment, riducendo così i tempi, i costi e il personale necessari per la gestione delle filiali remote eliminando allo stesso tempo anche eventuali errori umani di configurazione.

ZTP è disponibile solo per i dispositivi Aruba; i dispositivi di fornitori di terze parti possono essere rilevati avviando scansioni di rete o caricando un file CSV su AirWave. In un ambiente multi-vendor, gli utenti possono scegliere uno di questi metodi per rilevare i dispositivi e inserirli nelle cartelle AirWave appropriate per inviare automaticamente la configurazione a quei dispositivi.




*Aruba AirWave esempio funzionalità ZTP*

Nell'immagine su riportata, viene indicato un esempio di come la funzionalità di ZTP possa essere implementata:

- Lo switch che deve essere configurato si trova nel Campus 1 che ha il proprio server DHCP;
- L'istanza di AirWave si trova nella sede principale connessa tramite una rete privata;
- Lo switch in modalità factory-default si connette alla rete e invia una richiesta DHCP;
- Il server DHCP nel campus risponde non solo con il pool IP corretto per lo switch, ma anche con le credenziali AirWave, incluso l'indirizzo IP del server AirWave, la cartella, il gruppo e la password condivisa;
- Il processo ZTP dello switch utilizza queste informazioni per comunicare con il server AirWave nella sede centrale;
- Il server AirWave identifica il dispositivo e invia la configurazione associata al gruppo e alla cartella in base a parametri come il numero di modello e l'indirizzo MAC dello switch (se è stato fornito).

**MIGLIORA LA PIANIFICAZIONE ED IL PROVISIONING DELLA RETE**

- VisualRF consente di eseguire rapidamente pianificazione della copertura RF e cablata per nuovi siti.

**GESTISCE LE ULTIME TECNOLOGIE, ARCHITETTURE E PRODOTTI**

- Un'unica interfaccia di gestione per più generazioni di dispositivi;
- Supporto di AP autonomi, controllati dal controller e mesh, tra cui Aruba Open AirMesh;
- Monitoraggio di dispositivi wired utilizzando MIB standard;
- Generazione report sull'utilizzo delle porte wired per pianificazione delle capacità.

**INTERFACCIA WEB FACILE DA USARE**

- Accesso basato sui ruoli, diritti di visualizzazione e amministrazione privilegi su misura per le responsabilità lavorative;
- I grafici personalizzati delle informazioni chiave consentono di eseguire panoramiche e zoom per visibilità in specifici periodi di tempo;
- Identificazione e ricerca utenti per nome;
- Panoramica del cliente riepiloga i tipi di client collegati a la rete e fornisce visibilità ai clienti vegliati o VIP;
- Le visualizzazioni multiple del cruscotto forniscono visibilità su ogni aspetto di RF, client, applicazioni e servizi di rete.

**OPZIONI VIRTUALI DELL'APPARECCHIO**

La versione virtuale di AirWave è testata per garantire compatibilità e prestazioni con moltissime tipologie di apparati:

- Versione Virtuale che supporta fino a 4.000 dispositivi gestiti.

AirWave richiede una macchina virtuale opportunamente dimensionata

- VMware e Hyper V supportati

Aruba AirWave viene proposto in convenzione come software di gestione on premise, in grado di gestire sia la componente wired, che la componente wireless ed è disponibile in pacchetti di diversi tagli, sulla base del numero di dispositivi che possono essere gestiti dalla piattaforma in maniera centralizzata:

- Software per la gestione fino a 100 nodi (codice prodotto AW-AEDL-100C);
- Software per la gestione fino a 500 nodi (codice prodotto AW-AEDL-500C);
- Software per la gestione fino a 1000 nodi (codice prodotto AW-AEDL-1000C).

I diversi pacchetti possono essere mixati assieme, anche in tagli differenti e attivati sulla stessa piattaforma centralizzata.

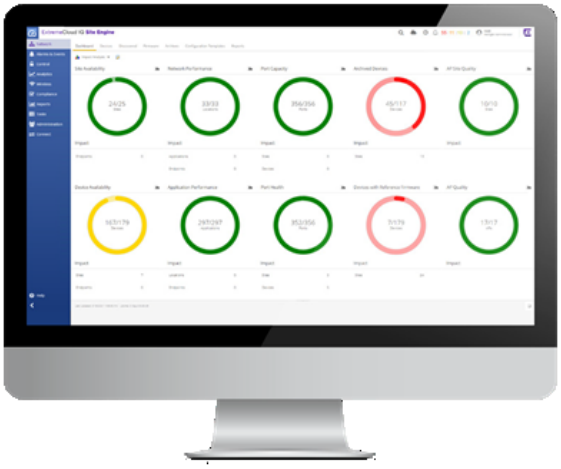
**HARDWARE**

AirWave Enterprise richiede Appliance Enterprise o macchine virtuali:

- VMware ESX(i) 6.7 e successivi (Red Hat Enterprise Linux 8 (64-bit) raccomandato).
- Hyper V Generation 2 (Windows 9, Windows 10, Windows 11)
- KVM Virtual Machine (Red Hat Enterprise Linux 8 (64-bit) raccomandato)
- Browser Supportati
- Google Chrome 39.0.2171.65 e successivi (Windows e macOS)
- Mozilla Firefox 34.0.5 e successivi (Windows e macOS)
- Safari 7 e successivi (macOS)
- Microsoft Edge version 79 e successivi (Windows)

### 2.9.3. Extreme Networks - XIQ Site Engine XIQ-SE_xxx_C

Extreme Networks XIQ Site Engine è una potente piattaforma software progettata per la gestione centralizzata e l'automazione delle reti wireless e cablate all'interno di un'organizzazione. La piattaforma offre una vasta gamma di funzionalità per semplificare l'implementazione, la configurazione, il monitoraggio e la gestione degli switch e degli access point wireless in modo efficiente ed efficace.



*XIQ-Site Engine – Web Interface*

Uno degli aspetti chiave di Extreme Networks XIQ Site Engine è la sua capacità di fornire una visualizzazione dettagliata e intuitiva dello stato degli switch e degli access point wireless. Gli amministratori di rete possono accedere a un pannello di controllo centralizzato per ottenere una panoramica completa di tutti i dispositivi di rete, inclusi gli switch e gli access point wireless. Questa visibilità consente di individuare rapidamente e risolvere eventuali problemi di rete, migliorando l'affidabilità e la disponibilità complessiva.

La piattaforma supporta anche la gestione degli accessi e delle politiche di sicurezza. Gli amministratori possono definire regole di sicurezza e applicare politiche di accesso granulari per garantire che solo gli utenti autorizzati possano accedere alla rete. Inoltre, XIQ Site Engine offre strumenti per l'identificazione e la mitigazione delle minacce alla sicurezza, fornendo una protezione avanzata contro attacchi informatici e violazioni dei dati.

Oltre alla gestione della sicurezza, XIQ Site Engine semplifica notevolmente l'implementazione e la configurazione degli switch. Gli amministratori possono utilizzare funzionalità di provisioning automatizzato per semplificare il processo di distribuzione degli switch e ridurre gli errori umani. La piattaforma offre anche strumenti di configurazione centralizzata, che consentono di apportare rapidamente modifiche alle impostazioni degli switch su scala, migliorando l'efficienza operativa complessiva.

XIQ Site Engine offre inoltre un robusto set di funzionalità di monitoraggio e analisi delle prestazioni degli switch. Gli amministratori possono ottenere informazioni dettagliate sulle prestazioni della rete, inclusi

dati sulla larghezza di banda, l'utilizzo delle risorse e le metriche di qualità del servizio (QoS). Queste informazioni consentono di identificare i colli di bottiglia della rete, ottimizzare le prestazioni e fornire un'esperienza di rete migliore agli utenti finali.

In sintesi, Extreme Networks XIQ Site Engine è una piattaforma software completa per la gestione delle reti, offrendo funzionalità di visualizzazione, gestione della sicurezza, provisioning automatizzato e monitoraggio delle prestazioni degli switch e degli access point wireless. La piattaforma mira a semplificare e ottimizzare le operazioni di rete, consentendo agli amministratori di gestire gli switch in modo più efficiente e fornire una connettività affidabile e sicura agli utenti finali.

**XIQ-SE: Soluzione di Gestione end to end**

Da una singola schermata, ExtremeCloud IQ - Site Engine offre una gestione end-to-end della rete cablata e wireless, dall'edge al data center. Supporta l'intero ciclo di vita della gestione di rete, partendo dalla fase di pianificazione della distribuzione iniziale tramite modelli di configurazione per definire in anticipo le impostazioni del sito, delle porte, dei servizi, del firmware di riferimento e degli attributi di rete, fino alla fase di distribuzione con Zero Touch Provisioning Plus (ZTP+) (che consente la distribuzione automatizzata di uno switch nuovo tramite modelli e flussi di lavoro), e infine alla fase finale in cui le operazioni giornaliere e on-demand (come l'aggiunta di nuovi servizi e VLAN) sono semplificate e le attività di manutenzione (come gli RMAs e le finestre di manutenzione del servizio) possono essere implementate.

ExtremeCloud IQ - Site Engine offre una visione dettagliata degli utenti, dei dispositivi e delle applicazioni con una dashboard di inventario e una topologia di rete di facile comprensione per una gestione efficiente. Le politiche e i nuovi servizi, come il bring your own device (BYOD), possono essere abilitati tramite l'interfaccia grafica integrata e applicati al punto di ingresso di rete tramite ExtremeControl per ExtremeCloud IQ - Site Engine. Per migliorare la gestione dei dispositivi di rete di terze parti, la dashboard mostra la loro topologia e scoperta.

Le mappe di topologia forniscono visualizzazioni di reti non fabric e fabric. Le visualizzazioni non fabric consentono, ad esempio, di visualizzare la presenza di VLAN o lo stato del collegamento dei percorsi primario e secondario all'interno di uno schema Ethernet Automatic Protection Switching (EAPS) di un'architettura ad anello Ethernet. Gli utenti possono visualizzare lo stato dei gruppi di aggregazione del

collegamento (LAG) e dei gruppi di aggregazione del collegamento multi-switch (MLAG) e determinare quali dispositivi partecipano all'aggregazione del collegamento. Gli utenti possono visualizzare una topologia di bridge port extender (BPE) e determinare quali bridge di controllo vengono utilizzati, quali BPE sono presenti e lo stato della topologia.

Per maggiori dettagli fare riferimento alla scheda tecnica di ExtremeCloudIQ-Site Engine

**La gestione della soluzione Fabric Connect**

Grazie al supporto delle funzionalità di gestione fabric integrate nativamente in ExtremeCloud IQ - Site Engine, il tempo di servizio viene notevolmente ridotto. Gli utenti beneficiano di flessibilità grazie alla possibilità di cambiare automaticamente la persona del sistema operativo dello switch dalla configurazione di fabbrica all'OS del motore di fabric durante la distribuzione della rete fabric. Altre funzionalità includono la configurazione e personalizzazione della topologia di fabric, nonché la configurazione dei servizi di fabric (ad esempio, L2VSN, L3VSN, ID, nome e tipo di servizio), degli elementi di routing virtuale distribuito (DVR) (ad esempio, Leaf, Controller e Router), dei protocolli di ridondanza del router (ad esempio, VRRP, RSMLT, DVR) e dei modelli di porta.

Le visualizzazioni specifiche per il fabric aiutano gli utenti a monitorare più facilmente i parametri relativi al fabric, come le aree fabric e i collegamenti Fabric Connect, per individuare le aree IS-IS presenti e determinare quali collegamenti fanno parte del fabric. Inoltre, gli utenti possono visualizzare i percorsi primari e secondari tra due switch di fabric nella rete e determinare in quale parte della rete è presente un determinato servizio di fabric e verificare le sue principali caratteristiche (ad esempio, L2VSN vs L3VSN, assegnazione VRF). Queste importanti capacità di visibilità assistono gli utenti nel monitoraggio e nella convalida delle implementazioni non fabric, fabric e combinate e semplificano il processo di risoluzione dei problemi quando necessario.

**La soluzione per la sicurezza al bordo della rete: XIQ-SE Control**

ExtremeCloud IQ - Site Engine Control consente di unificare la sicurezza delle reti cablate e wireless di un'organizzazione, offrendo una profonda visibilità e controllo sugli utenti, i dispositivi e le applicazioni. Con gli aggiornamenti mensili sulla sicurezza forniti, Extreme Networks si conforma ai requisiti di sicurezza richiesti dalle infrastrutture di rete odierna.

Con l'applicazione ExtremeControl disponibile come parte di ExtremeCloud IQ - Site Engine, la sicurezza degli accessi è abilitata tramite un controllo dell'accesso di rete (NAC) basato sui ruoli per tutti i dispositivi, inclusi quelli di terze parti. L'applicazione consente in modo sicuro il bring your own device (BYOD), l'accesso ospite e il controllo degli oggetti Internet of Things (IoT) per proteggere la rete da minacce esterne e salvaguardare i dati aziendali prevenendo attivamente l'accesso di utenti non autorizzati e endpoint compromessi. È possibile gestire in modo centralizzato e definire politiche granulari per soddisfare gli obblighi di conformità, individuare, autenticare e applicare politiche mirate a utenti e dispositivi.

È integrato con importanti piattaforme enterprise, comprese soluzioni per la sicurezza di rete, la gestione della mobilità aziendale, l'analisi dati, il cloud e il data center. Inoltre, offre un'API aperta verso l'alto (northbound API) per integrazioni personalizzate con le principali piattaforme enterprise. Per ulteriori informazioni su ExtremeControl, si prega di fare riferimento alla scheda tecnica di ExtremeControl per ExtremeCloud IQ - Site Engine.

Il modulo XIQ-SE Control è opzionale e non incluso nella fornitura.

**Analytics: la visibilità di livello applicativo sulla rete**

ExtremeCloud IQ - Site Engine Analytics fornisce informazioni aziendali utili provenienti dalla rete end-to-end, offrendo dettagli approfonditi sulle prestazioni delle applicazioni e della rete tramite telemetria delle applicazioni e ispezione approfondita dei pacchetti (DPI). ExtremeAnalytics per ExtremeCloud IQ - Site Engine accelera la risoluzione dei problemi separando le prestazioni della rete dalle prestazioni delle applicazioni, consentendoti di identificare rapidamente le cause principali. Monitora le applicazioni shadow IT, identifica e segnala le applicazioni dannose o indesiderate e contribuisce alla conformità in materia di sicurezza.

L'Analytics Engine all'interno di ExtremeAnalytics estende la visibilità delle applicazioni dai dispositivi cablati e wireless fino al campus e al data center. Grazie all'ispezione approfondita dei pacchetti, gli amministratori di rete possono visualizzare e analizzare il traffico di rete su più livelli per ottenere informazioni precise in tempo reale. Inoltre, l'integrazione con AWS, GCP e Azure offre una capacità unica di un singolo set di strumenti di analisi che copre campus, data center e istanze cloud. Per ulteriori

informazioni su ExtremeAnalytics, si prega di fare riferimento alla scheda tecnica di ExtremeAnalytics per ExtremeCloud IQ - Site Engine.

**Automazione esplicita con il modulo Task e Workflow**

ExtremeCloud IQ - Site Engine offre capacità di automazione dei flussi di lavoro tra domini attraverso un approccio grafico intuitivo per automatizzare facilmente le attività di rete. Strumenti di automazione e flusso di lavoro integrati, oltre al supporto per linguaggi di scripting comuni (come Python), contribuiscono a ridurre la gestione basata sull'interfaccia della riga di comando, alleviando l'onere sul personale IT e gli impatti di eventuali interruzioni non intenzionali. Un flusso di lavoro può essere attivato da qualsiasi evento, come il raggiungimento di una soglia, un messaggio di syslog o un trap ricevuto, un'azione dell'utente o addirittura una chiamata API esterna. Il flusso di lavoro può ri-configurare la rete o interagire con soluzioni di terze parti. Ad esempio, se viene rilevato il riavvio del dispositivo, i log tecnici e i dettagli possono essere raccolti e un ticket del servizio di assistenza può essere creato direttamente dal flusso di lavoro. Se viene rilevata un'elevata utilizzazione della CPU, il flusso di lavoro può raccogliere automaticamente informazioni aggiuntive sui processi in esecuzione. ExtremeCloud IQ - Site Engine può trasformare una sveglia alle 3:00 del mattino in un follow-up alle 10:00 del mattino.

**ExtremeCloud IQ – Site Engine: l'ecosistema e l'integrazione con le soluzioni IT**

ExtremeCloud IQ - Site Engine è integrato con le principali piattaforme enterprise per ottimizzare i processi aziendali, consentire un'analisi dei dati più robusta e offrire un'esperienza utente senza soluzione di continuità. ExtremeConnect offre integrazioni con importanti piattaforme enterprise per la sicurezza di rete, la gestione mobile, l'analisi dei dati, il cloud e le soluzioni per il data center.

Inoltre, viene offerta una suite completa di API aperte derivanti dal portfolio di infrastrutture di rete di Extreme, che include switch e punti di accesso wireless. Questo comprende metodi di integrazione classici come SNMP, Syslog, nonché metodi di integrazione più efficienti basati su REST API. Ulteriori informazioni sono disponibili nella pagina web delle API di ExtremeCloud IQ Site Engine.

### 2.9.4. Juniper - Junos Space Network Director S-JSPLT-S1-P-x00-C

Junos Space Network Director è una soluzione software di Network Management che include funzionalità di visualizzazione, analisi e gestione di reti Enterprise in ambito campus Lan e data center.

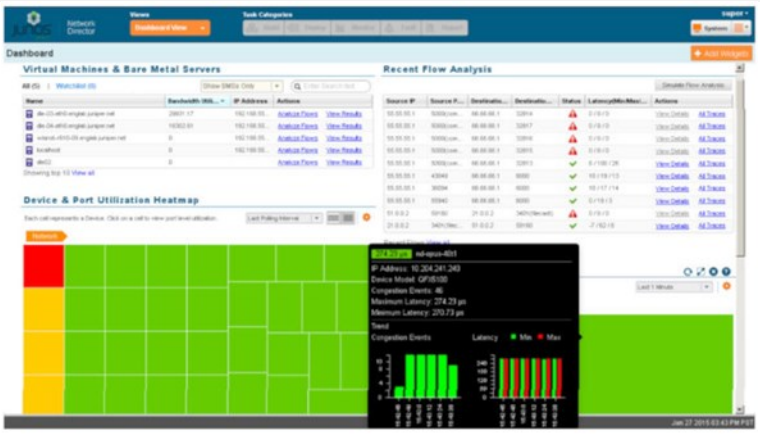
Junos Space Network Director fornisce un'unica console di gestione che permette di accedere alle funzioni di gestione, automazione e provisioning della piattaforma, che è costituita da tre componenti software principali:

- Junos Space Network Management Platform: fornisce tutte le funzioni tipiche di una piattaforma FCAPS (fault, configuration, accounting, perfomance and security);
- Junos Space Management Applications – applicazioni domain-specific che forniscono le funzionalità' di configurazione e provisioning dei servizi di rete sugli apparati Juniper Networks;
- Junos Space SDK (software development kit) – una soluzione di programmazione per integrare l'infrastruttura di rete nei processi e nelle applicazioni aziendali.

**Funzionalità in evidenza**

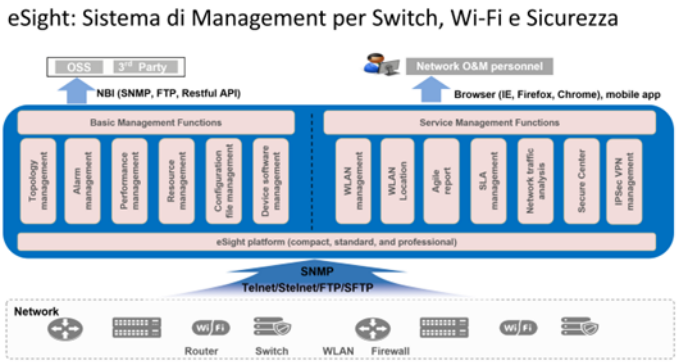
| | |
|---|---|
| Device Discovery | Strumento Wizard based per il discovery degli apparati di rete |
| Topology | Vista topologica dell'infrastruttura a diversi livelli |
| Inventory | Gestione degli asset relativi all'infrastruttura di rete |
| Software image | Gestione centralizzata delle release software |

| | |
|---|---|
| Configuration Template | Template per la gestione della configurazione degli apparati di rete |
| Configuration Management | Gestione avanzata dei file di configurazione: import, export, compare, backup/restore, scheduling |
| Fault and Performance | Eventi e performance management per tutta l'infrastruttura di rete |



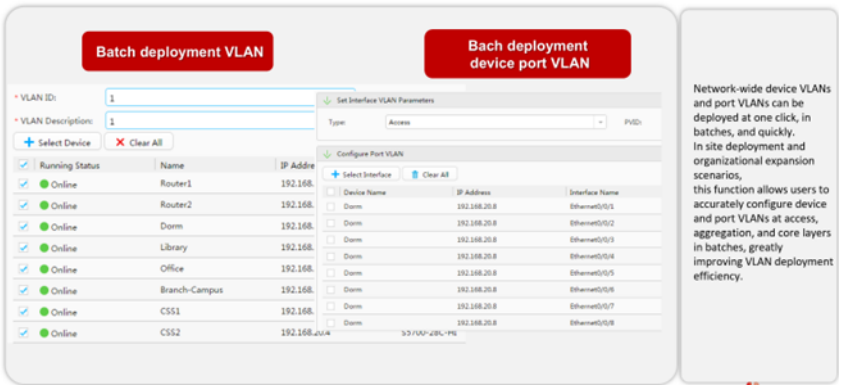

### 2.9.5. Huawei - eSight-x00-C

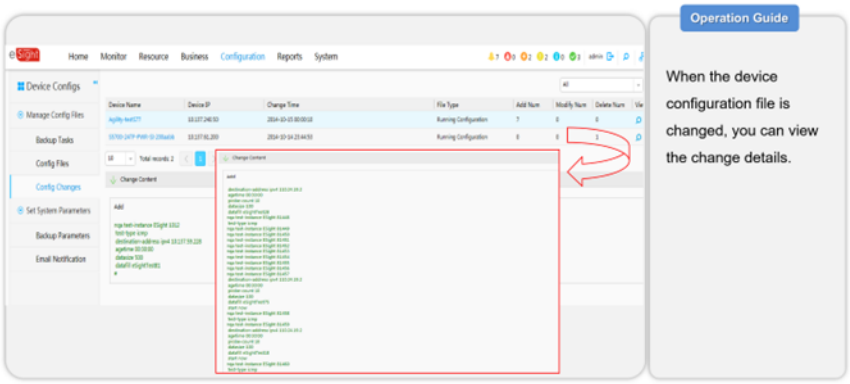
eSight è un software avanzato di gestione networking che permette il provisioning, il monitoraggio, allarmistica e ottimizzazione delle prestazioni dell'infrastruttura di rete switching, wireless e next generation firewall. Scala fino a 20000 nodi di rete.



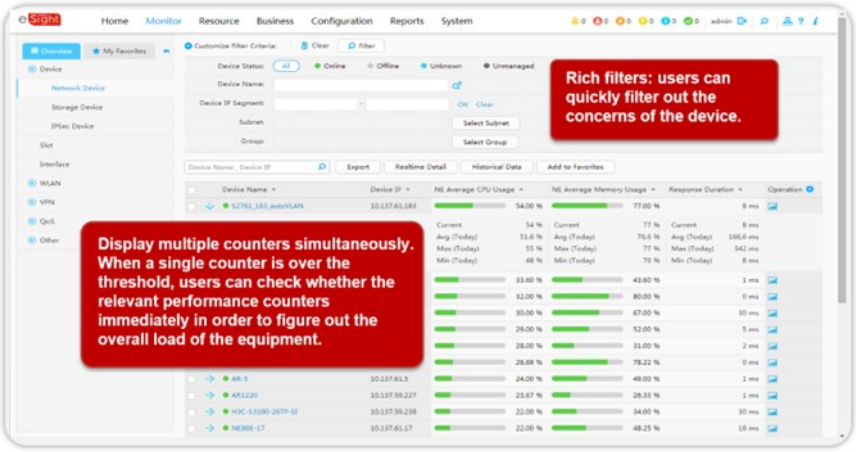

Le interfacce grafiche del software di gestione Wired e Wireless e le tecnologie uniche di visualizzazione dati semplificano la gestione accurata e tempestiva:

- Procedure guidate visive per semplificare le configurazioni e il provisioning dei servizi in maniera più rapida e senza errori;

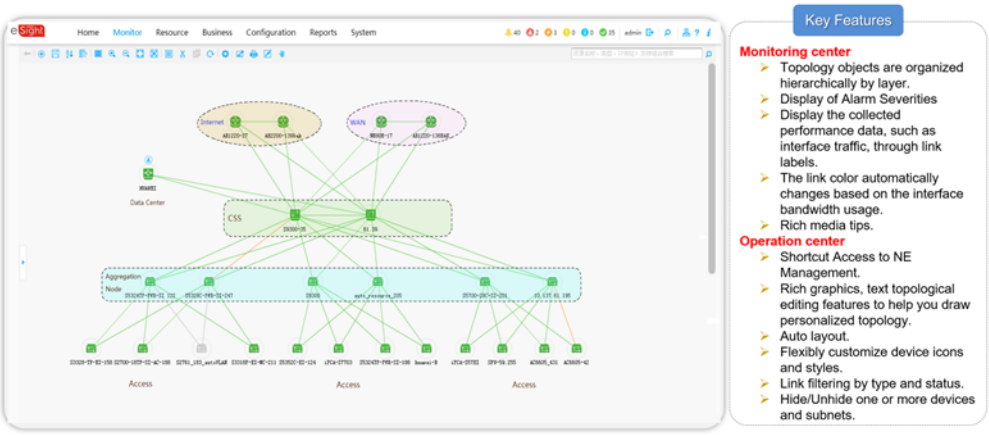



- Visualizzazioni topologiche dei network element (switch, access controller (AC), access point (AP)), corredate con i dati su utilizzo, prestazioni e interferenze, forniscono dettagli immediati sullo stato della rete switched e della Wireless LAN;




- La funzionalità di diagnostica intelligente identifica i guasti nei dispositivi della stazione lato utente (STA) causati da configurazioni sbagliate, ad esempio versioni del sistema operativo, impostazioni dell'adattatore di rete wireless e impostazioni dell'assistenza del sistema sbagliate, rendendo più efficiente la ricerca guasti e riducendo i costi;

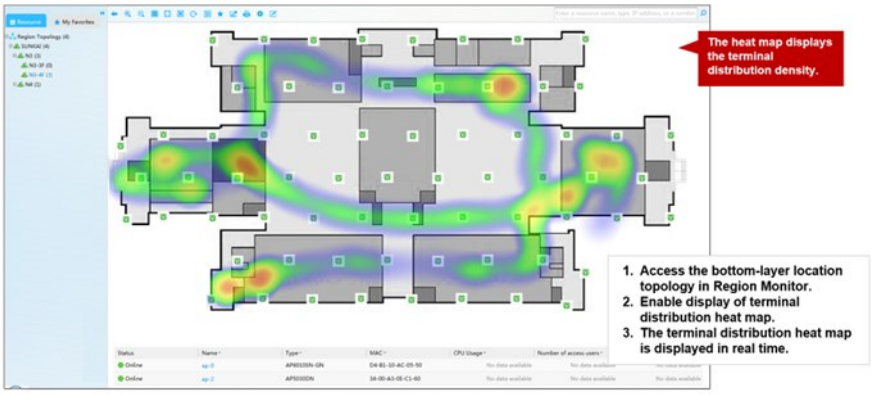



- Vengono utilizzate tecnologie innovative di visualizzazione dei dati, per presentare visualizzazioni il più possibile dettagliate degli access point e degli access controller all'interno della topologia;


- Analisi dello spettro dei segnali di interferenza e rappresentazioni termografiche delle posizioni e della copertura degli access point aiutano l'identificazione dei vuoti e dei conflitti nella copertura;

- Infrastruttura Wired e Wireless LAN costantemente monitorata in tempo reale; visualizzazioni della topologia locale basate sulla logica di rete mostrano access controller, access point, utenti, intensità di campo della rete wireless e condizioni dei guasti per ogni piano dell'edificio; funzioni per la gestione visiva integrate permettono la risoluzione rapida dei problemi;


- Categorizza, identifica e gestisce client non autorizzati, fonti di interferenza e attacchi di pirateria informatica basandosi sulle regole definite dall'amministratore per ridurre i rischi a cui è sottoposta la rete wireless;
- Wireless Real Location System per la mappatura degli utenti;




# 3. SD-WAN

## 3.1. Soluzione Fortinet

Le soluzioni SD-WAN, acronimo di Software-Defined Wide Area Network ovvero reti WAN definite via software, consentono di creare infrastrutture di rete ibride, definite da sistemi di orchestrazione

software, mediante l'implementazione di strati logici di rete (overlay). Queste reti logiche permettono alle organizzazioni, siano esse imprese o pubbliche amministrazioni, di accedere in maniera dinamica ai servizi forniti dalla rete indipendentemente dalle diverse tecnologie di connettività (MPLS, 4G/5G, banda larga) e secondo politiche di selezione del percorso basate sulla qualità della rete e non secondo scelte preconfigurate.

Queste tecnologie, adattandosi in tempo reale alle caratteristiche della rete consentono alle organizzazioni di accedere rapidamente e facilmente a tutte le tipologie di applicazioni business-critical siano esse su cloud sia ospitate presso i data center dell'organizzazione stessa.

Una soluzione SD-WAN consente di selezionare il miglior percorso di accesso ad una applicazione ovunque essa sia collocata: cloud pubblico, data center, cloud privato. La selezione avviene in maniera totalmente trasparente all'utente, che non cambia in alcun modo il proprio metodo di accesso alla rete o all'applicazione: è il meccanismo di orchestrazione di rete a selezionare dinamicamente gli instradamenti. La soluzione SD-WAN effettua le proprie scelte basandosi sulla valutazione della qualità della rete, andandone a verificare le prestazioni mediante alcuni indicatori specifici come, ad esempio, la latenza di accesso all'applicazione, l'eventuale perdita di pacchetti su un percorso, o la banda effettivamente disponibile per l'accesso.

Questo approccio differisce notevolmente da quello utilizzato nelle infrastrutture classiche dove la selezione dei percorsi è basata su scelte per lo più amministrative o su politiche di alta disponibilità.

La dinamicità delle infrastrutture di tipo SD-WAN è possibile attraverso alcune caratteristiche ad esse peculiari di seguito elencate.

**Riconoscimento delle applicazioni**

La soluzione SD-WAN è in grado di riconoscere le diverse applicazioni e di monitorarle, questo consente di basare le scelte di instradamento non su destinazioni statiche ma in base all'effettiva localizzazione di applicazioni critiche. Senza funzionalità per il riconoscimento delle applicazioni, il tracciamento delle stesse potrebbe rivelarsi estremamente complicato soprattutto per le applicazioni in cloud che variano in maniera dinamica e scarsamente predicibile la loro localizzazione all'interno della rete.

Con le soluzioni WAN tradizionali, pertanto, le organizzazioni possono solo affidarsi a politiche di routing di tipo classico basate su destinazioni spesso difficili da manutenere.

**Selezione dinamica del percorso**

Le soluzioni SD-WAN supportano la selezione dinamica del percorso indipendentemente dalla tecnologia di rete. In aggiunta alle già citate funzionalità di monitoraggio della rete, le soluzioni SD-WAN offrono anche una serie di parametri di configurazione per modificare i comportamenti in maniera dinamica: questi possono basarsi su scelte puramente amministrative, come ad esempio privilegiare una linea a basso costo rispetto ad una più pregiata, oppure su metodi automatici come la riservazione di banda per le applicazioni critiche alle quali viene garantita, in ogni momento, una disponibilità minima di risorse che ne consentano il funzionamento.

**Configurazione degli apparati senza interventi manuali**

Le soluzioni SD-WAN, oltre a consentire una separazione tra il piano di controllo e i dati possibile grazie al sistema di orchestrazione, consentono una rapida distribuzione e configurazione degli apparati di rete. Mediante il sistema di orchestrazione, che si avvale di una console di gestione centralizzata, è possibile semplificare al minimo indispensabile la configurazione degli apparati di rete con sistemi di zero-touch provisioning (ZTP). Attraverso lo ZTP, gli apparati ricevono automaticamente ed in maniera massiva le configurazioni dal sistema di orchestrazione, utilizzando template di configurazioni predefiniti e personalizzabili.

**Orchestrazione centralizzata**

L'infrastruttura di rete SD-WAN di Fortinet puo' essere gestita sia in maniera distribuita, configurando le policy su ogni singolo apparato, oppure in maniera centralizzata mediante FortiManager. Questo consente alle organizzazioni di semplificare la distribuzione centralizzata delle configurazioni e di stabilire l'automazione per risparmiare tempo e rispondere più rapidamente alle richieste del Business. Un'orchestrazione centralizzata è in grado di fornire un flusso di lavoro intuitivo per le policy aziendali al fine di definire in maniera rapida l'overlay di rete, realizzato tramite tunnel cifrati realizzati con l'utilizzo di VPN di tipo IPSec. Mediante il FortiManager e' possibile definire in maniera rapida i template di

configurazione per tutti gli apparati SD-WAN, consentendo una rapida prototipizzazione delle diverse topologie di rete come hub-spoke o mesh.

Queste caratteristiche, peculiari delle infrastrutture SD-WAN, si traducono in alcuni vantaggi tra cui:

**Riduzione della Complessità**

L'SD-WAN consente di collassare in un'unica piattaforma i servizi di routing, sicurezza, WAN optimization. L'utilizzo degli apparati FortiGate consente di utilizzare una completa suite di funzionalità di sicurezza da cui la definizione di **Secure SD-WAN.**

**Migliorare la Application Experience**

L'SD-WAN consente di incrementare la fruibilità delle applicazioni Cloud dando la priorità alle applicazioni business-critical e consentendo un accesso diretto a Internet presso le filiali che possano disporre di un collegamento Internet locale (Internet local break-out)

**Semplificazione del Management**

La piattaforma di management fornisce un Single-pane-of-glass e, con la funzionalità zero-touch provisioning sull'intera componente WAN Edge, semplifica l'implementazione dell'SD-WAN e dei servizi di sicurezza.

**Semplicità**

Con l'evoluzione delle infrastrutture di rete, la proliferazione di prodotti monofunzionali utilizzati separatamente per il networking e per la sicurezza può complicare l'operatività. SD-WAN utilizza l'automazione e altri vantaggi per semplificare la connettività in ambienti misti, compresi quelli on-premise, ibridi e cloud.

**Predisposizione agli ambienti multi-cloud**

Con la continua migrazione delle applicazioni verso le infrastrutture in cloud, adottare una strategia multi-cloud gestita mediante una soluzione SD-WAN semplifica l'interazione degli utenti con il complesso ambiente delle applicazioni. Multi-cloud è un concetto diverso dal cloud ibrido, in cui cloud pubblici e privati sono integrati per ottimizzare le prestazioni, la sicurezza e la flessibilità. Multi-cloud significa semplicemente che le organizzazioni hanno la flessibilità di selezionare il miglior fornitore di servizi cloud per soddisfare tutte le loro variegate esigenze in termini di infrastrutture e applicazioni.

**Sicurezza complessiva migliorata**

Una soluzione di Secure SD-WAN, con i servizi di sicurezza integrati, migliora la sicurezza complessiva di qualsiasi organizzazione. Viceversa, senza servizi di sicurezza integrati, può trasformarsi in un ulteriore vettore di attacco.

### 3.1.1. Componenti Hardware e Software

L'architettura della soluzione Fortinet Secure SD-WAN è composta dai seguenti elementi:

**Edge Devices:** sono i **FortiGate** presso le sedi Cliente che implementano le funzionalità SD-WAN e di Next Generation Firewall. Sono responsabili dello startup degli overlay (tunnel IPSec tra le sedi secondarie e le sedi principali e tunnel tra le varie sedi on demand in caso di comunicazione tra sedi spoke).

**Gestione Centralizzata:** il **FortiManager** è l'elemento responsabile di gestire centralmente i vari FortiGate implementando la configurazione (Overlay, Underlay, SD-WAN policy, Security Policy, Zero Touch Provisioning, etc.) sui vari FortiGate.

**Log & Reports Centralizzato:** gli apparati FortiGate dispongono di apposite schermate della GUI per la visualizzazione delle informazioni di traffico e dei trend relativi agli SLA monitorati. Inoltre le componenti SD-WAN si possono integrare con componenti esterne della Security Fabric di Fortinet per la raccolta dei log generati dai vari FortiGate, per la visualizzazione delle informazioni relative al traffico gestito e per la generazione dei reports.

**FortiGate**

Il Next Generation Firewall FortiGate collega reti e percorsi di sicurezza qualsiasi sia la tecnologia di accesso: Internet, 3G/4G o collegamenti WAN privati. Implementa il WAN Path Controller per la gestione dinamica dei percorsi di rete. Con l'aiuto della gestione delle applicazioni, consente di dare priorità alle applicazioni business-critical, infatti all'interno del sistema operativo FortiOS sono codificate oltre 5000 applicazioni, consentendo la visibilità granulare anche delle sotto-applicazioni ad esse collegate. Mediante le funzionalità SD-WAN dell'apparato Fortigate è possibile implementare la Path Awareness Intelligence, ossia le funzionalità intelligenti di riconoscimento del percorso per monitorare le transazioni a livello di applicazione, ed il failover dinamico sul miglior percorso disponibile.

Peculiarità della soluzione Fortinet è la sicurezza integrata all'interno degli apparati SD-WAN. Altre soluzioni SD-WAN adoperano soluzioni di terze parti per aggiungere funzionalità di sicurezza di tipo NGFW, sfruttando logiche di tipo VNF Service Chaining o soluzioni di security in Cloud. In quest'ultimo caso tutto il traffico deve essere reinstradato verso i data center del vendor per essere ispezionato, facendo cadere eventuali benefici del local breakout per l'accesso diretto ad Internet presso i vari branch oltre che, di fatto, aggiungendo complessità all'architettura complessiva che non può essere gestita per tutte le sue componenti da un'unica console. Viceversa, integrare sicurezza ed SD-WAN in una singola appliance si traduce anche in riduzione dei costi operativi in virtù della semplificazione e del consolidamento della gestione attraverso un single-pane-of-glass.

Fortinet implementa le diverse funzionalità sfruttando l'accelerazione in Hardware: ad esempio, il riconoscimento delle applicazioni (Skype, Salesforce, Office 365, etc.) viene fatto mediante Deep Paket Inspection e SSL Inspection in Hardware. Ciò consente, cona la massima rapidità ed efficienza, di scegliere esattamente quale applicazione deve essere instradata, su quale link (MPLS, Internet, etc.) e con quale politica (Bilanciamento, SLA, Throughput Massimo, etc.).

Tutto questo è completato dalle funzionalità di sicurezza integrate in un unico prodotto (NSS Labs: https://www.fortinet.com/products/next-generation-firewall#certifications), tra cui:

- Anti-Virus (con disponibilità firme Anti-Malware specifiche e dedicate per Mobile Malware e per Industrial Security)
- Intrusion Prevention/Detection System
- Data Leak Prevention
- Anti-Spam

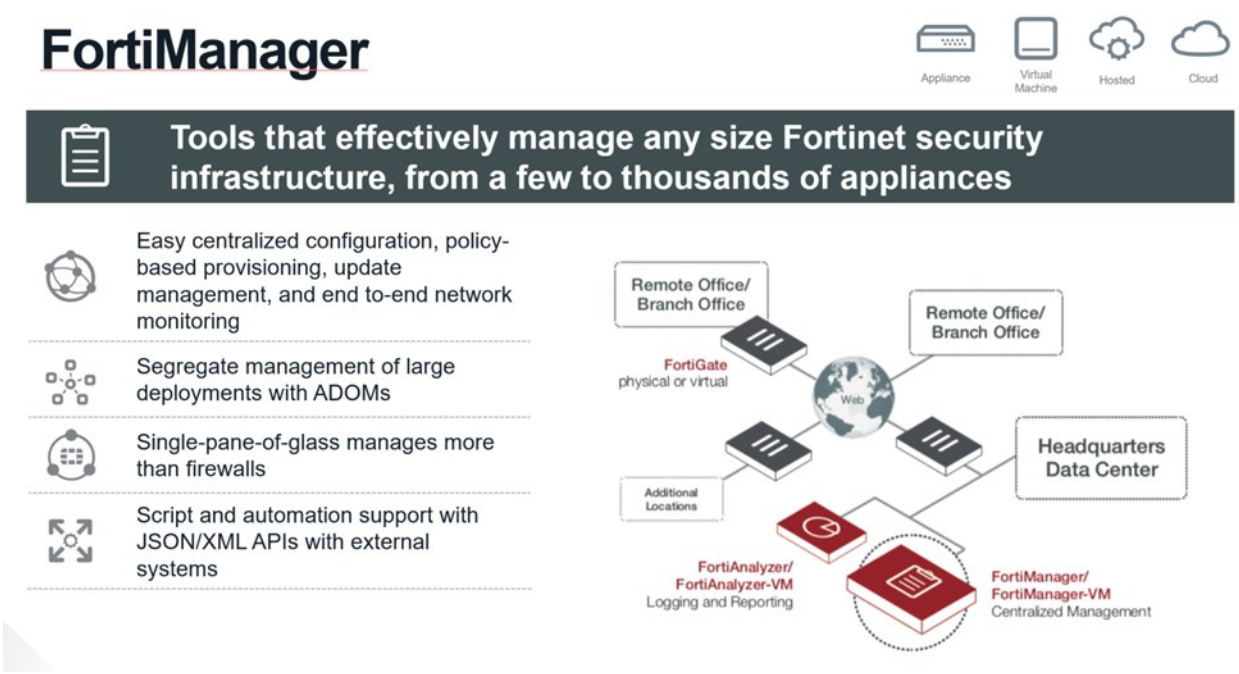
- Web Application Firewall
- Zero-Day/ATP Integration con tecnologia Fortinet Sandbox esterna
- Application Control
- VPN IPSec con strong encryption (AES256 SHA256 o superiori)
- SSL VPN

FortiGate implementa la funzionalità Virtual Domains (VDOM) in modo nativo. I VDOM possono essere utilizzati per dividere i FortiGate in più dispositivi virtuali che funzionano in modo indipendente. In ciascun VDOM possono essere create diverse configurazioni (incluse politiche SD-WAN, link, VPN, etc.). Poiché ogni VDOM è un dominio di routing indipendente, è possibile utilizzare reti sovrapposte sullo stesso dispositivo. Non è necessaria alcuna licenza aggiuntiva per abilitare la funzione VDOM.

Il minimo numero di VDOM disponibili è di 10 anche sui FortiGate entry level; sui Fortigate di fascia più alta è possibile aumentare la disponibilità di VDOM con opportune licenze.

All'interno di ciascun VDOM è possibile configurare anche le vrf (fino ad un massimo di 32) per separare logicamente le diverse tabelle di routing. Ogni interfaccia fisico/logica può essere associata ad una vrf all'interno della quale poi verranno configurati i relativi protocolli di routing statico / dinamico per la corretta propagazione delle network.

**FortiManager** è il componente che implementa il controller centralizzato con un unico pannello di controllo e semplifica la gestione e il monitoraggio, consentendo alle aziende di introdurre rapidamente nuove filiali e scalare facilmente.




### 3.1.2. Apparato SD-WAN FortiGate

L'apparato FortiGate è disponibile in Convenzione nei seguenti modelli:

- Dispositivo di Fascia Small: FortiGate FG-81F;
- Dispositivo di Fascia Medium: FortiGate FG-81F;
- Dispositivo di Fascia Large: FortiGate FG-101F;
- Dispositivo di Fascia ExtraLarge: FortiGate FG-601F.

Gli apparati in convenzione dispongono del bundle di licenza definito ATP (Advanced Threat Protection). Questo include, di base, le funzionalità di firewalling, di routing e per la gestione delle VPN che vengono utilizzate per definire gli instradamenti di base e per gestire gli overlay. Ad esse si aggiungono le funzionalità specifiche dell'SD-WAN per la gestione dei percorsi e la verifica degli SLA. Per finire, sono incluse nel bundle sopra citato anche specifiche funzionalità di sicurezza di Intrusion Prevention, Anti Malware, Anti Virus, Anti Spam ed Outbreak Prevention.

**Funzionalità supportate dall'apparato FortiGate**

L'apparato FortiGate supporta una serie di funzionalità SD-WAN specifiche e una serie di funzionalità accessorie che rendono più completa l'offerta SD-WAN di Fortinet.

Tra queste funzionalità ricordiamo:

- Traffic stearing da Layer 4 a layer 7 di oltre 5000 applicazioni;
- Firewall da Layer 4 a Layer 7 di nuova generazione (funzionalità di sicurezza NGFW come antivirus, prevenzione delle intrusioni (IPS), controllo delle applicazioni, URL filtering etc.);
- VPN Full-Mesh ed in Autodiscovery (AD-VPN) per comunicazioni overlay any-to-any;
- Supporto dei protocolli di routing RIP, OSPF, BGP, IS-IS per consentire la raggiungibilità dei siti remoti e creare le necessarie politiche di routing per la realizzazione dei tunnel automatici;
- Parallel Path Processing per ottimizzare ed accelerare l'elaborazione del traffico di rete su componenti Hardware proprietari specializzati (Network Processor e Content Processors). Ciò consente a diverse operazioni come Application Control, IPS, Anti-Virus di essere eseguite su Hardware dedicato senza influire sulla CPU del sistema.

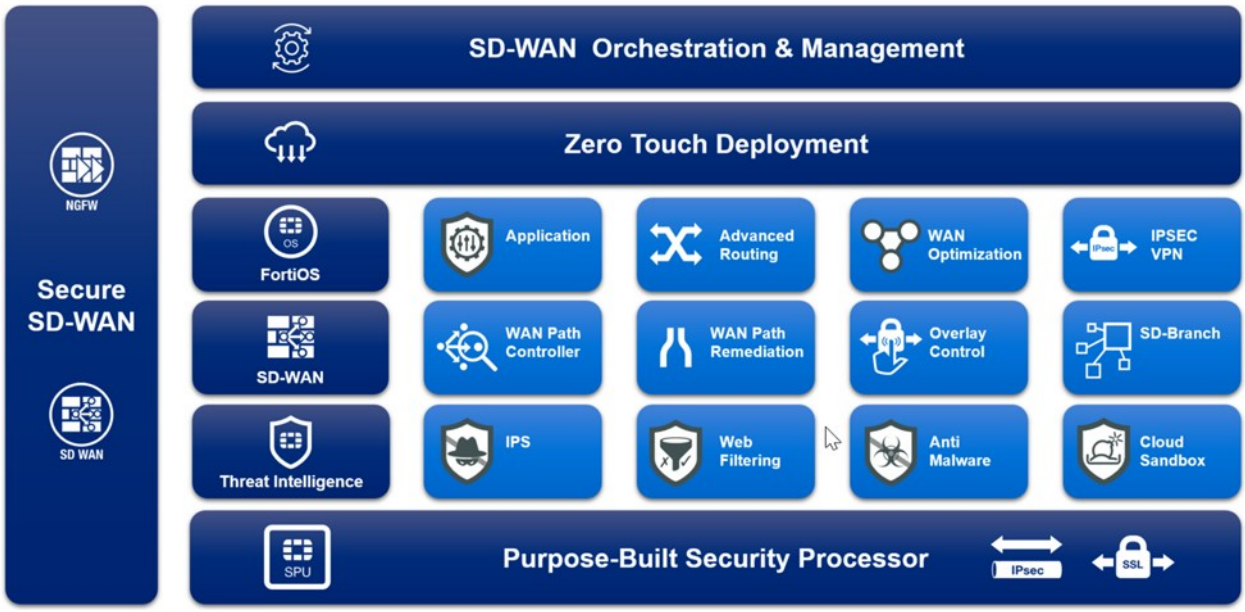
Oltre al supporto nativo delle funzionalità di NGFW l'apparato FortiGate si integra con altre componenti della Fortinet Security Fabric per fornire ulteriori funzionalità di sicurezza integrata. Mediante API è anche possibile l'integrazione di terze parti oppure è possibile sfruttare le possibilità date dalle API per creare infrastrutture di supporto alla configurazione automatica e all'integrazione con applicativi Custom del cliente o del Service Provider.

La lista delle partnership è disponibile all'indirizzo: https://www.fortinet.com/partners/partnerships/alliance-partners.html.

Informazioni relative all'integrazione di terze parti in ambito SD-WAN mediante API sono disponibili all'indirizzo: https://www.fortinet.com/solutions/mobile-carrier/physical-hybrid-vnf/sdn-integration.

**Funzionalità SD-WAN**

La figura seguente riporta lo schema logico dei vari componenti delle funzionalità SD-WAN all'interno della Fortinet Security Fabric.




Come è possibile vedere dalla figura, ad eccezione delle funzioni di ZTP, di management ed orchestrazione, tutte le altre funzionalità sono gestite del FortiGate e sono contenute all'interno del FortiOS.

Le funzionalità indicate sono usate dalle piattaforme SD-WAN per la creazione degli overlay e la gestione dei percorsi mantenendo le prestazioni e la sicurezza delle applicazioni sensibili e real-time.

SD-WAN con Application Aware Routing può misurare e monitorare le prestazioni di più servizi in una rete ibrida. Utilizza il routing dell'applicazione per offrire un controllo più granulare di dove e quando un'applicazione utilizza un servizio specifico, consentendo un migliore utilizzo della rete complessiva.

L'implementazione SD-WAN ha 4 oggetti principali:

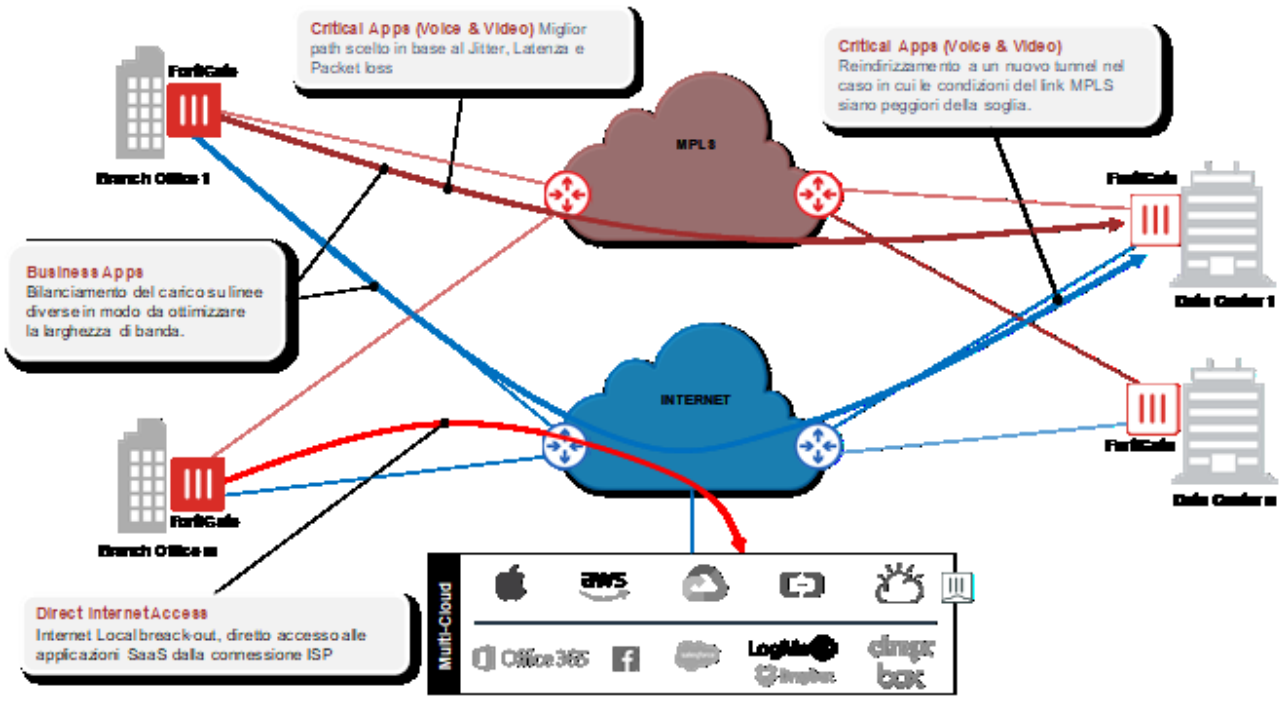
- Zone SD-WAN; SD-WAN è diviso in zone. Le interfacce dei membri SD-WAN vengono assegnate alle zone e le zone vengono utilizzate nelle policy come interfacce di origine e di destinazione. È possibile definire più zone per raggruppare insieme le interfacce SD-WAN, consentendo raggruppamenti logici per le interfacce overlay e underlay. Le zone vengono utilizzate nelle policy di firewalling per consentire un controllo più granulare. I membri SD-WAN non possono essere utilizzati direttamente nelle policy;

- Interfacce SD-WAN; definiti anche membri, i membri SD-WAN sono le porte e le interfacce utilizzate per eseguire il traffico. Almeno un'interfaccia deve essere configurata affinché SD-WAN funzioni; È possibile configurare fino a 255 interfacce membri. Per configurare i membri SD-WAN deve essere abilitato e le interfacce dei membri devono essere selezionate e aggiunte a una zona. Le interfacce FortiGate selezionate possono essere di qualsiasi tipo (fisiche, aggregate, VLAN, IPsec e altre), ma devono essere rimosse da qualsiasi altra configurazione su FortiGate. Una volta che i membri SD-WAN sono stati creati e aggiunti a una zona, la zona può essere utilizzata nelle politiche del firewall e l'intera SD-WAN può essere utilizzata nelle rotte statiche;
- Performance SLA; chiamati anche controlli di integrità, i Performance SLA vengono utilizzati per monitorare la qualità del collegamento dell'interfaccia membro e per rilevare gli errori di collegamento. Possono essere utilizzati per rimuovere percorsi e reindirizzare il traffico quando un membro SD-WAN non è in grado di rilevare il server. Possono anche essere utilizzati nelle regole SD-WAN per selezionare l'interfaccia membro preferita per l'inoltro del traffico;
- Regole SD-WAN; chiamate anche services, le regole SD-WAN vengono utilizzate per controllare la selezione del percorso. Il traffico specifico può essere inviato dinamicamente al collegamento migliore o utilizzare un percorso specifico. Sono disponibili cinque modalità:
    - auto: assegna alle interfacce una priorità in base alla qualità.
    - manuale: assegna manualmente una priorità alle interfacce.
    - priorità: assegnare alle interfacce una priorità in base alla qualità del fattore di costo del collegamento dell'interfaccia.
    - SLA: assegna alle interfacce una priorità in base alle impostazioni SLA selezionate.
    - Load Balancing: distribuisce il traffico tra tutti i collegamenti disponibili in base all'algoritmo di bilanciamento del carico.

**Architettura di riferimento**

Nella figura seguente è riportata l’architettura base di riferimento.

Per una corretta implementazione, e per fruire a pieno di tutti i vantaggi del paradigma SD-WAN, è consigliato che tutte le sedi della rete siano equipaggiate con gli apparati SD-WAN Fortinet. La presenza dell'apparato e quindi i benefici indotti da una architettura SD-WAN prescindono, infatti, dalla specifica tipologia o tecnologia di accesso della sede (singolo accesso, doppio accesso, MPLS, Internet, mobile).

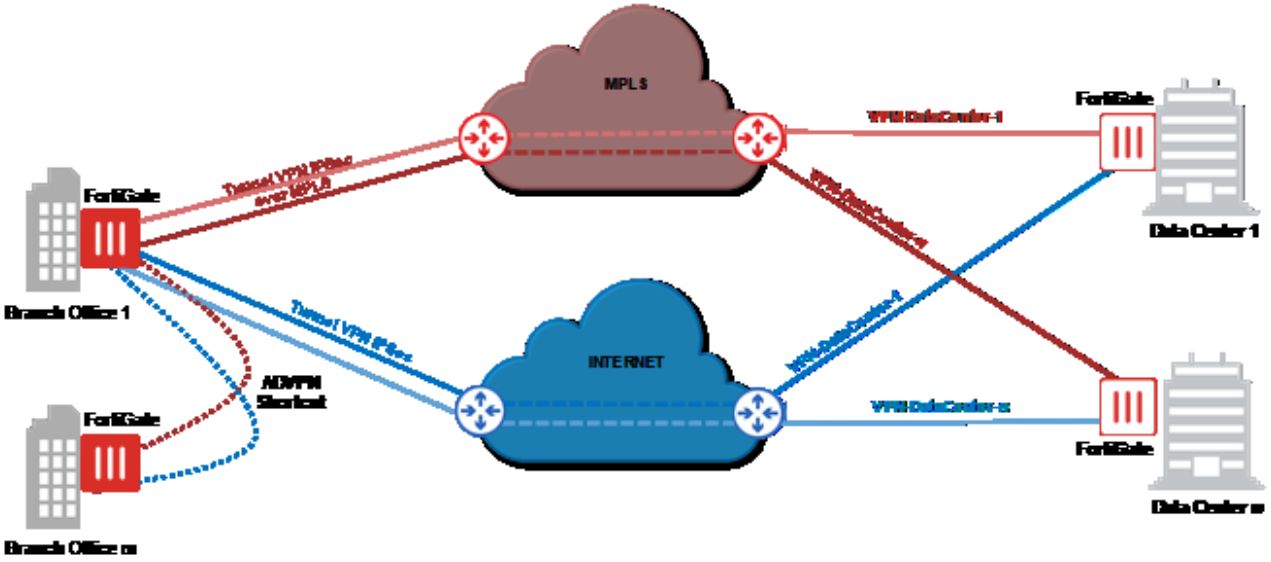



Nel caso dello schema sopra riportato è possibile ad esempio:

- instradare il traffico destinato ai data center utilizzando l'Overlay MPLS, l'Overlay Internet o entrambi;
- Instradare il traffico Internet sfruttando il link locale (Direct Internet Access) o verso il data center per poi utilizzare il link Internet centralizzato (ad esempio in caso di fault del link locale);
- Instradare un determinato tipologia di traffico sul link underlay MPLS (verso destinazioni di Branch Legacy non SD-WAN);
- L'instradamento del traffico verso il DC1 o il DCn viene gestito con SD-WAN Rules con la possibilità di gestire i due DC in modalità Active/Active o Active/Backup (DR);
- Tra i due DC viene instaurato un Tunnel punto punto solo in caso di necessità di connettività intra-DC.

La soluzione Fortinet SD-WAN supporta la creazione di tunnel VPN IPSec dinamici tramite Autodiscovery VPN (ADVPN). All'interno di ADVPN vengono configurati dei tunnel IPSec overlay tra hub e spoke e viene configurato del routing dinamico BGP attraverso l'overlay VPN. Quando uno spoke richiede la connettività diretta a un altro spoke, il pacchetto iniziale viene inviato tramite il sito hub. Successivamente l'hub comunica agli spoke la possibilità di creare uno shortcut diretto tra i due rispettivi IP underlay e viene quindi instaurato un tunnel ipsec dinamico diretto tra i due spoke su cui viene poi instradato il traffico senza transitare dall'Hub. I tunnel VPN di rilevamento automatico sono soggetti alla stessa

capacità di configurazione di qualsiasi altro collegamento VPN e possono essere configurati per essere abbattuti dopo un timeout di inattività o per restare attivi anche in assenza di traffico.




In caso di soluzioni con più punti di aggregazione è possibile creare architetture del tipo Dual Region - Dual Hub dove ogni sede remota fa riferimento ad un Hub differente della propria region e gli Hub poi sono interconnessi tra loro mediante tunnel IPSec in modo da garantire connettività tra spoke appartenenti a region differenti anche in modalità ADVPN.

### 3.1.3. FortiManager

FortiManager fornisce informazioni dettagliate sul traffico di rete e sulle minacce attraverso un unico pannello di controllo e offre funzionalità di classe enterprise ed una sofisticata gestione della sicurezza per una protezione unificata end-to-end per contenere le minacce avanzate. FortiManager offre anche la migliore scalabilità del settore per gestire fino a 100.000 dispositivi Fortinet. FortiManager, insieme alla famiglia FortiAnalyzer di appliance di registrazione e reporting centralizzate, fornisce una soluzione di gestione centralizzata completa e potente.

Le caratteristiche principali del FortiManager sono le seguenti:

- Gestione centralizzata degli apparati: Una singola console che consente di gestire apparati Fortigate, FortiSwitches, FortiAPs e fornire funzionalità di update manager centralizzato per tutti gli apparati gestiti
- Gestione centralizzata di policy e oggetti: Editor per la gestione facile e veloce di Policies, oggetti e profili completamente costruito in HTML5 con funzionalità drag&drop ed editor delle policies senza necessità di editare ogni singola policy per la modifica
- Capacità evolute di tracciamento delle revisioni, auditing delle attività effettuate dagli amministratori
- Gestione dei Workflows per una migliore implementazione dell'utilizzo multiutenza
- Gestione Centralizzata di SD-WAN, Reti Wireless e VPN
- Automazione: Gestione di templates and scripts per il provisioning di nuovi device o modifica degli esistenti. API JSON o XML per l'interazione con sistemi di automazione di terze parti
- Multitenancy e RBAC per una precisa definizione dei ruoli degli amministratori e del loro perimetro di gestione
- Software upgrade e security update centralizzati per i device gestiti

**Gestione centralizzata degli apparati**

L'offerta Fortinet consente una sofisticata gestione della sicurezza per una protezione end-to-end unificata. L'implementazione dell'infrastruttura di sicurezza basata su Fortinet è in grado di combattere le minacce avanzate e l'aggiunta di FortiManager fornisce una gestione single-pane-of-glass nell'intera rete. Le informazioni dettagliate su traffico e minacce di rete sono consolidate su un unico strumento di gestione e monitoraggio.

**Gestione centralizzata delle politiche SD-WAN**

Il FortiManager consente Monitorare centralmente le prestazioni dell'infrastruttura SD-WAN. Visualizzazione dei dispositivi su Mappa con icone colorate e tipizzate, passaggio interattivo del mouse per visualizzare le statistiche sul rendimento di ciascun membro del collegamento SD-WAN.

Visualizza tabella fornisce informazioni più dettagliate per ciascun membro del collegamento SD-WAN, inclusi lo stato del collegamento, le prestazioni dell'applicazione e l'utilizzo della larghezza di banda.

**Gestione delle configurazioni**

Configura collettivamente le impostazioni, gli oggetti e le politiche di ogni dispositivo Fortigate da un'unica interfaccia utente. Il gestore VPN semplifica la distribuzione e la gestione centrallizzata delle VPN, consente di definire una community VPN con provisioning centralizzato e monitoraggio delle connessioni VPN su Google Map. FortiManager consente anche la gestione centralizzata di componenti accessorie Fortinet, non incluse in offerta, come la componente FortiAP Manager che permette di configurare, implementare e monitorare FortiAP da un'unica console con la visualizzazione di Google Map. FortiClient Manager consente la configurazione, l'implementazione e il monitoraggio centralizzati di FortiClients.

**Workflow per Audit and Compliance**

FortiManager consente di esaminare, approvare e controllare le modifiche delle policy da una postazione centrale. Definire processi automatizzati per facilitare il rispetto della conformità delle policy e la gestione del ciclo di vita delle policy. Consente di implementare un flusso di lavoro forzato per ridurre il rischio di modifiche alle politiche di sicurezza non volute.

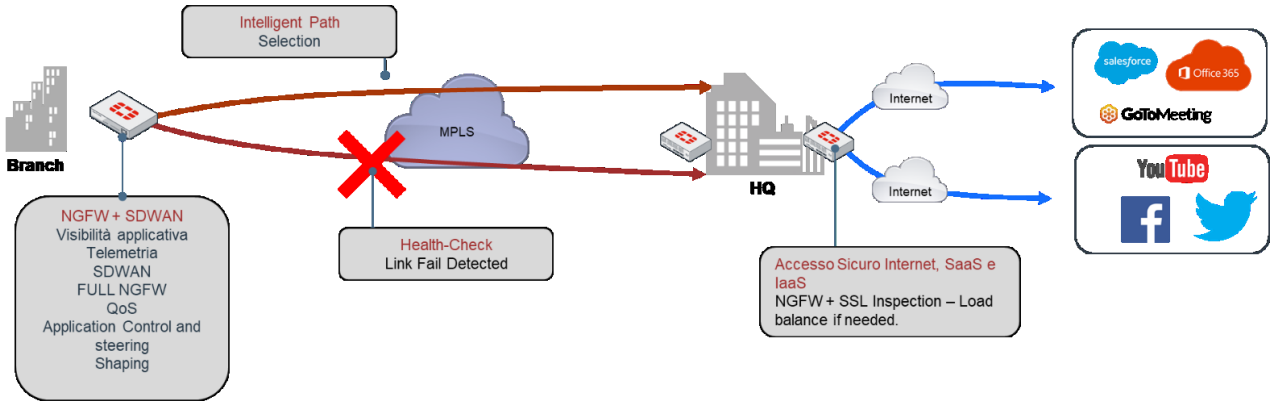
**Monitoraggio e reportistica**

L'accesso alle statistiche di sicurezza e di rete, il monitoraggio in tempo reale ed il reporting integrato offrono visibilità sulla rete e sulle attività degli utenti.

### 3.1.4. Casi d'uso

Analizziamo di seguito alcuni casi d'uso tipici per i quali l'utilizzo di una tecnologia SD-WAN può rappresentare un beneficio per l'utente.

**Caso A:** cliente con rete MPLS, con sedi remote con doppio Link MPLS (primario, Backup) e uscita internet centralizzata presso la sede Master.




In questo scenario un approccio classico presenta una seria di problematiche difficilmente indirizzabili senza SD-WAN. In condizioni di utilizzo normale si ha un utilizzo sub-ottimale delle risorse di rete in quanto solo metà dei link MPLS sono utilizzati a meno di non implementare soluzioni di routing che possano fornire un bilanciamento di carico sui link. Tuttavia, questo bilanciamento viene normalmente eseguito per pacchetto o, nella maggior parte dei casi, per sessione, cosa che non garantisce un uso veramente bilanciato delle risorse. Inoltre, il bilanciamento non trae beneficio dalla possibilità di selezionare i percorsi per applicazione. In questo scenario, in caso di congestione dei link o in caso di degrado non è possibile spostare automaticamente il traffico sul link secondario che può essere utilizzato solo come backup o nelle modalità di bilanciamento esposte sopra.

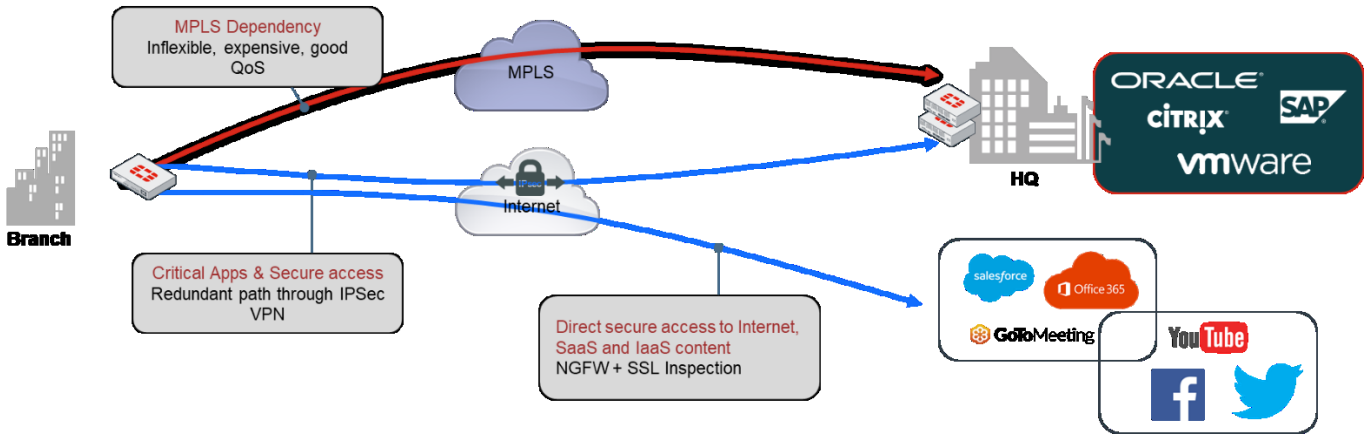
Nel caso in cui venga, invece, implementata una rete di tipo SD-WAN possiamo evidenziare una serie di vantaggi rispetto all'approccio standard:

- Tutti i link della rete MPLS sono utilizzati in modalità active-active senza spreco di risorse, il secondo link MPLS può essere utilizzato contemporaneamente al link principale attivando modalità di condivisione delle banda sulla base di una vasta scelta di parametri come sorgente o destinazione del traffico oppure in base all'applicazione da raggiungere.
- L'utilizzo delle consolle di gestione o della stessa GUI dell'apparato FortiGate garantisce la piena visibilità del traffico che passa sulla sua rete.
- Nel caso in cui uno dei due link MPLS è saturo, l'apparato SD-WAN Fortigate è in grado di spostare il traffico in eccesso in maniera automatica sull'altro link in base a specifiche politiche configurabili. Stessa operazione può essere fatta in caso di degrado del link in quanto è possibile legare alle policy anche gli strumenti di SLA monitoring messi a disposizione dall'apparato FortiGate.

- In caso di disponibilità all'interno della rete di un secondo link per l'accesso a internet è possibile realizzare una struttura a doppio hub con scelta automatica del link d'uscita in base alle diverse metriche previste dalle funzionalità SD-WAN, ad esempio, mediante l'utilizzo di probe di SLA monitoring delle applicazioni remote, è possibile scegliere quale dei due link internet utilizzare in base alla latenza del percorso verso l'applicazione selezionata. (ad esempio, monitoraggio degli SLA verso un server di posta remoto o di una applicazione di tipo SaaS)
- La presenza di un apparato FortiGate su ogni branch garantisce la protezione L7 NGFW (con IPS, Antivirus, etc) locale su ogni sede consentendo una segmentazione della rete granulare.

**Caso B:** cliente con rete MPLS, con sedi remote con doppio Link MPLS (primario, Backup), uscita internet centralizzata presso la sede Master e collegamento Internet secondario presso i branch. (local Internet breakout).

Il caso rappresentato schematicamente nella figura seguente è una variante del caso precendente in cui presso tutte, o alcune, sedi è presente un accesso Internet locale.

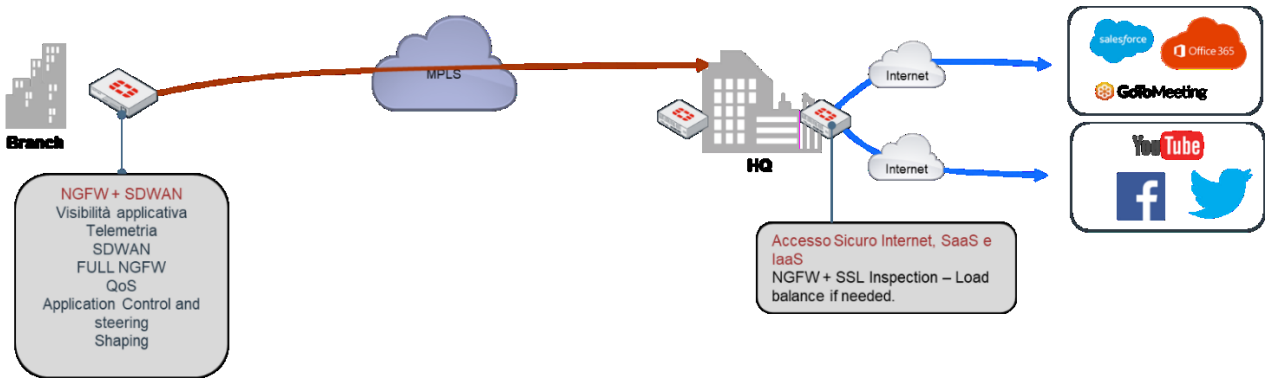



In questo caso l'implementazione di una rete SD-WAN consente di utilizzare nel computo dei percorsi anche il link Internet locale che può essere incluso anche nelle regole di monitoraggio degli SLA per la scelta di quale circuito utilizzare per l'accesso alle applicazioni. Le politiche SD-WAN consentono, in questo caso, di fornire un ulteriore bilanciamento delle risorse ottimizzando l'utilizzo dei link ed aumentano il ritorno dell'investimento sull'infrastruttura.

L'utilizzo di un overlay IPSec consente anche di fornire un accesso sicuro alle applicazioni in Data Center anche nel caso di interruzione o degrado dei collegamenti MPLS in quanto la rete SD-WAN può re-

instradare il traffico su un tunnel cifrato istanziato sopra la connettività Internet. Questo scenario necessita unicamente della raggiungibilità del gateway SD-WAN lato Internet alla stregua della realizzazione di un tipico accesso di tipo VPN.

**Caso C:** cliente con rete MPLS, con sedi remote con singolo Link MPLS e uscita Internet centralizzata presso la sede Master. Utenze tipiche di questo caso sono le Pubbliche Amministrazione medio-piccole con singolo accesso.




Sebbene il singolo link non consenta di ottimizzare i percorsi, l'utilizzo di una rete SD-WAN presenta diversi vantaggi.

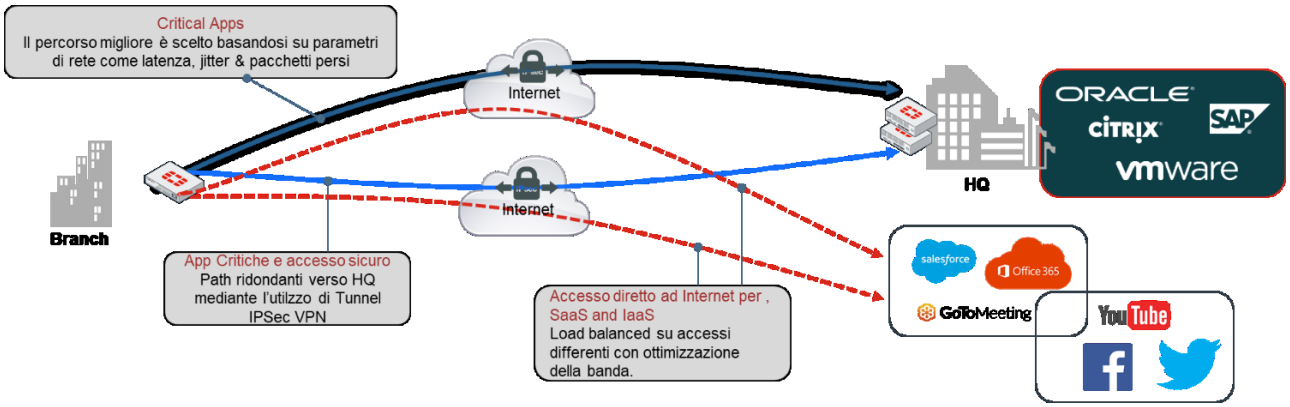
Senza SD-WAN:

- Sulla terminazione di rete del branch non vi è visibilità della tipologia di traffico e, pertanto, non vi sono i mezzi per ottimizzare l'utilizzo della banda;
- In caso di congestione del link non è possibile capire nel dettaglio quale utenza sta saturando la banda e se qualche applicazione sta avendo un comportamento anomalo in rete a meno di non implementare soluzioni di monitoraggio presenti, invece, di default su SD-WAN;
- In caso di accessi multipli Internet sull'hub non è possibile selezionare a priori il link da utilizzare in base alle metriche ed agli SLA impostati;
- Se si utilizza una CPE standard l'unica protezione del traffico potrebbe essere quella presente sul FW perimetrale della sede Master.

Con l'implementazione delle politiche SD-WAN è, invece, possibile:

- Selezionare a priori il link d'uscita del traffico in base agli SLA impostati;
- Avere una visibilità granulare del traffico che passa sulla rete;
- Usufruire delle funzionalità di sicurezza degli apparati FortiGate per aumentare la sicurezza della rete delocalizzando alcune funzionalità sui branch senza impattare i firewall perimetrali.

**Caso D:** Doppio link Internet




Rispetto ai casi precedenti i link geografici potrebbero essere sostituiti da link Internet in luogo dei link MPLS.

In questo caso il traffico INTRANET tra le sedi verrà gestito in Overlay mediante Tunnel IPSEC tra le sedi:

- In caso di traffico Hub&Spoke tra sede remota e CED il tunnel IPSEC saranno realizzati come Punto Punto tra il Fortigate della sede remota e il Fortigate della sede Master;
- In caso di traffico Any-to-Any si utilizzerà la funzionalità ADVPN con tunnel IPSEC dinamici on demand tra tutte le sedi.

L'accesso Internet locale potrà essere utilizzato per la creazione della componente Overlay e come local Internet Breakout per ottimizzare l'accesso ai servizi Pubblici.

**Caso E**: Link secondario su tecnologia radiomobile

Una variazione dei casi precedenti può essere rappresentata dall'utilizzo di un link radiomobile al posto di uno dei due accessi Internet. Le regole di implementazione non variano ma si avrà cura di impostare

una metrica di utilizza diversa tra il link radiomobile ed il link fisso in modo da influenzare la scelta dei percorsi in base alla disponibilità primaria del link fisso.

Su ciascuna delle connettività verrà creato un tunnel IPSEC verso l'hub, questi tunnel verranno gestiti utilizzando le logiche SDWAN.

Con SDWAN sarà possibile:

- Monitorare lo stato dei link ed utilizzare il percorso migliore su base SLA configurabili. In caso di degrado di uno dei percorsi il traffico verrà rediretto sul secondo link indipendentemente se sia fisso o radio;
- Creare shortcut IPSEC automatici tra i Branch in caso di traffico diretto;
- Utilizzare entrambe le connettività in bilanciamento secondo logiche applicative (Layer 4 IDB o Application Signatures Layer7).

# 4. Prodotti per l'accesso Wireless

## 4.1. Access Point per ambienti interni

### 4.1.1. Huawei AirEngine

# 5. Gruppi di continuità