



KUPNÍ SMLOUVA

Sít'ová infrastruktura

podle ustanovení § 2079 a násl. zákona č. 89/2012Sb., občanského zákoníku ve znění pozdějších předpisů (dále jen „OZ“), kterou níže uvedeného dne měsíce a roku uzavřeli:

České vysoké učení technické v Praze, Fakulta dopravní

Sídlo: Jugoslávských partyzánů 1580/3, 160 00 Praha 6 – Dejvice

Korespond. adresa: Konviktská 20, 110 00 Praha 1

IČO: 68407700

DIC: CZ 68407700

zastoupený ve věcech smluvních: prof. Ing. Ondřej Příbyl, Ph.D. - děkan

zastoupený ve věcech technických: [REDACTED], e-mail: [REDACTED], tel: [REDACTED],

mobil: [REDACTED]

Bankovní spojení: [REDACTED]

Číslo účtu: [REDACTED]

dále jen „kupující“

a

TECOM spol. s r.o.

Sídlo: Praha 10, Štěrboholská 1421/37, PSČ 10200

IČO: 41196856

DIC: CZ41196856

zápis v OR: u Městského soudu v Praze obchodní rejstřík oddíl C, vložka 3751

zastoupený ve věcech smluvních: Ing. Jaroslav Novotný, jednatel

zastoupený ve věcech technických: [REDACTED]

Bankovní spojení: [REDACTED]

Číslo účtu: [REDACTED]

dále jen „prodávající“

I. Předmět smlouvy

1. Prodávající se zavazuje odevzdat za podmínek v této smlouvě sjednaných kupujícímu předmět koupě specifikovaný v čl. II. této smlouvy a převést na něj vlastnické právo písemným protokolárním předáním zboží.
2. Kupující se zavazuje předmět koupě převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínech stanovených touto smlouvou a poskytnout prodávajícímu dohodnutou součinnost.
3. Podkladem pro uzavření smlouvy je nabídka prodávajícího předložená na veřejnou zakázku s názvem „Sít'ová infrastruktura pro FD ČVUT“, která byla zadána v otevřeném řízení dle § 3 písm. b) a § 56 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „ZZVZ“).

4. Zakázka je součástí projektu financovaného z prostředků Evropské unie v rámci Operačního programu Výzkum, vývoj a vzdělávání (OP VVV)
Název projektu: Infrastrukturní a laboratorní vybavení FD ČVUT
Registrační číslo projektu: CZ.02.2.67/0.0/0.0/16_016/0002482

II. Předmět koupě

1. Předmětem koupě je dodávka síťové infrastruktury (dále také jen „zboží“), která umožní přístup studentů k informačním zdrojům univerzity, zajistí pokrytí prostor WIFI signálem a posílí páteří infrastrukturu a kritické lokality na Fakultě dopravní. Síťová infrastruktura bude sestavena z následujících prvků:
- 1) Přístupové hlavní centrální prvky
 - a. Firewall
 - b. Propojovací prvek lokality 1
 - c. propojovací prvek lokality 2
 - 2) VPN koncentrátor včetně licencí
 - 3) Aktivní prvky přístupové infrastruktury
 - 4) Wifi kontrolér
 - 5) Access Pointy (AP)
 - 6) Software management

Bližší technická specifikace zboží je uvedena v Příloze č. 1 a č. 2 této smlouvy.

2. Všechny komponenty zboží budou nové (tj. nikoliv repasované apod.) a budou předány ve funkčním a bezvadném stavu, budou nepoužité, nezastavené, nezapůjčené, nezatížené leasingem nebo jinými právními vadami a nesmí porušovat práva třetích osob k patentu nebo k jiné formě duševního vlastnictví.
3. Součástí dodávky síťové infrastruktury jsou dále:
- a) dodávka veškerého příslušenství (zejména instalačního materiálu, kabelů apod.), které je nutné pro provoz a implementaci síťové infrastruktury;
 - b) doprava zboží do místa dodání;
 - c) montáž, instalace a konfigurace zboží, zprovoznění dodaného řešení a integrace/implementace systému do infrastruktury kupujícího;
 - d) zaškolení pracovníků (viz čl. V, bod 5 této smlouvy);
 - e) kompletní software, resp. licence potřebné pro provoz Síťové infrastruktury;
 - f) poskytnutí záruky za jakost, včetně záručního servisu a technické podpory v rozsahu dle čl. VII. této smlouvy a dále licencí a softwarových aktualizací dle Přílohy č. 1 té smlouvy, a to do 30.6.2023 (konec projektu) – dále jen „základní záruka a licence“
 - g) veškeré poplatky spojené s dovozem zboží, cla, daně, dovozní a vývozní přírážky, licenční a veškeré další poplatky spojené s dodávkou zboží až do jeho funkčního předání v místě plnění;
 - h) návody k obsluze všech dodaných zařízení, v českém, anglickém nebo slovenském jazyce v tištěné nebo elektronické podobě (na vhodném médiu), popř. předepsané doklady a certifikáty a dále dodací list;
 - i) zpráva/dokumentace popisující stav implementace;
 - j) oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.
4. Součástí předmětu plnění dle této smlouvy je dále poskytnutí záruky za jakost, včetně záručního servisu a technické podpory v rozsahu dle čl. VII. této smlouvy a dále licencí a softwarových aktualizací dle Přílohy č. 1 té smlouvy, a to od 1.7.2023 na dobu 36 měsíců (dále jen „rozšířená záruka a licence“).
5. Prodávající je při realizaci předmětu smlouvy povinen dodržet platné technické normy a ekologické požadavky a používat obaly šetrné k životnímu prostředí. Prodávající je povinen všechny obaly dodané spolu se zbožím odebírat zpět, tyto obaly vhodným způsobem recyklovat, případně znovu používat.

III. Kupní cena a platební podmínky

1. Kupní cena zboží dle této smlouvy (tj. kupní cena za dodávku síťové infrastruktury, včetně plnění dle čl. II., bod 3 této Smlouvy) činí celkem:

2.805.285,00 Kč bez DPH
589.109,85 Kč DPH ve výši 21%
3.394.394,85 Kč včetně DPH

Z čehož je kupní cena za

A. Přístupové hlavní centrální prvky	1.334.100,- Kč bez DPH
B. VPN koncentrátor včetně licencí	115.200,- Kč bez DPH
C. Aktivní prvky přístupové infrastruktury	445.900,- Kč bez DPH
D. Wifi kontrolér	326.925,- Kč bez DPH
E. Access Pointy (AP)	461.110,- Kč bez DPH
F. Software management	122.050,- Kč bez DPH

2. Cena za rozšířenou záruku a licence dle čl. II., bod 4 této smlouvy činí:

495 000,- Kč bez DPH
103 950,- Kč DPH ve výši 21%
598 950,- Kč včetně DPH

3. Kupní cena je stanovena dohodou smluvních stran jako cena pevná a nejvýše přípustná, která zahrnuje veškeré náklady prodávajícího spojené s plněním předmětu této smlouvy.
4. Kupní cena dle čl. III, bod. 1 této smlouvy bude uhrazena na základě daňového dokladu vystaveného prodávajícím po řádném dodání zboží. Daňový doklad musí být vystaven v měně CZK a v hodnotě odpovídající kupní ceně stanovené v čl. III., bod 1 této smlouvy. Ve faktuře musí být dále uvedeny všechny položky a jejich cena dle čl. III., bod 1 této smlouvy.
5. Cena za rozšířenou záruku a licence dle čl. III., bod. 2 této smlouvy bude hrazena postupně v poměrné výši (Cena dle čl. III. bod 2 této smlouvy přepočtena na měsíce) vždy na 12 kalendářních měsíců dopředu na základě daňového dokladu, který bude vystaven prodávajícím dne 31.5.2023 a dále vždy po uplynutí 12 kalendářních měsíců od vystavení předchozího daňového dokladu. Dnem uskutečnění zdanitelného plnění pro rozšířenou záruku a licence na prvních 12 měsících je den vystavení dokladu, a pro rozšířenou záruku a licence na každé další období den shodného měsíce a data s tímto dnem v příslušném následujícím kalendářním roce.
6. Splatnost daňových dokladů vystavených dle této smlouvy činí 30 kalendářních dní.
7. Daňový doklad musí obsahovat mimo náležitostí podle § 29 zákona o DPH dále tyto náležitosti:
 - a) IČO,
 - b) den splatnosti,
 - c) označení peněžního ústavu a číslo účtu, ve prospěch kterého má být provedena platba, konstantní a variabilní symbol,
 - d) odvolávka na smlouvu,
 - e) odvolávka na objednávku,
 - f) název a registrační číslo projektu (viz čl. I., bod 4. této smlouvy),
 - g) razítko a podpis osoby oprávněné k vystavení dílčího a konečného účetního dokladu,
 - h) soupis příloh.

Přílohou faktury za dodávku síťové infrastruktury musí být předávací protokol podepsaný oprávněnou osobou kupujícího.

8. V případě, že faktura nebude obsahovat výše uvedené náležitosti, je kupující oprávněn fakturu vrátit do doby její splatnosti způsobem, který prokazuje, že do tohoto data prodávající vrácenou fakturu

od kupujícího převzal. V takovém případě je prodávající povinen fakturu opravit a v případě, že by oprava činila fakturu nepřehlednou, vystavit fakturu novou. Opravená nebo nová faktura musí být znovu zaslána kupujícímu. Za doby splatnosti opravené nebo nové faktury není kupující v prodlení s placením ceny zboží.

9. Povinnost kupujícího zaplatit dohodnutou cenu je splněna dnem odepsání fakturované částky z bankovního účtu kupujícího.

IV. Doba a místo plnění

1. Prodávající se zavazuje dodat kupujícímu zboží nejpozději **do 3 měsíců** ode dne účinnosti této smlouvy.
2. Termín a přibližná hodina dodání zboží budou ze strany prodávajícího písemně sdělena kupujícímu alespoň 7 dnů před plánovaným dnem dodání zboží.
3. Místem dodání je: České vysoké učení technické v Praze, Fakulta dopravní:
 - Lokalita č. 1: Konviktská 20, Praha 1
 - Lokalita č. 2: Horská 3, Praha 2

V. Dodací podmínky a školení

1. Zboží je pokládáno za dodané po jeho odevzdání v místě plnění, instalaci, konfiguraci, integraci do infrastruktury kupujícího a podpisu předávacího protokolu.
2. Předávací protokol je za kupujícího oprávněn podepsat osoba jednající ve věcech technických nebo jím pověřený pracovník. Jedno vyhotovení předávacího protokolu si ponechá prodávající pro své potřeby a druhé vyhotovení zůstává kupujícímu.
3. V případě, že pracovník kupujícího odmítne předávací protokol podepsat nebo v případě, kdy vytčené vady zboží odmítne podepsat pracovník prodávajícího, je kupující povinen bez zbytečného odkladu tuto skutečnost prodávajícímu písemně oznámit.
4. Předávací protokol bude obsahovat alespoň tyto náležitosti:
 - a) Registrační čísla projektu;
 - b) Název veřejné zakázky;
 - c) popis předávaného zboží;
 - d) zhodnocení kvality předávaného zboží;
 - e) soupis případných vad zboží, rozhodne-li se kupující zboží převzít i s nimi;
 - f) dohodu o způsobu a termínu odstranění případných vad, přičemž nedojde-li k žádné dohodě platí, že všechny vady musí být odstraněny do 30 dnů od předání zboží;
 - g) výsledek přejímacího řízení, přičemž odmítne-li kupující zboží převzít, uvede do předávacího protokolu důvody pro takové odmítnutí;
 - h) podpisy zástupců obou smluvních stran, kteří dodání a převzetí zboží provedli.
5. **ZAŠKOLENÍ OBSLUHY:** Prodávající je povinen v rámci konfigurace zaškolit v dostatečném rozsahu pro bezpečné ovládání a základní údržbu zboží jeho obsluhu v počtu alespoň 3 osob – pracovníků kupujícího 3kolení bude provedeno na pracovišti kupujícího, a to u jednotlivých prvků v rozsahu dle přílohy č. 1 této smlouvy. V případě, že budou dodány jednotlivé prvky jiné než od výrobce HPE a CISCO, bude školení provedeno ve dvojnásobném počtu hodin.

VI. Součinnost smluvních stran

1. Smluvní strany jsou povinny vyvíjet veškeré úsilí k vytvoření potřebných podmínek pro realizaci předmětu smlouvy, které vyplývají z jejich smluvního postavení. To platí i v případech, kde to není výslovně uloženo v jednotlivých ustanoveních této smlouvy. Především jsou smluvní strany povinny vyvinout součinnost v rámci smlouvou upravených postupů a vyvinout potřebné úsilí, které lze na nich v souladu s pravidly poctivého obchodního styku požadovat, k řádnému splnění jejich smluvních povinností.
2. Pokud jsou kterékoli ze smluvních stran známy okolnosti, které jí brání, aby dostála svým smluvním

povinností, sdělí to neprodleně písemně druhé smluvní straně. Smluvní strany se zavazují neprodleně odstranit v rámci svých možností všechny okolnosti, které jsou na jejich straně a které brání splnění jejich smluvních povinností. Pokud k odstranění těchto okolností nedojde, je druhá smluvní strana oprávněna požadovat splnění povinnosti v náhradním termínu, který stanoví s přihlédnutím k povaze záležitosti.

3. Prodávající bude dle ustanovení § 2 písm. e) zák. č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění, osobou povinnou spolupůsobit při výkonu finanční kontroly. Zároveň se prodávající zavazuje k archivaci veškerých písemných dokladů týkajících se plnění předmětu koupě dle této smlouvy. Kupující je dále povinen poskytnout veškeré požadované informace, dokladovat svoji činnost, poskytovat veškerou dokumentaci vztahující se k projektu a umožnit vstup pověřeným osobám do svých objektů a na pozemky k ověřování podmínek plnění předmětu koupě dle této smlouvy. Prodávající se dále zavazuje dodržovat veškerá pravidla a podmínky vyplývající pro něj z pravidel pro poskytnutí dotace.
4. Prodávající je po celou dobu trvání smlouvy povinen splňovat všechny kvalifikační předpoklady bezprostředně související s realizací této smlouvy, které byly prokázány v předchozím zadávacím řízení uvedeném v čl. I, bod 3 této smlouvy. Prodávající je povinen předložit doklady prokazující splnění výše uvedených kvalifikačních předpokladů do 15 kalendářních dnů ode dne doručení písemné výzvy ze strany kupujícího.
5. Poddodavatelé:
 - 5.1. V příloze č. 2 této smlouvy (Seznam poddodavatelů) jsou specifikovány ty části předmětu plnění dle této smlouvy, které budou poskytovány poddodavateli prodávajícího.
 - 5.2. Změnu poddodavatele je prodávající oprávněn provést pouze se souhlasem kupujícího. Prodávající je povinen jakoukoliv změnu na pozici poddodavatele předem písemně oznámit kupujícímu. Nový poddodavatel nahrazující poddodavatele uvedeného v nabídce prodávajícího musí splňovat všechny kvalifikační předpoklady, a to v takovém rozsahu, ve kterém byly kupujícím požadovány v zadávací dokumentaci a které splňoval původní poddodavatel uvedený v nabídce prodávajícího. O těchto skutečnostech prodávající za nového poddodavatele doloží doklady o splnění jeho kvalifikačních předpokladů.

Kupující je povinen se ve lhůtě 7 pracovních dnů ode dne doručení písemného oznámení vyjádřit, zda změnu poddodavatele povoluje či nikoliv. Pokud prodávající předloží kupujícímu v rámci změny poddodavatele doklady požadované v tomto bodě smlouvy a kupující se nevyjádří ve stanovené lhůtě ke změně poddodavatele, má se za to, že kupující se změnou na pozici poddodavatele souhlasí.
 - 5.3. Prodávající je povinen vést a průběžně aktualizovat reálný seznam všech poddodavatelů podílejících se na realizaci této smlouvy. Tento přehled je povinen neprodleně, nejpozději do 7 kalendářních dnů ode dne doručení žádosti, předložit kupujícímu.

VII. Smluvní záruka, záruční servis a technická podpora

1. Prodávající poskytuje na zboží smluvní záruku, a to v období od dodání zboží do 30.6.2023 a dále od 1.7.2023 v délce 36 měsíců. Tato záruka se vztahuje na plnou funkčnost, kvalitu a kompletnost zboží.

Záruka, záruční servis a podpora dle tohoto čl. VII. smlouvy se nevztahuje na VPN koncentrátor, kdy u toho prvku je poskytnuta záruka za jakost dle OZ v délce 2 let od dodání. Tato záruka se vztahuje na plnou funkčnost, kvalitu a kompletnost zboží.
2. Záruční doba počíná běžet dnem protokolárního předání a převzetí zboží. Záruka se vztahuje na vady zboží, které se projeví u zboží během záruční doby s výjimkou vad, u nichž prodávající prokáže, že jejich vznik zavinil kupující. Záruční doba neběží po dobu, po kterou kupující nemůže užívat zboží pro jeho vady, za které odpovídá prodávající.
3. Prodávající se zavazuje, že zboží bude mít po dobu trvání záruční doby vlastnosti stanovené příslušnou dokumentací včetně jejich změn a doplňků, technickými normami, které se na jeho provedení vztahují, jinak vlastnosti a jakost odpovídající účelu smlouvy a přiměřenou zvláštnostem zboží, použité technologii a materiálu. Není-li stanoveno jinak, je prodávající odpovědný za vady plnění podle ustanovení OZ.
4. **Bezplatný záruční servis - NBD Exchange: týká se pouze položek**
 - Přístupové hlavní centrální prvky
 - Access Pointy (AP) - službu NBD Exchange lze nahradit dodáním záložních AP v počtu AP1-2k, AP2 a AP3 po jednom kuse

U výše uvedených položek bude poskytnut servis 24/7 na místě dodání s reakcí a odstraněním vady nejpozději následující pracovní den od nahlášení závady (tzv. next business day – NBD Exchange). Výměny vadných komponent je třeba provádět výhradně v místě instalace.

Bezplatný záruční servis zahrnuje bezplatnou opravu, případně výměnu vadných součástí či celého zboží, a to včetně veškerých nákladů spojených s opravou na místě, popřípadě dodáním opravených respektive nových dílů nebo zboží až do místa plnění. Při odstranění vady výměnou vadného dílu bude dodán vždy nový výrobek (tj. zejména nikoliv repasovaný). Vyměněný vadný díl dodavatel převezme a odstraní v souladu s právními předpisy. Záruční opravu či výměnu vadných komponent provede pracovník prodávajícího s odpovídající kvalifikací. Osvědčení o této kvalifikaci je prodávající povinen na požádání předložit kupujícímu.

5. V případě položek:
 - Aktivní prvky přístupové infrastruktury
 - Wifi kontrolér

je prodávající povinen v záruční době adekvátně reagovat na nahlášenou vadu ve lhůtě nejpozději do 5 kalendářních dní od nahlášení vady, a to dle potřeby buď telefonicky, e-mailem nebo osobní návštěvou technika prodávajícího. Lhůta pro odstranění vady nesmí být delší než 30 kalendářních dní. Tyto lhůty počínají plynout ode dne doručení písemné reklamace vady. V případě dodávky specifického náhradního dílu bude domluvena přiměřená lhůta pro odstranění závady.

6. TECHNICKÁ PODPORA – SUPPORT

Po dobu záruky bude kupujícímu poskytována TECHNICKÁ PODPORA – SUPPORT, a to přímo od výrobce daného zařízení. Technickou podporou se rozumí SW aktualizace dané části, dostupnost aktuální technické dokumentace k danému řešení a možnost obrátit se na specializované pracovníky prostřednictvím helpdesk portálu.

7. Práva a povinnosti z poskytnuté záruky nezanikají, ohledně kupujícímu předaného zboží, ani pro případ odstoupení jedné ze stran od smlouvy.
8. Nároky z odpovědnosti za vady se nedotýkají nároků na náhradu škody nebo na smluvní pokutu.

VIII. Nabytí vlastnického práva

1. Kupující nabyvá vlastnické právo k dodanému zboží jeho převzetím.

IX. Přechod nebezpečí škody na zboží

1. Nebezpečí škody na zboží přejde na kupujícího současně s nabytím vlastnického práva.

X. Smluvní pokuty

1. V případě, že bude prodávající v prodlení s řádným dodáním zboží je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,1 % z Kupní ceny dle čl. III, bod. 1 této smlouvy (včetně DPH), a to za každý, byť jen započatý den prodlení. V případě, že prodávající prokáže, že prodlení vzniklo z viny na straně kupujícího, zanikne kupujícímu právo smluvní pokutu uplatňovat.
2. V případě, že prodávající nedodrží lhůtu pro nástup na odstranění závad stanovenou v této smlouvě, je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z Kupní ceny dle čl. III, bod. 1 této smlouvy (včetně DPH), a to za každý, byť jen započatý den prodlení.
3. V případě, že prodávající nedodrží lhůtu pro odstranění závad stanovenou v této smlouvě, je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z Kupní ceny dle čl. III, bod. 1 této smlouvy (včetně DPH), a to za každý, byť jen započatý den prodlení.
4. V případě, že kupující bude v prodlení s úhradou kupní ceny za zboží je povinen zaplatit prodávajícímu úroky z prodlení ve výši 0,05 % z dlužné částky (včetně DPH), a to za každý, byť jen započatý den prodlení.

5. Zaplacením smluvní pokuty není dotčeno právo na náhradu škody, která vznikla smluvní straně požadující smluvní pokutu v příčinné souvislosti s porušením smlouvy, se kterým je splněna povinnost platit smluvní pokuty. Nárok kupujícího na náhradu škody, jakož i náhradu škody jsou smluvní strany oprávněny vymáhat kdykoli, a to bez ohledu na případné odstoupení kterékoli ze smluvních stran od smlouvy.

XI. Zánik závazků

Závazky smluvních stran ze smlouvy zanikají:

1. Splněním

Závazky smluvních stran ze smlouvy zanikají především jejich splněním.

2. Dohodou smluvních stran

Jednotlivé závazky smluvních stran, jakož i smlouva jako celek, mohou rovněž zaniknout, dohodnou-li se na tom smluvní strany formou písemného dodatku ke smlouvě. Takový dodatek musí být písemný a obsahovat vypořádání všech závazků, na které smluvní strany, které takový dodatek uzavírají, mohly pomyslet, jinak je neplatná.

3. Odstoupením od smlouvy

Kterákoli ze smluvních stran může odstoupit od smlouvy, poruší-li druhá strana podstatným způsobem své smluvní povinnosti, přestože byla na tuto skutečnost prokazatelným způsobem (doporučeným dopisem) upozorněna.

Stanoví-li oprávněná smluvní strana druhé smluvní straně pro splnění jejího závazku náhradní (dodatečnou) lhůtu, vzniká jí právo odstoupit od smlouvy až po marném uplynutí této lhůty, to neplatí, jestliže druhá smluvní strana v průběhu této lhůty prohlásí, že svůj závazek nesplní. V takovém případě může dotčená smluvní strana odstoupit od smlouvy i před uplynutím lhůty dodatečného plnění, poté, co prohlášení druhé smluvní strany obdržela.

Kupující má dále právo bez předchozího písemného upozornění od smlouvy odstoupit:

- a) při prodlení s dodáním zboží ze strany prodávajícího po dobu delší než 30 dnů; a nebo
- b) při zjištění, že parametry zboží neodpovídají požadavkům kupujícího stanoveným v zadávací dokumentaci nebo nabídce prodávajícího; a nebo
- c) při zjištění, že zboží, které je předmětem plnění není nové, je použité, zastavené, zapůjčené, zatížené leasingem nebo jinými právními vadami a porušuje práva třetích osob k patentu nebo k jiné formě duševního vlastnictví; a nebo
- d) v případě, že prodávající uvedl ve své nabídce podané v zadávacím řízení specifikovaném v čl. I bod 3. této smlouvy informace nebo doklady, které neodpovídají skutečnosti a měly nebo mohly mít vliv na výsledek zadávacího řízení; a nebo
- e) bude-li zahájeno insolvenční řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, v platném znění, jehož předmětem bude úpadek nebo hrozící úpadek prodávajícího, prodávající je povinen tuto skutečnost oznámit neprodleně, nejpozději do 7 dnů ode dne zahájení řízení kupujícímu; a
- f) v případě, že mu nebude udělena předem přislíbená dotace z OP VVV.

4. Následná nemožnost plnění

Závazek zaniká pro nemožnost plnění, stane-li se dluh po vzniku závazku nesplnitelným (§ 2006 a násl. občanského zákoníku).

5. Skončením účinnosti smlouvy nebo jejím zánikem

Skončením účinnosti smlouvy nebo jejím zánikem zanikají všechny závazky smluvních stran ze smlouvy. Skončením účinnosti smlouvy nebo jejím zánikem nezánikají nároky na náhradu škody, zaplacení smluvních pokut sjednaných pro případ porušení smluvních povinností, a ty závazky smluvních stran, které podle smlouvy nebo vzhledem ke své povaze mají trvat i nadále, nebo u kterých tak stanoví zákon.

XII. Závěrečná ustanovení

- 1.** Právní vztahy smluvních stran vzniklé z této smlouvy i právní vztahy smluvních stran v této smlouvě výslovně neupravené se řídí platnými předpisy České republiky. Zejména příslušnými ustanoveními OZ v platném znění.
- 2.** Smlouvu lze měnit pouze písemnými dodatky, podepsanými oprávněnými zástupci obou smluvních stran.
- 3.** Veškerá textová dokumentace, kterou při plnění smlouvy předává či předkládá prodávající kupujícímu, musí být předána či předložena v českém jazyce, popř. v anglickém nebo slovenském jazyce.
- 4.** Pro výpočet smluvní pokuty určené procentem a úroku z prodlení je rozhodná kupní cena včetně DPH.
- 5.** Proávající není oprávněn postoupit pohledávku plynoucí z této smlouvy třetí osobě bez předchozího písemného souhlasu kupujícího.
- 6.** Smluvní strany se ve smyslu ustanovení § 89a zákona č. 99/1963 Sb., občanský soudní řád, v platném znění dohodly, že místně příslušným soudem k projednávání a rozhodování sporů a jiných právních věcí, vyplývajících z této smlouvy založeného právního vztahu, jakož i ze vztahů s tímto vztahem souvisejících, je obecný soud kupujícího.
- 7.** Písemnosti mezi stranami této smlouvy, s jejichž obsahem je spojen vznik, změna nebo zánik práv a povinností upravených touto smlouvou (zejména odstoupení od smlouvy) se doručují do vlastních rukou. Povinnost smluvní strany doručit písemnost do vlastních rukou druhé smluvní straně je splněna při doručování poštou, jakmile pošta písemnost adresátovi do vlastních rukou doručí. Účinky doručení nastanou i tehdy, jestliže pošta písemnost smluvní straně vrátí jako nedoručitelnou a adresát svým jednáním doručení zmařil, nebo přijetí písemnosti odmítl.
- 8.** Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v informačním systému veřejné správy – Registru smluv.
- 9.** Kupující se zavazuje zajistit uveřejnění smlouvy prostřednictvím registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv, v platném znění (zákon o registru smluv).
- 10.** Kupující se zavazuje zaslat prodávajícímu potvrzení o uveřejnění smlouvy v Registru smluv. V případě, že do 15 dnů od podpisu smlouvy prodávající od kupujícího toto potvrzení neobdrží, zavazuje se prodávající kontaktovat kupujícího za účelem zjištění stavu věci.
- 11.** Smlouva je vyhotovena v jednom vyhotovení v elektronické podobě.
- 12.** Nedílnou součástí této smlouvy jsou následující přílohy:
 - 12.1 příloha č. 1: Požadavky zadavatele na předmět plnění
 - 12.2 příloha č. 2: Nabídka kupujícího – navržené technické řešení
 - 12.3 příloha č. 3: Seznam poddodavatelů

Kupující:

V Praze dne 27.2.2023

České vysoké učení technické v Praze
Fakulta dopravní
prof. Ing. Ondřej Příbyl, Ph.D. - děkan

Prodávající:

V Praze dne 23.2.2023

TECOM spol. s r.o.
Ing. Jaroslav Novotný, jednatel

Veřejná zakázka: „Sítová infrastruktura pro FD ČVUT“

Technická specifikace sítové infrastruktury

Poptávaná sítová infrastruktura se skládá z těchto prvků:

1. Přístupové hlavní centrální prvky
 - a. Firewall
 - b. Propojovací prvek lokality 1
 - c. propojovací prvek lokality 2
2. VPN koncentrátor včetně licencí (může být součástí firewallu 1a)
3. Aktivní prvky přístupové infrastruktury
4. Wifi kontrolér
5. Access Pointy (AP)
6. Software management

Obecné požadavky:

Ke všem dodaným prvkům a SW, bude v rámci dodání požadováno:

Dodání požadovaného HW, nebo SW dle technické specifikace. Poskytnutí záruky či podpory dle požadavků uvedených u jednotlivých sekcí. V rámci konfigurace bude uvedeno, zda je vyžadováno školení lokálních pracovníků a v jakém rozsahu. Vzhledem k aktuálním znalostem lokálních administrátorů bude u jiných značek, nežli HPE a CISCO, vyžadován dvojnásobný časový požadavek na školení a podporu nežli u výše uvedených značek.

Konfigurační (implementační) podpora bude vyžadována v místě instalace kvalifikovaným pracovníkem dle uvedené specifikace.

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)

Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce min. 36 měsíců.

Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

Součástí dodávky je montáž, instalace a konfigurace zboží, zprovoznění dodaného řešení a integrace/implementace systému do infrastruktury kupujícího.

V rámci implementace musí být dodána zpráva/dokumentace popisující tento stav implementace. Zpráva bude obsahovat seznam a popis implementovaných a dotčených entit. Dále souhrn konfiguračních nastavení, popis průběhu implementace a popis nezbytných úprav a opatření v současné infrastruktuře (pokud byly úpravy nutné).

1. Přístupové hlavní centrální prvky

Stručná specifikace:

V rámci dodávky je požadováno dodání jednoho hlavního přístupové bezpečnostního FW a dvou propojovacích prvků pro lokality dle požadavku (lokality jsou propojené skrze interní propojení vnitřní sítě ČVUT)

Technická specifikace:

a) U bezpečnostního FW centrální lokality vyžadujeme:

Technická specifikace:

Max velikost 2U, redundantní napájení. Možnost rozšíření na bezvýpadkový cluster ze 2 zařízení.

Požadavek na porty: min 4x 40GbE QSFP+, 12x RJ45 10/100/1000, 6x SFP

Požadavky na záruky, support, maintenance: Řešení musí obsahovat všechny HW komponenty a potřebné licence (subskripce) na dobu min. 36 měsíců.

Záruka NBD Exchange, a to do 30.6.2023 a dále min. 36 měsíců. Záruka obsahuje i technickou podporu výrobce.

Požadavky na školení: 8 hod

b) U propojovacího prvku lokality 1:

Technická specifikace:

Redundantní napájení, 48x GbE, 4xSFP+, 2xQSFP+, Air flow front to back s možností záměny na back to front, L2 a L3 funkce

Požadavky na záruky, support, maintenance: Záruka NBD Exchange, a to do 30.6.2023 a dále min. 36 měsíců. Záruka obsahuje i technickou podporu výrobce.

Požadavky na školení: 8 hod

c) U propojovacího prvku lokality 2:

Technická specifikace:

L2 funkce 48x GbE, 4xSFP+

Požadavky na záruky, support, maintenance: Záruka NBD Exchange, a to do 30.6.2023 a dále min. 36 měsíců. Záruka obsahuje i technickou podporu výrobce.

Požadavky na školení: 8 hod

A. FW

ZÁKLADNÍ TECHNICKÉ POŽADAVKY

- Požadujeme platformu postavenou na HW akcelерованé architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, akcelerace IPsec VPN, porovnávání se signaturovou databází, ...)
- Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 3 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
- Požadujeme dodání zařízení ve formátu HW appliance o velikosti 2U
- Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem.

- Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality
- Zařízení musí být vybavené redundantním napájecím zdrojem. Zdroje musí být vyměnitelné za provozu bez výpadku systému. Zdroje budou součástí dodávky, pokud nejsou integrované.
- Zařízení musí být dodáno v režimu vysoké dostupnosti. Bez výpadkový cluster bude sestaven celkem ze 2 zařízení – součástí dodávky musí být všechna zařízení včetně všech potřebných licencí.

HW parametry

- Počet síťových rozhraní copper, RJ45 10/100/1000 - min 14x
- Počet rozhraní 40 GE QSFP+– min 4x
- Počet rozhraní 25 GE SFP28 – min 4x
- Počet rozhraní GE SFP Slots– min 8x
- Dedikovaný konzolový port – min 1x
- Dedikovaný port pro komunikaci v režimu vysoké dostupnosti
- Dedikované porty pro správu – min 1x
- USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 1x

Výkonnostní parametry

- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 75 Gbps, 75 Gbps, 40 Gbps
- Latence firewallu (64 B UDP paket) - max 3 mikro sec
- Počet naráz otevřených spojení – min 7 800 000
- Počet nových spojení za sekundu - min. 450 000
- Počet firewall pravidel min 80 000
- Podpora virtualizace, min 200 oddělených kontextů
- Podpora funkce bezdrátový kontrolér – min 2000
- Zařízení musí obsahovat integrovaný výkonný disk pro ukládání logů, min 2 x 400 GB.

Networking a Vysoká dostupnost (HA)

- Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nody v clusteru
- HA musí podporovat až 4 nody v HA režimu
- Režim fungování L2 – transparentní režim, L3 – NAT/Router
- Podpora VLAN
- Podpora multicast, vytváření politiky pro multicast routování
- Podpora 802.3ad link aggregation
- Funkce Load Balancing – možnost rozdělování zátěže směřující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
- Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace
- Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
- Policy-based routing
- Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky)

- Zařízení musí podporovat možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN).
- Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízení komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti.
- Integrované SD-WAN řešení musí podporovat podle dokumentace výrobce min. 200 členů virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu.

UTM funkce

Funkce detekce aplikací na L7 (Application Control)

- detekce známých aplikací na základě signatur
- signaturový database automaticky aktualizované výrobcem
- alespoň 4 000 podporovaných aplikací
- pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci)
- možnost tvorby vlastních signatur
- detekované aplikace je možné: povolit, monitorovat, blokovat
- na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
- funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.

Funkce detekce a potlačení narušení (IPS/IDS)

- signatury automaticky aktualizované výrobcem
- alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
- možnost tvorby vlastních signatur
- funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
- funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu
- deklarovaná propustnost IPS inspekce min 12 Gbps

Funkce antivirové kontroly

- ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem
- signatury automaticky aktualizované výrobcem
- požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
- možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce
- deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 7 Gbps

- funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
- Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
- Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací.

Funkce kategorizace a blokace webových stránek

- založená na centrálně spravované databázi výrobce
- minimálně 50 filtračních kategorií
- možnost definice vlastních kategorií
- možnost definice vlastních seznamů zakázaných URL
- kategorizace musí zahrnovat i české a slovenské internetové stránky

Funkce blokování video obsahu portálu YouTube

- založená na centrálně spravované databázi výrobce
- minimálně 8 filtračních kategorií
- možnost definice vlastních kanálů na základě channel ID

Funkce DNS filtrování

- Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobně kategorie jako u předchozího bodu)
- Možnost definovat vlastní tzv. deny-list domén
- Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
- Možnost importu seznamu blokováných domén do DNS filtru
- Detekce a blokování komunikace do botnet sítí

Funkce ochrany před únikem citlivých informací (DLP)

- možnost analýzy běžných typů dokumentů a protokolů
- možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum

Funkce blokace stahování konkrétních typů souborů

- možnosti zablokovat stahování souborů s konkrétními typy, jako např. MSI, EXE...
- funkce blokace stahování konkrétních typů souborů se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.

Emailový antispamový modul

- jednoduchá antispamová a antivirová inspekce elektronické pošty

Podpora SSL dekrypce

- podpora SSL dekrypce a inspekce pro ochranu jak koncových zařízení, nebo serverů
- funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
- zařízení musí u SSL inspekce dosáhnout min. propustnost 9 Gbps

Podpora pravidel pro obranu proti útokům typu DoS

- zařízení musí umožnit uplatnit pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení.
- podpora detekce anomálií na 3. a 4. vrstvě
- podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION
- funkce musí umožňovat provoz nejen blokovat, ale i sledovat pro možnost orientace na síti

Explicitní proxy

- podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
- podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
- funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
- Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém server

Firewall

- Možnost nastavovat firewall politiku na základě geografických údajů
- Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
- Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
- Viditelnost do provozu na aplikační úrovni
- Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy
- Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filtering (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
- Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
- Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
- Podpora funkce reverzní proxy
- Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
- Administrátorské účty mohou být volitelně zabezpečeny pomocí dvou faktorového ověření

Multi-tenance (virtualizace)

- Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů atp.
- Součástí dodávky musí být licence na min. 200 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)

- Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)

Management

- FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
- Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
- Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

B. Lokalita1 - Přepínač L3

Routing / Switching	Layer 3 Advanced
Management	Fully Managed
Port Types	
LAN Ports	48 autosensing 10/100/1000 ports
SFP+ Ports	4 fixed 1000/10000 SFP+ ports
QSFP+ Ports	2 QSFP+ 40-GbE ports
Console Port	serial console port/ USB
Napájení	
Power supply slots	2 zdroje s plnou redundancí
Požadavek na chlazení	Front to back s možností výměny za back to Front
Memory and Processor	
Memory and Processor	Min 1 GB flash packet buffer size: min8 MB
Performance	
Switching Capacity	Min 300 Gbps
Routing Table Size	Min 10000 entries (IPv4), 7000 entries (IPv6)
MAC Address Table Size	min 100000 entries
Management	
Management	command-line interface, out-of-band management (RJ-45 Ethernet), SNMP Manager, Telnet, FTP, MNG SW

C. Lokalita 2

Přepínače L2

Požadavky na funkce a protokoly
Podpora "jumbo rámců" včetně velikosti 9198 Byte
Podpora linkové agregace IEEE 802.3ad
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4
Minimální počet LACP skupin/linek ve skupině: 4/4

Podpora VLAN podle IEEE 802.1Q, minimálně 128 aktivních VLAN
IEEE 802.1s - Multiple Spanning Tree
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
NTP pro IPv4 a IPv6 včetně MD5 autentizace
Statické směrování IPv4 a IPv6
IGMP v2 a v3
Hardware podpora IPv4 a IPv6 ACL
ACL definice na základě skupiny fyzických portů
ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
BPDU guard a Root guard
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps
ICMPv4 a ICMPv6 rate-limiting per port
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
Dynamické zařazování do VLAN
802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC
Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
Podpora IPv4 a IPv6 QoS
Minimálně 8 front pro IEEE 802.1p
Management
CLI formou USB Console Port
Konfigurace zařízení v člověku čitelné textové formě
Podpora automatických i manuálních snapshotů konfigurace systému
USB port pro diagnostiku, přenos konfigurace a firmware
Podpora managementu přes IPv4 i IPv6
Podpora SSHv2 server, HTTPS server a SFTP klient
Podpora kryptografických algoritmů SSH: AES256, HMAC-SHA2-256, DHG15 nebo vyšší
Podpora SNMPv2c a SNMPv3
RMON
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
Lokálně vynucené RBAC na úrovni přepínače
Dualní flash image
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování do více syslog serverů
Podpora Syslog over TLS
Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
Podpora RADIUS včetně RADIUS CoA (RFC3576)
Podpora RADIUS IPSec
Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
Analýza síťového provozu sFlow podle RFC 3176
Port mirroring (SPAN), alespoň 4 různé obousměrné session
Podpora Zero Touch Provisioning (ZTP)
REST API pro automatizaci nastavení

2. VPN koncentrátor včetně licencí

Požadujeme řešení s podporou připojení klientů do VPN pomocí proprietární SSL VPN.

Stručné požadavky:

Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS. Řešení musí mít možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření.

Tato funkce může být součástí bezpečnostního FW centrální lokality.

Požadavky na zaškolení: školení 4 hod

Požadavky na záruky, support, maintenance: Záruka 2 roky. Není požadováno NBD Exchange a technická podpora.

Funkce SSL VPN

- Nabízené řešení musí podporovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS.
- Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče.
- Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupná pro Android i iOS.
- Zařízení musí umožňovat rozšíření pro využití dostupného dvou faktorového ověření
- Vynucení ověření klientského certifikátu pro zvýšení zabezpečení.
- Minimální počet současně navázaných SSL VPN tunelů: 9 000
- Minimální propustnost SSL VPN: 8 Gbps

Funkce IPsec VPN

- podpora site-to-site VPN
- podpora klientských VPN
- dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek
- funkce klientských IPsec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence.
- Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 18 000
- Minimální počet klientských IPSEC VPN tunelů: 90 000
- propustnost IPsec VPN min. 45 Gbps (měřeno při AES256-SHA256)
- podpora konfigurace redundatních IPsec VPN tunelů za pomoci statického směrování
- podpora konfigurace redundatních IPsec VPN tunelů za pomoci dynamického směrování
- podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
- Podpora VXLAN
- Podpora L2TP, PPTP, GRE
- podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec

3. Aktivní prvky přístupové infrastruktury

Stručná specifikace:

V rámci dodávky bude požadováno dodání PoE Switchů:

4x 14x1GbE Port switch PoE, min 2x SFP+, maximální hloubka 26cm

1x 72x1GbE Port switch PoE, min 6x SFP+, maximální hloubka 32cm

5x 24x1GbE Port switch PoE, min 4x SFP+, maximální hloubka 32cm

3x 48x1GbE Port switch PoE, min 6x SFP+, maximální hloubka 32cm

S ohledem na prostor na umístění switchů je nutné dodržovat rozměry na maximální dle požadavku. V rámci nasazení switchů bude požadováno měření stávající kabeláže pro 1GbE minimálně kvalifikačním přístrojem včetně certifikátů. V rámci dodávky se předpokládá i případné drobné opravy na zakončení v patch panelu a zásuvkách v maximální míře 20% z celkového počtu koncových míst. Součástí není případná výměna vadné kabeláže.

Všechny switche musí možnost PoE na všech metalických portech a být plně managovatelné. Pro splnění počtu portů, je možné v rámci jednoho požadovaného switche dodat jeden blok splňující daný požadavek portů a technickou specifikaci.

Požadavky na záruky, support, maintenance: Záruka, a to do 30.6.2023 a dále min. 36 měsíců. (Není požadováno NBD Exchange). Záruka obsahuje i technickou podporu výrobce.

Požadavky na zaškolení: 8 hod

Technická specifikace:

Všechny switche stejného výrobce a stejné modelové řady. L2 switch, ve formátu pro rack, maximální velikost 1U, 10GE interface zpětně kompatibilní s 1Gbit/s transceivery, všechny porty dostupné ze předu, interní napájecí zdroj, Podpora PoE+ dle standardu 802.3at, PoE+ napájení dostupné na všech metalických portech, podpora Energy Efficient Ethernet (802.3az), Minimálně 12MB paketový buffer, 14 portový switch požadujeme bezventilátorový.

Požadavky na funkce a protokoly
Podpora "jumbo rámců" včetně velikosti 9198 Byte
Podpora linkové agregace IEEE 802.3ad
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4
Minimální počet LACP skupin/linek ve skupině: 4/4
Podpora VLAN podle IEEE 802.1Q, minimálně 128 aktivních VLAN
IEEE 802.1s - Multiple Spanning Tree
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
NTP pro IPv4 a IPv6 včetně MD5 autentizace
Statické směrování IPv4 a IPv6
IGMP v2 a v3
Hardware podpora IPv4 a IPv6 ACL
ACL definice na základě skupiny fyzických portů
ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN

BPDU guard a Root guard
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps
ICMPv4 a ICMPv6 rate-limiting per port
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
Dynamické zařazování do VLAN
802.1x volitelně bez omezení přístupu (pro monitoring a snadné nasazení)
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC
Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
Podpora IPv4 a IPv6 QoS
Minimálně 8 front pro IEEE 802.1p
Management
CLI formou USB Console Port
Konfigurace zařízení v člověku čitelné textové formě
Podpora automatických i manuálních snapshotů konfigurace systému
USB port pro diagnostiku, přenos konfigurace a firmware
Podpora managementu přes IPv4 i IPv6
Podpora SSHv2 server, HTTPS server a SFTP klient
Podpora kryptografických algoritmů SSH: AES256, HMAC-SHA2-256, DHG15 nebo vyšší
Podpora SNMPv2c a SNMPv3
RMON
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
Lokálně vynucené RBAC na úrovni přepínače
Dualní flash image
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování do více syslog serverů
Podpora Syslog over TLS
Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
Podpora RADIUS včetně RADIUS CoA (RFC3576)
Podpora RADIUS IPsec
Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
Analýza síťového provozu sFlow podle RFC 3176
Port mirroring (SPAN), alespoň 4 různé obousměrné session
Podpora Zero Touch Provisioning (ZTP)
REST API pro automatizaci nastavení
Automatická konfigurace portu podle připojeného zařízení
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů

4. Wifi kontrolér

Stručné požadavky:

V rámci dodávky je požadováno dodání Centrálního Wifi systému se správou skrze HW kontrolér.

Je požadován HW kontrolér (ne virtuální kontrolér) max velikost 1U, interní zdroj, Min 4x 1GbE-T, 2xSFP (možno combo s T), 2x 10Gbit SFP+

Možnost o rozšíření o další kontroléry do cluster módu

Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. Počet licencí je vyžadován na daný počet AP (uvedený v další části) s rezervou min 10 licencí.

S možností fungování AP i bez kontroléru (některá AP mohou fungovat v odlišných lokalitách bez možnosti napojení na kontrolér a musí fungovat jako propojený autonomní systém – např. pomocí virtuálního kontroléru).

Požadavky na záruky, support, maintenance: Záruka, a to do 30.6.2023 a dále min. 36 měsíců. (Není požadováno NBD Exchange). Záruka obsahuje i technickou podporu výrobce.

Požadavky na zaškolení: 8 hod

Technická specifikace:

Podpora standardu 802.11ax, a zpětná kompatibilita s 802.11a/b/g/n/ac
Minimální podporovaný počet AP bez nutnosti přidávání hardware: 256 AP
Minimální počet současně připojených klientů: 8 000
Minimální výkon statefull firewallu: 12 Gbit/s, 1mil. Session
Sdílení licencí mezi více kontrolery
Podpora Redundance (HA) kontrolerů v režimech: active-active a active-standby. Výpadek aktivního kontroleru v redundantním páru nemá dopad na provoz již připojených klientů (tj. bez potřeby opětovné autentizace)
Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP, podpora roamingu přes AP na vzdálené lokalitě
Režimy přenosu uživatelských dat: tunelování přes kontrolér a lokální AP bridging
Autentizace AP ke kontroleru pomocí certifikátu
Podpora minimálně 4000 aktivních VLAN podle IEEE 802.1Q
Minimální počet záznamů v tabulce MAC adres: 32 000
Podpora linkové agregace IEEE 802.3ad
IEEE 802.1w - Rapid spanning Tree
Podpora STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
Detekce protilehlého zařízení LLDP
Statické směrování IPv4 a IPv6
Dynamické směrování OSPFv2 včetně podpory stub a NSSA
Podpora Multicast: IGMP a MLD
DHCP server pro IPv4 a IPv6
NTP klient pro IPv4 a IPv6 včetně MD5 autentizace
Podpora překladu adres PAT/NAT
VLAN Pooling
Podpora IPv6: konfigurace, správa (SSH, SNMP, Syslog, DHCPv6, RADIUS, PING), IPv6 Extension Header (EH) Filtering, syst. komunikace mezi AP a kontrolérem. Kompatibilita s RFC 2460, RFC 3162, RFC 3736, RFC 6106
Typy autentizace: WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace, "captive portal", 802.1X ověření s následným ověřením MAC
Typy autentizace: Enhanced Open (OWE), SAE (Simultaneous Authentication of Equals), WPA3 Enterprise Basic, WPA3-Enterprise SuiteB
Autentizace sdíleným klíčem s možností definovat několik různých PSK na jednom SSID (např. Identity PSK)
Podporované autentizační/autorizační zdroje: RADIUS, LDAP, RFC 3576 Change of Authorization

Funkce řízení a ochrany rádiového spektra s automatickou optimalizací sítě (přidělování kanálů, fast roaming, rozdělení klientů na jednotlivá AP)
Aktivní scanování 802.11 kanálů pro výběr nejlepšího včetně automatického zastavení scanování v případě že probíhá časově senzitivní provoz (např. VoIP)
Klasifikace klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu
Vestavěný "captive portal" pro hosty s podporou nativních IPv6 klientů. s možností úpravy vzhledu a přidáním vlastního loga s, včetně vestavěného rozhraní pro vytváření dočasných guest účtů
Podpora pro 802.11u, 802.11v a 802.11k
Automatické dynamické rozpoznání a prioritizace hlasových protokolů jako SIP, SCCP, VOCERA a SVP pomocí funkce DPI a jejich SLA monitoring
Podporované úrovně oprávnění administrátorů: administrator, read-only, guest-provisioning
Podpora RestAPI pro automatizovanou konfiguraci kontroléru
Automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu
Grafický uživatelský dashboard zobrazující kvalitu a obsazenost kanálů, jednotlivé klienty, náhledy na VoIP přes WiFi síť a zobrazující informace o MOS (mean opinion score) aktivních hovorů. Možnost realtime analýzy kvality prováděných hovorů
Podpora rozpoznávání aplikací na 7. vrstvě (aplikace typu: Youtube, Facebook, Dropbox, BitTorrent, Skype, Office365, apod.). Možnost jejich povolování, zakazování, prioritizace nebo omezení s možností vytvořit minimálně 20 souběžných aplikačních pravidel k omezení provozu konkrétních aplikací.
Centrální správa, aktualizace, konfigurace vč. bezpečnostních politik a QoS profilů pro všechna AP
Blacklist zařízení překračující nastavitelné prahy (opakovaná špatná autentizace, porušení bezpečnostní politiky)
Podpora RadSec (RADIUS over TLS)
Podpora Radius Accounting, roaming klienta mezi AP vyvolá Interim Update
Podpora tvorby bezpečnostních politik na základě časových pravidel
Podpora Bonjour services gateway, zpracování mDNS paketů, možnost filtrování služeb mezi subnety
Podpora L2 a L3 roaming bez nutnosti speciálního SW na klientovi
Podpora bezdrátových MESH sítí s protokolem pro výběr optimální cesty v rámci MESH stromu, podporovaná hloubka min. 8 hopů
Podpora Rogue Wireless detekce a containment
Podpora PKI
Možnost licenčního rozšíření o funkci VPN koncentrátor (SSL a IPsec VPN klienti)
Ochrana řídicích rámců - 802.11w
Rozšiřitelnost o web content filtering (URL, kategorie, reputace) vykonávaný kontrolerem
Management
CLI formou RJ45 serial konsole port
Ethernet port pro out-of-band management
USB port pro přenos konfigurace a firmware
Dual boot flash
Podpora SSHv2, SCP a HTTPS web GUI
SNMPv2c, SNMPv3
Podpora SYSLOG s možností různé úrovně logování do více syslog serverů
Podpora příjmu a filtrování zpráv z externího SYSLOGu (např. Firewall, IPS) s možností reakce na vybrané zprávy formou ACL nebo Blacklistu WiFi klienta
Podpora monitorování síťového provozu pomocí IPFIX
Integrované diagnostické nástroje: ping, traceroute, AAA test
Nástroj pro odchyťování WLAN datového provozu včetně 802.11 hlaviček a možnost jeho zaslání do Ethernetového analyzátoru
Podpora upgrade firmware pomocí: HTTPS, TFTP, FTP a USB
Plná kompatibilita s nabízenými přístupovými body

5. Access Point (AP)

Stručné požadavky:

Všechny AP s podporou Wi-Fi 6. Součástí každého AP musí být montážní kit na zeď. Min 50% AP musí mít externí napájecí adaptér (50% je myšleno od každého typu, pokud jsou napáječe rozdílné)

Vzhledem k nedostatku kabeláže je u většiny vyžadováno AP s integrovaným switchem s minimem počtem portů 4x RJ45 pro připojení dalších zařízení.

Počty AP

AP1 - 28x AP s min 4x 1GbE připojení RJ45 pro připojení dalších zařízení,

AP2 - 8x AP s min 1x 1GbE připojení RJ45 pro připojení dalších zařízení,

AP3 – 4x AP bez nutnosti připojení dalších zařízení

Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.

Požadavky na záruky, support, maintenance:

Požadavky na záruky, support, maintenance: Záruka NBD Exchange, a to do 30.6.2023 a dále min. 36 měsíců. Záruka obsahuje i technickou podporu výrobce.

– službu Exchange lze nahradit dodáním záložních AP v počtu AP1-2k, AP2 a AP3 po jednom kuse.

Požadavky na zaškolení: 6 hod

Technická specifikace:

AP1

- Datový tok min 1000Mbit/s pro 5GHz, 570Mbit/s pro 2,4GHz
- Min počet ethernet portů 5 (4 pro další zařízení) 100/1000 Mbit/s RJ45

AP2

- Datový tok min 1000Mbit/s pro 5GHz, 570Mbit/s pro 2,4GHz
- Min počet ethernet portů 1 (1 pro další zařízení) 100/1000 Mbit/s RJ45

AP3

- Datový tok min 4500Mbit/s pro 5GHz, 570Mbit/s pro 2,4GHz

Společné požadavky na všechny AP

Požadavek na funkcionalitu
Indoor přístupový bod
Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax
Certifikace Wi-Fi Alliance: Wi-Fi CERTIFIED 6™ a WPA3™-Enterprise
Podpora napájení z AC napájecího zdroje
Rozsah provozních teplot 0° až +50°C bez nutnosti redukce výkonu nebo omezení funkcí
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz
Možnost nastavení vysílacího výkonu
Minimálně 15 inzerovaných BSSID na rádio
Nastavitelný DTIM interval pro jednotlivé SSID

Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP
Integrovaný TPM pro bezpečné uložení certifikátů
Podpora WPA3-CNSA, WPA3-SAE, OWE
Podpora 802.11ac explicitního beamformingu
Podpora airtime fairness
Prioritizace jednotlivých SSID na základě vysílacího času
Vypínatelné indikační LED diody informující o stavu zařízení
Prioritizace 5GHz pásma – Band Steering či obdobné
Automatická detekce Rogue AP
Mapování SSID do různých VLAN podle IEEE 802.1Q
VLAN Pooling
Podpora Wireless MESH s protokolem pro optimální výběr cesty v rámci MESH stromu
Podpora Layer-2 izolace bezdrátových klientů
Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu)
Hardware filtry pro filtraci intermodulačního rušení pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček
DHCP server, směrování a NAT pro bezdrátové klienty
AP v režimu IPsec VPN klient s možností tvorby L2 či L3 VPN
CLI formou serial konsole port
Automatická identifikace připojeného zařízení a jeho operačního systému
Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP
Optimalizace provozu: multicast-to-unicast konverze
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)
Podpora filtrování přístupu na web
Podpora RadSec (RADIUS over TLS)
802.11w ochrana management rámců
Podpora MAC a 802.1X autentizace Wi-Fi klientů s využitím lokální databáze v AP
AP se ověřuje před připojením do LAN pomocí 802.1X - podpora PEAP a EAP-TLS suplicant
Volitelně možnost spravovat AP cloud management nástrojem
SSHv2, SNMPv2c a SNMPv3

6. Software management

Stručné požadavky:

V rámci dodávky požadujeme dodání pro správu Wifi prostředí a správu stávající sítě infrastruktury skládající se z prvků Cisco a HPE (Comware)

Sw může být v rámci jednoho řešení, případně 2 s oddělením Wifi řešení a sítě infrastruktury

- A. SW pro dohled WiFi infrastruktury včetně licencí (počet licencí dle počtu wifi zařízení + 10 navíc jako rezerva)

- B. Management nástroj pro správu sítě s podporou správy stávajících produktů Cisco a HP (Comware) a nově dodávaných zařízení mimo WiFi zařízení pro min 10 zařízení s možností rozšíření min do 1000 zařízení

Požadavky na zaškolení: 6 hod

Technická specifikace:

- A. SW pro dohled Wifi
SW pro dohled WiFi infrastruktury včetně licencí (počet licencí dle počtu wifi zařízení + 10 navíc jako rezerva)

Management nástroj pro správu WiFi sítě s podporou správy produktů výrobce a kompatibilní s nabízenými AP a kontrolérem
Virtuální appliance (OVA formát) bez nutnosti pořizovat další licence např. pro OS nebo databáze.
Správa prvků: přístupových bodů, WiFi kontrolerů a přepínačů
Licence pro správu všech bezdrátových prvků, možnost flexibilního rozšiřování až do min 1000 zařízení.
Manuální a automatické discovery síťových zařízení pomocí SNMP, HTTP a CDP skenování.
Monitorovací nebo plný-managed režim pro nově objevená zařízení jako ochrana před nechtěným přepsáním konfigurace.
Role pro jednotlivé síťové operátory na úrovni síťových zařízení a jejich funkcí.
Webové uživatelské rozhraní s podporou HTTPS
Real-time monitoring každého uživatele v síti včetně charakteristik jako jsou: kvalita RF signálu, utilizace pásma (in/out), autentizační status a čas, historie roamingu, délka trvání připojení, typ klientského zařízení, asociace s SSID, objem a seznam používaných L7 aplikací a navštívených webových kategorií.
Vyhledávání koncových uživatelů na základě MAC adresy, IP adresy, uživatelského jména a LAN hostname.
Konfigurace formu politik aplikovatelných na všechna zařízení, jejich skupinu nebo jednotlivé zařízení.
Tvorba konfiguračních šablon: jak nových tak z běžících zařízení
Podpora konfigurační změn a upgrade firmware pomocí jednorázových nebo opakujících se pracovních úloh (scheduled-job).
Archivace konfigurací
Audit konfigurace, porovnávání rozdílů proti přednastaveným politikám individuálně pro jednotlivá a hromadně proti skupině zařízení. V případě nesouladu definice a runtime stavu konfigurační rollback.
Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel.
Podpora alarmování s možností nastavitelných prahů pro jednotlivé události. Podporované události: odchylka od baseline konfigurace, RF metrika, nově objevené zařízení, Radius autentizace, Rogue AP, nadměrné utilizace AP (bandwidth), počet připojených klientů, nadměrná utilizace klientem (bandwidth), Up/Down zařízení, Up/Down Radio, IDS událost.
Možnost monitorování stability a odezvy ostatních síťových služeb pro jednotlivé klienty jako je průměrný čas odpovědi DHCP, DNS či čas zpracování RADIUS autentizace.
Vytváření reportů v PDF formátech reportující různé přehledové statistiky o využití sítě a jejím stavu. Automatizované pravidelné zaslání reportů mailem.

- B. SW pro dohled síťové infrastruktury

Management nástroj pro správu sítě s podporou správy stávajících produktů Cisco a HP (Comware) a nově dodávaných zařízení mimo WiFi zařízení.

- Správa minimálně 100 síťových zařízení (např. přepínačů, routerů), možnost flexibilního rozšiřování min do 1000
- Manuální a automatické discovery síťových zařízení

- Možnost tvorby SNMP, TELNET a SSH šablon pro hromadný přístup k zařízením
- Definice přístupových práv pro jednotlivé operátory na úrovni síťových zařízení a jejich funkcí
- Možnost přizpůsobení prostředí ovládací obrazovky (např. pomocí widgetů), zvlášť pro každého síťového operátora
- Vizualizace topologie: Layer-2, Layer-3 a spanning tree, možnost tvorby vlastních hierarchických pohledů
- Vizualizace datového centra: DC, místnosti, racky, osazení včetně hledání
- Správa a vizualizace virtuálních sítí v hypervisorech VMware, Hyper-V a Linux KVM pro přehled spojení virtuální a fyzické infrastruktury
- Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel
- Performance management síťových zařízení: dostupnost zařízení i linek, vytížení procesoru, využití operační paměti, vytížení linek
- Performance management pro libovolné SNMP statistiky, dlouhodobou historii i real-time grafy obnovované už od každých 5 sekund
- Importování vlastních MIB a kompilátor
- Podpora SYSLOG
- VLAN management: změna nastavení, přidávání, přiřazení portů
- ACL management: ACL šablony, optimalizační nástroje, zálohování a deployment
- Alarmování, práce se syslog a SNMP trapy včetně vytváření vlastních reakcí na události nebo notifikace ve formě emailu či SMS.
- Korelace alarmů formou sumarizace počtů shodných událostí, jejich příčin (root cause) a následků (child alarms).
- Audit zařízení: typ zařízení včetně jednotlivých komponent, verze operačního systému, sériová čísla, informace o jednotlivých portech, historický audit jednotlivých zařízení (např. přesuny)
- Vyhledávání a historie zařízení na základě MAC, IP nebo názvu
- Bezpečnostní systém analýzy logů s možností integrace IDS/IPS systému schopný dohledat krajní port útočníka a izolovat
- Vestavěné RESTful API s možností volání libovolné funkce aplikace pro možnost integrace do aplikací třetích stran.
- Podpora konfigurace VXLAN a EVPN.
- Možnost rozšíření zásuvnými moduly o funkce RADIUS, NAC, TACACS+ a správa SLA
- Všechny zásuvné moduly musí umožňovat centrální řízení z jedné aplikace
- Podpora vysoké dostupnosti software, možnost běhu v clusteru.

Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 36 měsíců.

Je požadovaná přímá technická podpora výrobce po dobu min. 36 měsíců.

Veřejná zakázka: „Sítová infrastruktura pro FD ČVUT“

Technická specifikace nabízené sítové infrastruktury

Struktura dokumentu odpovídá struktuře dokumentu ze zadání „3492427-3. Technická specifikace_SI“

Nabízená sítová infrastruktura se skládá z těchto prvků:

1. Přístupové hlavní centrální prvky
 - a. Firewall
 - b. Propojovací prvek lokality 1
 - c. propojovací prvek lokality 2
2. VPN koncentrátor včetně licencí (může být součástí firewallu 1a)
3. Aktivní prvky přístupové infrastruktury
4. Wifi kontrolér
5. Access Pointy (AP)
6. Software management

Splnění obecných požadavků:

V rámci nabídky je nabízen HW a SW dle technické specifikace.

V rámci celé dodávky jsou nabízeny výrobky 2 výrobců.

1. HPE
2. Fortinet

V rámci školení pracovníků bude tedy v rámci nabídky poskytnuto školení pracovní dle požadavku. Jelikož je v rámci nabídky nabízena u FW a VPN koncentrátoru (1a a 2) jiná značka nežli HPE a Cisco (Fortinet), bude součástí dodávky školení ve dvojnásobné délce, nežli je v požadavcích.

Konfigurační (implementační) podpora bude poskytnuta v místě instalace kvalifikovaným pracovníkem dle uvedené specifikace.

Hardware bude dodán zcela nový, plně funkční a kompletní (včetně příslušenství).

Součástí dodávky jsou veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.

V rámci dodávky bude doloženo oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních včetně sériových čísel dodávaných zařízení. Všechny zařízení jsou určeny pro český trh.

Součástí dodávky je montáž, instalace a konfigurace zboží, zprovoznění dodaného řešení a integrace/implementace systému do infrastruktury kupujícího.

V rámci implementace bude dodána i zpráva popisující tento stav po implementaci. Zpráva bude obsahovat seznam a popis implementovaných a dotčených entit. Dále souhrn konfiguračních nastavení, popis průběhu implementace a popis nezbytných úprav a opatření v současné infrastruktuře (pokud budou úpravy nutné).

1. Přístupové hlavní centrální prvky

Stručný popis nabízeného řešení :

V rámci dodávky je nabízena dodávka jednoho hlavního přístupové bezpečnostního FW a dvou switchů pro jednotlivé lokality dle požadavku.

Nabízené prvky v rámci nabídky a stručná technická specifikace dle přímých požadavků:

a) Bezpečnostního FW centrální lokality:

V rámci nabídky nabízíme enterprise řešení od výrobce Fortinet

Nabízený model:

výrobce FORTINET

1x FG-1100E FortiGate 1100E

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložený datový list „fortigate-1100e-series.pdf“

Záruky, support, maintenance: Záruka NBD Exchange do 31.7.2026. Unified Threat Protection 36 měsíců. Záruka obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 16 hod

b) Propojovacího prvek lokality 1:

v rámci nabídky nabízíme jednu z nejvyšších řad switche od výrobce HPE s redundantními zdroji a vyměnitelnými moduly chlazení s možností změny směru proudění vzduchu dle potřeby serverovny.

Nabízené modely:

výrobce HPE

1x JL864A HPE 5901AF 48G 4XG 2QSFP+ Switch + příslušenství

2x JD362B HPE X361 150W AC Power Supply

2x JL837A HPE 5944 Prt2Pwr Fan Module

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložený datový list „HPE-FlexFabric-5900-Switch-Series-Datasheet.pdf“

Záruky, support, maintenance: Záruka NBD EXCHANGE do 31.7.2026. Záruka obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 8 hod

c) U propojovacího prvku lokality 2:

Nabízíme model ze stejné řady, jako u aktivních prvků

Nabízený model:

výrobce HPE

1x JL675A Aruba 6100 48G CL4 4SFP+ Switch

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložený datový list „DS_6100Series.pdf“

Záruky, support, maintenance: Záruka „limited lifetime“ NBD Exchange min 60 měsíců. Záruka obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 8 hod

2. VPN koncentrátor včetně licencí

Nabízíme řešení splňující požadavky, které je rozšířenou součástí Firewallu.

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložený datový list „fortigate-1100e-series.pdf“.

Záruky, support, maintenance: Stejně jako u FW v části 1a - FG-1100E

Školení v rámci dodávky: 8 hod

3. Aktivní prvky přístupové infrastruktury

Nabízíme switche Aruba 61xx řady splňující požadavky zadání. V rámci požadavku na 1 switch „72x1GbE Port switch PoE, min 6x SFP+, maximální hloubka 32cm“ nabízíme blok 2 switchů 1x24x1GbE(JL677A) a + 1x48x1GbE(JL675A). Dále místo „3x 48x1GbE Port switch PoE, min 6x SFP+, maximální hloubka 32cm“ 3x2x24x1GbE, tedy 6x JL677A. Součástí je jejich propojení.

Nabízené modely

výrobce HPE

4x JL679A Aruba 6100 12G CL4 2SFP+ PoE Switch
12x JL677A Aruba 6100 24G CL4 4SFP+ PoE Switch
1x JL675A Aruba 6100 48G CL4 4SFP+ PoE Switch

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložený list „DS_6100Series.pdf“.

Záruky, support, maintenance: Záruka „limited lifetime“ NBD Exchange min 60 měsíců. Záruka obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 8 hod

4. Wifi kontrolér

V rámci celého nabízené řešení nabízíme kompletně vše na HPE Aruba řešení.

Nabízený model:

výrobce HPE

1x JW735A Aruba 7205 (RW) Controller

Součástí je i dodávka montážního kitu do racku.

V rámci dodávky jsou potřebné licence pro 55 zařízení.

Tedy licence **JW472AAE+ JW473AAE**

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložený datový list „DS_7200Series.pdf“

Záruky, support, maintenance: Záruka NBD Exchange do 31.7.2026. Záruka obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 8 hod

5. Access Point (AP)

V rámci celého nabízené řešení nabízíme kompletně vše na HPE Aruba řešení.

V rámci dodávky nabízíme tyto AP, které splňují požadované parametry.

I když mají AP záruku dle požadavku, nabízíme navýšené množství, dle varianty o alternativě záruk. Součástí je wall mount KIT pro všechny AP. U varianty s integrovaným switchem je k dispozici i desk mount kit. Součástí je i dodávka požadovaného počtu zdrojů pro jednotlivé druhy AP.

Nabízíme tyto AP v tomto počtu:

AP1 - 30x R3V56A Aruba AP-505HR (EU) Remote AP Bundle

AP2 - 9x R2H28A Aruba AP-505 (RW) Unified AP

AP3 - 5x Q9H62A Aruba AP-515 (RW) Unified AP

Technická specifikace:

Splňuje požadavky zadávací dokumentace, viz příložené datové listy

„DS_AP500HSeries.pdf“, „DS_AP500Series.pdf“, „DS_AP510Series.pdf“

Záruky, support, maintenance: Záruka „limited lifetime“ NBD Exchange min 60 měsíců. Záruka obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 6 hod

6. Software management

V rámci nabídky nabízíme 2 SW pro požadovaný management.

- A. Pro dohled na wifi SW HPE AirWave
- B. Pro dohled síťové infrastruktury IMC - HPE Intelligent Management Center

Konkrétní nabízené produkty včetně potřebných licencí jsou tyto:

- A. U SW AirWave jsou potřebné pouze licence pro daný počet zařízení. Součástí nabídky jsou tedy pouze licence potřebné pro daný počet zařízení. Volili jsem větší rezervu, nežli je požadována. Součástí je celkem 55 licencí, pro 55 zařízení.

Konkrétně nabízený produkt:

55x JW546AAE Aruba AirWave 1 Device Lic E-LTU

- B. U SW IMC, jsou součástí nabídky licence pro požadovaný počet 100 zařízení.

V rámci nabídky jsou tedy součástí:

1x JG747AAE HPE IMC Std SW Plat w / 50-node E-LTU

1x JG749AAE HPE IMC Std and Ent Add 50-node E-LTU

Technická specifikace:

- A. Splňuje požadavky zadávací dokumentace, viz příložený datový list „DS_AW.pdf“
- B. Splňuje požadavky zadávací dokumentace, viz příložené datové listy „HPE Intelligent Management Center Standard Software Platform-c04111576.pdf“, „HPE IMC Standard Software Platform with 50-node E-LTU-PSN5443908CZEN.pdf“

Záruky, support, maintenance: Záruka NBD Exchange do 31.7.2026. Obsahuje i technickou podporu výrobce.

Školení v rámci dodávky: 6 hod

DATA SHEET

ARUBA CX 6100 SWITCH
SERIES

PRODUCT OVERVIEW

The Aruba CX 6100 Switch Series is modern family of entry level access switches ideal for enterprise branch offices and SMB networks. Optimized for reliable, simple and secure access, the CX 6100 switches provide a convenient wired access solution for networks supporting IoT, mobile and cloud applications.

The CX 6100 series is based on the Aruba ASIC architecture with the programmable AOS-CX operating system used across the entire Aruba CX portfolio for a more consistent, more efficient operator experience. This fully managed layer 2 switch series has convenient built-in high speed uplinks with up to 370W of PoE to support IoT devices such as security cameras and wireless APs, and includes a compact and fanless model ideal for use in quiet work spaces.

The CX 6100 supports management choices that include Web GUI, CLI, cloud-based and on-premise Aruba Central, so you can choose the best fit for your needs today with flexibility to change without replacing hardware. With enhanced access security, traffic prioritization, and IPv6 support, the CX 6100 also simplifies ownership and brings peace of mind with no switch software licensing and a Limited Lifetime Warranty.

PRODUCT DIFFERENTIATORS

AOS-CX - a modern software system

The Aruba CX 6100 Switch Series is based on AOS-CX, a modern, database-driven operating system that is built on a modular Linux architecture. This operating system provides the following unique capabilities:

- Easy access to all network configuration state information
- REST APIs for fine-grained programmability of network tasks
- A micro-services architecture that enables full integration with other workflow systems and services



KEY FEATURES

- Enterprise-class Layer 2 connectivity with support for ACLs, robust QoS and static routing
 - Convenient built-in 1/10GbE uplinks and up to 370W of Class 4 PoE for support of IoT devices
 - Compact and fanless 12 port model for quiet deployment
 - Management flexibility with support for Aruba Central, easy-to-use Web GUI, CLI, and Aruba NetEdit
 - Simple deployment with Zero Touch Provisioning
 - Software defined ready with REST APIs
 - Simplify adds, moves and changes with colorless ports
- All software processes communicate with the database rather than each other, ensuring near real-time state and resiliency

Aruba ASICs - programmable innovation

Based on over 30 years of continuous investment, Aruba's ASICs create the basis for innovative and agile software feature advancements, unparalleled performance and deep visibility. These programmable ASICs are purpose-built to allow for a tighter integration of switch hardware and software within campus and data center architectures to optimize performance and capacity. The Aruba CX 6100 is based on the Aruba ASIC architecture.



Aruba Central - unified single pane of glass management

Flexible cloud-based or on-premises management for unified network operations of wired, WLAN, SD-WAN, and public cloud infrastructure. Designed to simplify day zero through day two operations with streamlined workflows. Switch management capabilities include configuration, onboarding, monitoring, troubleshooting, and reporting.

Aruba NetEdit – automated switch configuration and management

The entire Aruba CX portfolio empowers IT teams to orchestrate multiple switch configuration changes for smooth end-to-end service rollouts. Aruba NetEdit introduces automation that allows for rapid network-wide changes, and ensures policy conformance post network updates. Intelligent capabilities include search, edit, validation (including conformance checking), deployment and audit features. Capabilities include:

- Centralized configuration with validation for consistency and compliance
- Time savings via simultaneous viewing and editing of multiple configurations
- Customized validation tests for corporate compliance and network design
- Automated large-scale configuration deployment without programming

Note: A separate software license is required to use Aruba NetEdit.

Mobility and IoT performance

The Aruba CX 6100 Switch Series uses internally developed Aruba ASICs that provide very low latency, increased packet buffering, and adaptive power consumption. Each switch includes the following:

- Up to 176 Gbps in non-blocking bandwidth and up to 98.6 Mpps for forwarding
- Selectable queue configurations that allow for increased performance by defining a number of queues and associated memory buffering to best meet the requirements of network applications

Simplify adds, moves and changes

Reduce manual IT operation tasks around initial deployment or on-going configuration changes to accommodate adds, moves and changes with colorless ports using local user roles and local-MAC-Authentication (LMA). Instead of statically pre-configuring access ports to VLANs and maintaining the switch port to VLAN mapping, colorless ports can automatically apply the role/policy required.

Enterprise-class access connectivity

To address branch office and small enterprise environments, the CX 6100 family includes five fixed 1U models. Each switch includes built-in high speed uplinks that automatically detect the use of 1G or 10G transceivers to deliver non-blocking performance. Additional highlights:

- 1U models support 24 and 48 access ports of IEEE 802.3 1GbE with four built-in 1GbE/10GbE uplink SFP+ ports. The 24 and 48 port PoE models support up to 370W IEEE 802.3at Class 4 Power over Ethernet for up to 30W per port
- Compact and fanless model supports 12 ports of IEEE 802.3 1GbE with four uplinks (two built-in 1GbE/10GbE uplink SFP/SFP+ ports, two built-in 1GbE ports), and 139W IEEE 802.3at Class 4 Power over Ethernet for up to 30W per port
- Support for Energy Efficient Ethernet IEEE 802.3az reduces power consumption during periods of low network traffic
- Support for pre-standard PoE detects and provides power to pre-standard PoE devices
- Auto-MDIX provides automatic adjustments for straight-through or crossover cables on all 10/100/1000 ports
- Unsupported Transceiver Mode (UTM) allows to insert and enable all unsupported 1G and 10G transceivers and cables. Note that there is no warranty nor support for the transceiver/cable when this feature is used
- Jumbo frames allow for high-performance backups and disaster-recovery systems; provides a maximum frame size of 9198 bytes
- Packet storm protection against broadcast, multicast and unknown unicast storms with user-defined thresholds



Resiliency and availability

To support a highly-available Layer 2 access deployment, the CX 6100 supports the following features:

- Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni directional traffic is detected, preventing loops in STP-based networks
- IEEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm
- IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required; and legacy support for IEEE 802.1d and IEEE 802.1w
- SmartLink provides easy-to-configure link redundancy of active and standby links

Quality of Service (QoS) features

To support congestion actions and traffic prioritization, the CX 6100 includes the following:

- Strict priority (SP) queuing
- Traffic prioritization (IEEE 802.1p) for real-time classification
- Class of Service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- Rate limiting sets per-port ingress enforced maximums and per-port, per-queue minimums
- Large buffers for graceful congestion management

Simplified configuration and management

The CX 6100 series supports a choice of management interfaces including easy to use Web GUI, industry standard CLI, Aruba NetEdit, and Aruba Central for unified network operations of wired, WLAN, SD-WAN, and public cloud infrastructure. Features include:

- Built-in programmable and easy-to-use REST API interface
- Industry-standard CLI with a hierarchical structure for reduced training time and expense. Delivers increased productivity in multivendor environments
- sFlow (RFC 3176) is ASIC-based wire speed network monitoring and accounting with no impact on network performance; network operators can gather a variety of network statistics and information for capacity planning and real-time network monitoring purposes

- Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection and local and remote syslog capabilities allow logging of all access
- SNMPv1/v2c/v3 support provides Read capability of industry standard Management Information Base (MIB), and private extensions
- SNMP support includes: Write Set Speed and Duplex, Write Port Security, Write POE Priority, Write Config Mgmt, SNMP-Read single OID for average CPU and memory, SNMP MIB View
- SNMP Trap include: Transceiver Traps (insertion/removal), SNMP Trap, SNMP MIB-SNMB Authentication, SNMPv2 MIB, Port Sec MIB-Port Sec, Config MIB-Running Config Change, Config MIB, AAA Server MIB, AAA Server State
- Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Supports events, alarms, history, and statistics groups as well as a private alarm extension group
- TFTP and SFTP support offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/IP network; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security
- Debug and sampler utility supports ping and traceroute for IPv4 and IPv6
- Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock-dependent devices within the network so the devices can provide diverse applications based on the consistent time
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications
- Dual flash images provides independent primary and secondary operating system files for backup while upgrading
- Multiple configuration files can be stored to a flash image
- Unidirectional link detection (UDLD) monitors the link between two switches and blocks the ports on both ends of the link if the link goes down at any point between the two devices



Layer 2 Switching

The following Layer 2 services are supported:

- VLAN support and tagging support for IEEE 802.1Q (4094 VLAN IDs) and 512 VLANs simultaneously
- Jumbo packet support improves the performance of large data transfers; supports frame size of up to 9,220 bytes
- Rapid Per-VLAN Spanning Tree (RPVST+) allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+
- STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
- MVRP allows automatic learning and dynamic assignment of VLANs
- Bridge Protocol Data Unit (BPDU) tunneling transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs
- Port mirroring duplicates port traffic (ingress and egress) to a monitoring port; supports 4 mirroring groups
- Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network

Layer 3 Services

The following Layer 3 services are supported:

- Address Resolution Protocol (ARP) determines the MAC address of another IP host in the same subnet; supports static ARPs
- Domain Name System (DNS) provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server
- Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility
- Dynamic Host Configuration Protocol (DHCP) simplifies the management of large IP networks and supports client; DHCPv4 Relay support enables DHCP operation across subnets

Layer 3 Routing

The following Layer 3 routing services are supported:

- Static IP routing provides manually configured routes.
- Dual stack static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routing
- Dual IP stack maintains separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design

Multicast

- IGMP Snooping allows multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN
- Multicast Listener Discovery (MLD) enables discovery of IPv6 multicast listeners; support MLD v1 and v2
- Internet Group Management Protocol (IGMP) utilizes Any-Source Multicast (ASM) to manage IPv4 multicast networks; supports IGMPv1, v2, and v3
- IP multicast snooping (data-driven IGMP) prevents flooding of IP multicast traffic

IPv6 capabilities

- IPv6 host enables switches to be managed in an IPv6 network
- Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols
- MLD snooping forwards IPv6 multicast traffic to the appropriate interface
- IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic
- IPv6 static routing

Security

Each Aruba CX 6100 Switch comes with an integrated trusted platform module (TPM) for platform integrity. This ensures the boot process started from a trusted combination of AOS-CX switches. Other security features include:

- Access control list (ACL) support for both IPv4 and IPv6; allows for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources; rules can either deny or permit traffic to be forwarded; rules can be based on a Layer 2 header or a Layer 3 protocol header
- ACLs also provide filtering based on the IP field, source/destination IP address/subnet, and source/destination TCP/UDP port number on a per-VLAN or per-port basis



- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS+) delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security
- Management access security for both on- and off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication. Additionally, TACACS+ can also provide admin authorization services
- Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks
- Supports multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
- Supports MAC-based client authentication
- Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications
- Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3
- Switch CPU protection provides automatic protection against malicious network traffic trying to shut down the switch
- ICMP throttling defeats ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic
- Identity-driven ACL enables implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user
- STP BPDU port protection blocks Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs, preventing forged BPDU attacks
- STP root guard protects the root bridge from malicious attacks or configuration mistakes
- Dynamic ARP protection blocks ARP broadcasts from unauthorized hosts, preventing eavesdropping or theft of network data
- DHCP (snooping) protection blocks DHCP packets from unauthorized DHCP servers, preventing denial-of-service attacks
- Supports DHCPv4 Relay
- Port security allows access only to specified MAC addresses, which can be learned or specified by the administrator
- MAC address lockout prevents particular configured MAC addresses from connecting to the network
- Source-port filtering allows only specified ports to communicate with each other
- Secure shell encrypts all transmitted data for secure remote CLI access over IP networks
- Secure Sockets Layer (SSL) encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch
- Secure FTP allows secure file transfer to and from the switch; protects against unwanted file downloads or unauthorized copying of a switch configuration file
- Critical Authentication Role ensures that important infrastructure devices such as IP phones are allowed network access even in the absence of a RADIUS server
- MAC Pinning allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected
- Security banner displays a customized security policy when users log in to the switch
- Dynamic IPv4 Lockdown works with DHCP protection to block traffic from unauthorized hosts, preventing IP source address spoofing
- DHCP smart relay allows the DHCP relay agent to use secondary IP addresses when the DHCP server does not reply the DHCP-OFFER message

Convergence

- LLDP-MED (Media Endpoint Discovery) defines a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones
- PoE allocations supports multiple methods (allocation by usage or class, with LLDP and LLDP-MED) to allocate PoE power for more efficient power management and energy savings.
- Auto VLAN configuration for voice RADIUS VLAN: uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones
- Supports CDPv2 to configure legacy IP phones



Additional information

- Green initiative support for RoHS (EN 50581:2012) and WEEE regulations

Customer first, customer last support

When your network is important to your business, then your business needs the backing of Aruba Support Services. Partner with Aruba product experts to increase your team productivity, keep pace with technology advances, software releases, and obtain break-fix support.

-Foundation Care for Aruba support services include priority access to Aruba Technical Assistance Center(TAC) engineers 24x7x365, flexible hardware and onsite support options, and total coverage for Aruba products. Aruba switches with assigned Aruba Central subscriptions benefit with option for additional hardware support only.

-Aruba Pro Care adds fast access to senior Aruba TAC engineers, who are assigned as a single point of contact for case management, reducing the time spent addressing and resolving issues.

For complete details on Foundation Care and Aruba Pro Care, please visit: <https://www.arubanetworks.com/supportservices/>

Warranty, services and support

- Limited Lifetime Warranty, see <https://www.arubanetworks.com/support-services/product-warranties/> for warranty and support information included with your product purchase
- For software releases and documentation, refer to <https://asp.arubanetworks.com/downloads>
- For more detailed information on Aruba AOS-CX software release and features, please visit the [AOS-CX Switch Software Documentation Portal](#)
- Explore and compare switch features for each platform and software release on the [Aruba Switch Feature Navigator](#)
- For support and services information, visit <https://www.arubanetworks.com/support-services/arubacare/>



SPECIFICATIONS

	Aruba 6100 48G Class4 PoE 4SFP+ 370W Switch (JL675A)	Aruba 6100 48G 4SFP+ Switch (JL676A)	Aruba 6100 24G Class4 PoE 4SFP+ 370W Switch (JL677A)
Description	48x ports 10/100/1000BASE-T Ports 4x 1G/10G SFP ports Supports PoE Standards IEEE 802.3af, 802.3at 1x USB-C Console Port 1x USB Type-A Host port	48x ports 10/100/1000BASE-T Ports 4x 1G/10G SFP ports 1x USB-C Console Port 1x USB Type-A Host port	24x ports 10/100/1000BASE-T Ports 4x 1G/10G SFP ports Supports PoE Standards IEEE 802.3af, 802.3at 1x USB-C Console Port 1x USB Type-A Host port
Power supplies	Fixed power supply Up to 370W of Class 4 PoE Power	Fixed power supply	Fixed power supply Up to 370W of Class 4 PoE Power
Fans	Fixed fans	Fixed fans	Fixed fans
Physical characteristics			
Dimensions	(H) 4.39 cm (W) 44.2 cm (D) 30.48 cm (1.73" x 17.4" x 12.0")	(H) 4.39 cm (W) 44.2 cm (D) 24.74 cm (1.73" x 17.4" x 9.74")	(H) 4.39 cm (W) 44.2 cm (D) 26.82 cm (1.73" x 17.4" x 10.56")
Configuration Weight	5.02 kg (11.07 lbs)	3.42 kg (7.54 lbs)	4.19kg (9.24 lbs)
Additional Specifications			
CPU	Dual Core ARM Cortex A9 @ 1016 Mhz	Dual Core ARM Cortex A9 @ 1016 Mhz	Dual Core ARM Cortex A9 @ 1016 Mhz
Memory and Flash	4 GB DDR3 16 GB eMMC	4 GB DDR3 16 GB eMMC	4 GB DDR3 16 GB eMMC
Packet Buffer	12.38MB (4.5MB Ingress/7.875MB Egress)	12.38MB (4.5MB Ingress/7.875MB Egress)	12.38MB (4.5MB Ingress/7.875MB Egress)
Performance			
Model Switching Capacity	176 Gbps	176 Gbps	128 Gbps
Model Throughput Capacity	98.6 Mpps	98.6 Mpps	95.2 Mpps
Average Latency (LIFO-64-bytes packets)	1 Gbps: 1.9 μSec , 10 Gbps: 1.8 μSec	1 Gbps: 1.9 μSec , 10 Gbps: 1.8 μSec	1 Gbps: 1.5 μSec , 10 Gbps: 1.8 μSec
Switched Virtual Interfaces (dual stack)	16	16	16
IPv4 Host Table (ARP)	1,024	1,024	1,024
IPv6 Host Table (ND)	512	512	512
IPv4 Unicast Routes	512	512	512
IPv6 Unicast Routes	512	512	512



SPECIFICATIONS (CONTINUED)

	Aruba 6100 48G Class4 PoE 4SFP+ 370W Switch (JL675A)	Aruba 6100 48G 4SFP+ Switch (JL676A)	Aruba 6100 24G Class4 PoE 4SFP+ 370W Switch (JL677A)
Performance (continued)			
MAC Table Capacity	8,192	8,192	8,192
IGMP Groups	512	512	512
MLD Groups	512	512	512
IPv4/IPv6/MAC ACL Entries (ingress)	256 / 128 / 256	256 / 128 / 256	256 / 128 / 256
Environment			
Operating Temperature	32°F to 113°F (0°C to 45°C) up to 5000 ft (1.5 km) derate -1°C for every 1000 ft (305 m) from 5000 ft (1.5 km) to 10000 ft (3.0 km)	32°F to 113°F (0°C to 45°C) up to 5000 ft (1.5 km) derate -1°C for every 1000 ft (305 m) from 5000 ft (1.5 km) to 10000 ft (3.0 km)	32°F to 113°F (0°C to 45°C) up to 5000 ft (1.5 km) derate -1°C for every 1000 ft (305 m) from 5000 ft (1.5 km) to 10000 ft (3.0 km)
Operating Relative Humidity	15% to 95% at 104°F (40°C) non-condensing	15% to 95% at 104°F (40°C) non-condensing	15% to 95% at 104°F (40°C) non-condensing
Non-Operating	-40°F to 158°F (-40°C to 70°C) up to 15000 ft (4.6 km)	-40°F to 158°F (-40°C to 70°C) up to 15000 ft (4.6 km)	-40°F to 158°F (-40°C to 70°C) up to 15000 ft (4.6 km)
Non-Operating Storage Relative Humidity	15% to 90% @ 149°F (65°C) non-condensing	15% to 90% @ 149°F (65°C) non-condensing	15% to 90% @ 149°F (65°C) non-condensing
Max Operating Altitude	10000 feet (3 km) Max	10000 feet (3 km) Max	10000 feet (3 km) Max
Max Non-Operating Altitude	15000 feet (4.6 km) Max	15000 feet (4.6 km) Max	15000 feet (4.6 km) Max
Acoustic	Sound Power, LWAd = 4.3 Bel Sound Pressure, LpAm (Bystander) = 29.8 dB	Sound Power, LWAd = 3.6 Bel Sound Pressure, LpAm (Bystander) = 24.6 dB	Sound Power, LWAd = 3.9 Bel Sound Pressure, LpAm (Bystander) = 24.3 dB
Primary Airflow	Side-to-side	Side-to-side	Side-to-side
Electrical Characteristics			
Frequency	50 / 60 Hz	50 / 60 Hz	50 / 60 Hz
AC Voltage	100-127 VAC / 200-240 VAC	100-127 VAC / 200-240 VAC	100-127 VAC / 200-240 VAC
Current	4.9 A / 2.4 A	0.8 A / 0.5 A	4.6 A / 2.3 A
Power Consumption (230 VAC)	Idle: 30.6W Max Power (w/o PoE): 45W Max Power (w/ PoE): 480W	Idle: 20.6W Max Power (w/o PoE): 44.2W	Idle: 22.9W Max Power (w/o PoE): 32.7W Max Power (w/ PoE): 455W



SPECIFICATIONS (CONTINUED)

	Aruba 6100 48G Class4 PoE 4SFP+ 370W Switch (JL675A)	Aruba 6100 48G 4SFP+ Switch (JL676A)	Aruba 6100 24G Class4 PoE 4SFP+ 370W Switch (JL677A)
Safety			
	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60825-1 UL 62368-1 Ed. 2; IEC 62368-1 Ed. 2; EN 62368-1:2014	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60825-1 UL 62368-1 Ed. 2; IEC 62368-1 Ed. 2; EN 62368-1:2014	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60825-1 UL 62368-1 Ed. 2; IEC 62368-1 Ed. 2; EN 62368-1:2014
Emissions			
	VCCI-CISPR 32, Class A; CNS 13438; ICES-003 Issue 6 Class A; FCC CFR 47 Part 15, Class A; EN 55032: 2015 +AC:2016 / CISPR-32, Class A	VCCI-CISPR 32, Class A; CNS 13438; ICES-003 Issue 6 Class A; FCC CFR 47 Part 15, Class A; EN 55032: 2015 +AC:2016 / CISPR-32, Class A	VCCI-CISPR 32, Class A; CNS 13438; ICES-003 Issue 6 Class A; FCC CFR 47 Part 15, Class A; EN 55032: 2015 +AC:2016 / CISPR-32, Class A
Lasers			
	EN 60825-1:2007 / IEC 60825-1:2007 Class 1 Class 1 Laser Products / Laser Klasse 1 (Applicable for accessories - Optical Transceivers only)	EN 60825-1:2007 / IEC 60825-1:2007 Class 1 Class 1 Laser Products / Laser Klasse 1 (Applicable for accessories - Optical Transceivers only)	EN 60825-1:2007 / IEC 60825-1:2007 Class 1 Class 1 Laser Products / Laser Klasse 1 (Applicable for accessories - Optical Transceivers only)
Immunity			
Generic	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35
EN	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017
ESD	IEC 61000-4-2	IEC 61000-4-2	IEC 61000-4-2
Radiated	IEC 61000-4-3	IEC 61000-4-3	IEC 61000-4-3
EFT/Burst	IEC 61000-4-4	IEC 61000-4-4	IEC 61000-4-4
Surge	IEC 61000-4-5	IEC 61000-4-5	IEC 61000-4-5
Conducted	IEC 61000-4-6	IEC 61000-4-6	IEC 61000-4-6
Power frequency magnetic field	IEC 61000-4-8	IEC 61000-4-8	IEC 61000-4-8
Voltage dips and interruptions	IEC 61000-4-11	IEC 61000-4-11	IEC 61000-4-11
Harmonics	EN 61000-3-2, IEC 61000-3-2	EN 61000-3-2, IEC 61000-3-2	EN 61000-3-2, IEC 61000-3-2
Flicker	EN 61000-3-3, IEC 61000-3-3	EN 61000-3-3, IEC 61000-3-3	EN 61000-3-3, IEC 61000-3-3
Mounting and Enclosure			
	Mounts in an EIA-standard 19-inch telco rack or equipment cabinet (rack-mounting kit included); horizontal surface mounting.	Mounts in an EIA-standard 19-inch telco rack or equipment cabinet (rack-mounting kit included); horizontal surface mounting.	Mounts in an EIA-standard 19-inch telco rack or equipment cabinet (rack-mounting kit included); horizontal surface mounting.



SPECIFICATIONS (CONTINUED)

	Aruba 6100 24G 4SFP+ Switch (JL678A)	Aruba 6100 12G Class4 PoE 2G/2SFP+ 139W Switch (JL679A)
Description	24x ports 10/100/1000BASE-T Ports 4x 1G/10G SFP ports 1x USB-C Console Port 1x USB Type-A Host port	12x ports 10/100/1000BASE-T Ports 2x 1G/10G SFP ports 2x 1GbE ports Supports PoE Standards IEEE 802.3af, 802.3at 1x USB-C Console Port 1x USB Type-A Host port
Power supplies	Fixed power supply	Fixed power supply Up to 139W of Class 4 PoE Power
Fans	Fixed fans	Fanless
Physical characteristics		
Dimensions	(H) 4.39 cm (W) 44.2 cm (D) 20.12 cm (1.73" x 17.4" x 7.92")	(H) 4.39 cm (W) 25.4 cm (D) 25.5 cm (1.73" x 10.0" x 10.04")
Configuration Weight	2.62 kg (5.78 lbs)	2.78 kg (6.13 lbs)
Additional Specifications		
CPU	Dual Core ARM Cortex A9 @ 1016 Mhz	Dual Core ARM Cortex A9 @ 1016 Mhz
Memory and Flash	4 GB DDR3 16 GB eMMC	4 GB DDR3 16 GB eMMC
Packet Buffer	12.38MB (4.5MB Ingress/7.875MB Egress)	12.38MB (4.5MB Ingress/7.875MB Egress)
Performance		
Model Switching Capacity	128 Gbps	68 Gbps
Model Throughput Capacity	95.2 Mpps	45.1 Mpps
Average Latency (LIFO-64-bytes packets)	1 Gbps: 1.5 μSec , 10 Gbps: 1.8 μSec	1 Gbps: 2.3 μSec , 10 Gbps: 2.6 μSec
Switched Virtual Interfaces (dual stack)	16	16
IPv4 Host Table (ARP)	1,024	1,024
IPv6 Host Table (ND)	512	512
IPv4 Unicast Routes	512	512
IPv6 Unicast Routes	512	512



SPECIFICATIONS (CONTINUED)

	Aruba 6100 24G 4SFP+ Switch (JL678A)	Aruba 6100 12G Class4 PoE 2G/2SFP+ 139W Switch (JL679A)
Performance (continued)		
MAC Table Capacity	8,192	8,192
IGMP Groups	512	512
MLD Groups	512	512
IPv4/IPv6/MAC ACL Entries (ingress)	256 / 128 / 256	256 / 128 / 256
Environment		
Operating Temperature	32°F to 113°F (0°C to 45°C) up to 5000 ft (1.5 km) derate -1°C for every 1000 ft (305 m) from 5000 ft (1.5 km) to 10000 ft (3.0 km)	32°F to 113°F (0°C to 45°C) up to 5000 ft (1.5 km) derate -1°C for every 1000 ft (305 m) from 5000 ft (1.5 km) to 10000 ft (3.0 km)
Operating Relative Humidity	15% to 95% at 104°F (40°C) non-condensing	15% to 95% at 104°F (40°C) non-condensing
Non-Operating	-40°F to 158°F (-40°C to 70°C) up to 15000 ft (4.6 km)	-40°F to 158°F (-40°C to 70°C) up to 15000 ft (4.6 km)
Non-Operating Storage Relative Humidity	15% to 90% @ 149°F (65°C) non-condensing	15% to 90% @ 149°F (65°C) non-condensing
Max Operating Altitude	10000 feet (3 km) Max	10000 feet (3 km) Max
Max Non-Operating Altitude	15000 feet (4.6 km) Max	15000 feet (4.6 km) Max
Acoustic	Sound Power, LWAd = 3.9 Bel Sound Pressure, LpAm (Bystander) = 20.9 dB	Sound Power, LWAd = 0 Bel Sound Pressure, LpAm (Bystander) = 0 dB
Primary Airflow	Side-to-side	-
Electrical Characteristics		
Frequency	50 / 60 Hz	50 / 60 Hz
AC Voltage	100-127 VAC / 200-240 VAC	100-127 VAC / 200-240 VAC
Current	0.6 A / 0.4 A	1.8 A / 0.9 A
Power Consumption (230 VAC)	Idle: 15.4W Max Power (w/o PoE): 33W	Idle: 16W Max Power (w/o PoE): 21.9W Max Power (w/ PoE): 170W



SPECIFICATIONS (CONTINUED)

	Aruba 6100 24G 4SFP+ Switch (JL678A)	Aruba 6100 12G Class4 PoE 2G/2SFP+ 139W Switch (JL679A)
Safety		
	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60825-1 UL 62368-1 Ed. 2; IEC 62368-1 Ed. 2; EN 62368-1:2014	UL 60950-1; IEC 60950-1; EN 60950-1; CAN/CSA-C22.2 No. 60950-1; EN 60825-1 UL 62368-1 Ed. 2; IEC 62368-1 Ed. 2; EN 62368-1:2014
Emissions		
	VCCI-CISPR 32, Class A; CNS 13438; ICES-003 Issue 6 Class A; FCC CFR 47 Part 15, Class A; EN 55032: 2015 +AC:2016 / CISPR-32, Class A	VCCI-CISPR 32, Class A; CNS 13438; ICES-003 Issue 6 Class A; FCC CFR 47 Part 15, Class A; EN 55032: 2015 +AC:2016 / CISPR-32, Class A
Lasers		
	EN 60825-1:2007 / IEC 60825-1:2007 Class 1 Class 1 Laser Products / Laser Klasse 1 (Applicable for accessories - Optical Transceivers only)	EN 60825-1:2007 / IEC 60825-1:2007 Class 1 Class 1 Laser Products / Laser Klasse 1 (Applicable for accessories - Optical Transceivers only)
Immunity		
Generic	CISPR 24 / CISPR 35	CISPR 24 / CISPR 35
EN	EN 55024:2010 / EN 55035:2017	EN 55024:2010 / EN 55035:2017
ESD	IEC 61000-4-2	IEC 61000-4-2
Radiated	IEC 61000-4-3	IEC 61000-4-3
EFT/Burst	IEC 61000-4-4	IEC 61000-4-4
Surge	IEC 61000-4-5	IEC 61000-4-5
Conducted	IEC 61000-4-6	IEC 61000-4-6
Power frequency magnetic field	IEC 61000-4-8	IEC 61000-4-8
Voltage dips and interruptions	IEC 61000-4-11	IEC 61000-4-11
Harmonics	EN 61000-3-2, IEC 61000-3-2	EN 61000-3-2, IEC 61000-3-2
Flicker	EN 61000-3-3, IEC 61000-3-3	EN 61000-3-3, IEC 61000-3-3
Mounting and Enclosure		
	Mounts in an EIA-standard 19-inch telco rack or equipment cabinet (rack-mounting kit included); horizontal surface mounting.	Mounts in an EIA-standard 19-inch telco rack or equipment cabinet (rack-mounting kit included); horizontal surface mounting; wall mounting; Kensington Security Slot



STANDARDS AND PROTOCOLS

- RFC 1591 DNS (client)
- SSHv1/SSHv2 Secure Shell
- IEEE 802.1D MAC Bridges
- IEEE 802.1p Priority
- IEEE 802.1Q VLANs
- IEEE 802.1s Multiple Spanning Trees
- IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- IEEE 802.3 Type 10BASE-T
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- IEEE 802.3at Power over Ethernet
- IEEE 802.3az Energy Efficient Ethernet
- IEEE 802.3x Flow Control
- RFC 768 UDP
- RFC 783 TFTP Protocol (revision 2)
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 1350 TFTP Protocol (revision 2)
- RFC 2131 DHCP client
- RFC 4330 Simple Network Time Protocol (SNTP) v4
- RFC 951 BOOTP (VLAN 1 Only)
- RFC 1542 BOOTP Extensions (VLAN 1 only)
- IGMPv2/IGMPv3
- IGMP/MLD Snooping
- RFC 1981 IPv6 Path MTU Discovery
- RFC 2460 IPv6 Specification
- RFC 2925 Remote Operations MIB (Ping only)
- RFC 3315 DHCPv6 (client only)
- RFC 3513 IPv6 Addressing Architecture
- RFC 3596 DNS Extension for IPv6
- RFC 3176 sFlow
- RFC 4022 MIB for TCP
- RFC 4113 MIB for UDP (Partially)
- RFC 4251 SSHv6 Architecture
- RFC 4252 SSHv6 Authentication
- RFC 4253 SSHv6 Transport Layer
- RFC 4254 SSHv6 Connection
- RFC 4293 MIB for IP
- RFC 4419 Key Exchange for SSH
- RFC 4443 ICMPv6
- RFC 4861 IPv6 Neighbor Discovery
- RFC 4862 IPv6 Stateless Address Auto-configuration
- RFC 1213 MIB
- RFC 1493 Bridge MIB
- RFC 2674 802.1p and IEEE 802.1Q Bridge MIB (Partial support. MIB objects supported: ieee8021BridgeBasePort, ieee8021BridgeBasePort, ieee8021BridgePortMrpJoinTime, ieee8021BridgePortMrpLeaveTime, ieee8021BridgePortMrpLeaveAllTime)
- RFC 2737 Entity MIB
- RFC 2863 The Interfaces Group MIB
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- RFC 1098 A Simple Network Management Protocol (SNMP)
- ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
- SNMPv1/v2c/v3
- RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events)
- RFC 1098 A Simple Network Management Protocol (SNMP)
- RFC 2474 DiffServ precedence, with 2/4/8 queues per port
- RFC 2475 DiffServ Architecture
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2598 DiffServ Expedited Forwarding (EF)
- IEEE 802.1X Port Based Network Access Control
- RFC 1492 TACACS+
- RFC 2138 RADIUS Authentication
- RFC 2866 RADIUS Accounting
- Secure Sockets Layer (SSL)



ARUBA CX 6100 SWITCHES AND ACCESSORIES

Switch Models

- Aruba 6100 48G Class4 PoE 4SFP+ 370W Switch (JL675A)
- Aruba 6100 48G 4SFP+ Switch (JL676A)
- Aruba 6100 24G Class4 PoE 4SFP+ 370W Switch (JL677A)
- Aruba 6100 24G 4SFP+ Switch (JL678A)
- Aruba 6100 12G Class4 PoE 2G/2SFP+ 139W Switch (JL679A)

Accessories

- Aruba X511 12-port Cable Guard (JL742A)
- Aruba X414 1U Universal 4-post Rack Mount Kit (J9583B)
- Aruba USB-A to RJ45 PC-to-Switch Cable (R9G48A)
- Aruba USB-A to RJ45 PIN3TX-6RX Cable (R8Z87A)
- Aruba USB-A to USB-C PC-to-Switch Cable (R9J32A)
- Aruba USB-C to USB-C PC-to-Switch Cable (R9J33A)

Transceivers

- Aruba 1G SFP LC SX 500m MMF Transceiver (J4858D)
- Aruba 1G SFP LC LX 10km SMF Transceiver (J4859D)
- Aruba 1G SFP RJ45 T 100m Cat5e Transceiver (J8177D)
- Aruba 10G SFP+ LC SR 300m MMF Transceiver (J9150D)
- Aruba 10G SFP+ LC LR 10km SMF Transceiver (J9151E)

Software

- Aruba NetEdit Single Node: 1 year (JL639AAE)
- Aruba NetEdit Single Node: 3 years (JL640AAE)

Aruba Central Foundation Licenses

- Aruba Central 25xx/6100/8 to 12 port Switch Foundation 1 year Subscription E-STU (Q9Y68AAE)
- Aruba Central 25xx/6100/8 to 12 port Switch Foundation 3 year Subscription E-STU (Q9Y69AAE)
- Aruba Central 25xx/6100/8 to 12 port Switch Foundation 5 year Subscription E-STU (Q9Y70AAE)
- Aruba Central 25xx/6100/8 to 12 port Switch Foundation 7 year Subscription E-STU (Q9Y71AAE)
- Aruba Central 25xx/6100/8 to 12 port Switch Foundation 10 year Subscription E-STU (Q9Y72AAE)

- Aruba Central On-Premises 25xx/6100/8 to 12 port Switch Foundation 1 year Subscription E-STU (R6U73AAE)
- Aruba Central On-Premises 25xx/6100/8 to 12 port Switch Foundation 3 year Subscription E-STU (R6U74AAE)
- Aruba Central On-Premises 25xx/6100/8 to 12 port Switch Foundation 5 year Subscription E-STU (R6U75AAE)
- Aruba Central On-Premises 25xx/6100/8 to 12 port Switch Foundation 7 year Subscription E-STU (R6U76AAE)
- Aruba Central On-Premises 25xx/6100/8 to 12 port Switch Foundation 10 year Subscription E-STU (R6U77AAE)

For details and complete listing of Aruba Central licensing options, please refer to the Aruba Central Data Sheet.

Support

- JL675A: 4 Hour Onsite 3 Year (HY2L6E)
- JL676A: 4 Hour Onsite 3 Year (HY2M9E)
- JL677A: 4 Hour Onsite 3 Year (HL5Z0E)
- JL678A: 4 Hour Onsite 3 Year (HY2Q5E)
- JL679A: 4 Hour Onsite 3 Year (HY2R8E)

For Aruba Central hardware only support, 24x7 TAC support, and many other support options, go to Support Services Central SKU lookup tool.

DATA SHEET

ARUBA 7200 SERIES MOBILITY CONTROLLERS

Improved network performance, visibility, and control

Aruba 7200 Series Mobility Controllers enhance WLAN performance for high performance, high density enterprise requirements. The 7200 Series centralizes all control functionality for individual Aruba access points (APs) to improve AP utilization, security, and client roaming. Ideally suited for large campuses and high density environments, the 7200 Series can be deployed using Zero Touch Provisioning (ZTP) to simplify deployment.

SIMPLE AND SECURE ACCESS

The 7200 Series serves a key role in Dynamic Segmentation, providing Aruba's Policy Enforcement Firewall (PEF) to enforce policies based on user role, device type, application, and network location - and simplifying and securing wired and wireless network access. Traffic is encapsulated in GRE tunnels for complete encryption all the way from an AP or switch. This feature can be enabled with the ArubaOS PEF license and eliminates the need to manually configure SSIDs, VLANs or ACLs for each new client on the network.

HIGH PERFORMANCE AND RELIABILITY

Each 7200 Series provides connectivity for up to 32,728 concurrent users or client devices, 2,048 access points and over 2 million active firewall sessions. With up to 80 virtual CPUs and 100Gbps of maximum throughput to perform Policy Enforcement Firewall (PEF) features, the 7200 Series are in a class of their own -- ideal for the most demanding enterprise, college, and large public venue requirements.



KEY FEATURES

- Support for new Wi-Fi 6 (802.11 ax), WPA3 and Enhanced Open – and existing standards
- Patented ClientMatch technology can now group together Wi-Fi 6-capable devices
- Dynamic Segmentation enforces wired and wireless access policies to simplify and secure the network
- Application awareness for 3,000+ applications without additional hardware
- Built in AI-powered wireless/RF optimization
- Unifies policy enforcement for WLAN, LAN and WAN traffic

For enhanced resiliency and availability, the 7200 Series can be clustered together in a network managed by Aruba Mobility Master.



Front: 7205



Back: 7205



Front: 7210/7220/7240/7240XM



Back: 7210/7220/7240/7240XM



Front: 7280



Back: 7280



24/7 MISSION-CRITICAL NETWORKING

Aruba's unique, patented wireless technologies are based on AI-powered machine learning algorithms and integrated directly into ArubaOS. Adaptive Radio Management, AirMatch and ClientMatch (now enhanced with Wi-Fi 6 grouping) provide RF optimization techniques to improve user experience and network health based on changing environmental conditions, correct for noisy or congested RF and resolve sticky client issues during user roaming. RFProtect provides advanced spectrum analysis and wireless intrusion protection (WIPS/WIDS) to help identify and mitigate Wi-Fi and non-Wi-Fi sources of interference, as well as containment of potential security risks. Learn more about Aruba's software features on the ArubaOS datasheet.

When deployed with the Aruba Mobility Master, the 7200 Series can be joined to a controller cluster to increase scale, improve reliability using enhanced High Availability (HA), adopt configurations seamlessly based on hierarchy, support Live Upgrades to reduce maintenance windows and share licenses from a global licensing pool. The 7200 Series also serves a key, policy enforcement role in Aruba's 360 Secure Fabric. For network management, Aruba AirWave provides real-time monitoring, reporting and Wi-Fi location services.

Learn more about the 7200 Series Mobility Controller features in the [ArubaOS datasheet](#).

SD-WAN DEPLOYMENT

For organizations that are now managing multiple WAN connections, the 7200 Series can be connected to Aruba's SD-WAN fabric right out of the box. SD-WAN is a rich WAN management solutions that is used to simplify management of traffic entering and exiting branch sites. Please refer to the [SD-WAN datasheet](#) for more information.

MICROSOFT FEATURES

Aruba's integration with Microsoft enables unique application intelligence that detects Microsoft 365, Teams and Skype for Business traffic and then prioritizes them over less critical applications. Through management interfaces on ArubaOS, Aruba Central, and Aruba AirWave, IT can visualize call quality metrics such as MOS, latency, jitter, and packet loss for additional insight.

ENHANCED CAPABILITIES:

Wi-Fi 6 (802.11ax) enhanced with ClientMatch

The latest Wi-Fi standard brings enhanced performance, speed, and efficiency with key features such as OFDMA, 1024-QAM, and bidirectional MU-MIMO. Combined with Aruba's patented ClientMatch technology, 802.11ax clients will now be grouped together to optimize the multi-user experience.

Enhanced wireless security

Support for WPA3 brings stronger encryption and authentication methods, while Enhanced Open brings automatic security to open networks. New WPA2-MPSK feature enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device need to be changed, no additional key changes are needed for other devices on the network.

Dynamic Segmentation

To simplify and better secure wired and wireless network access, the 7200 Series can enforce per-user and device roles across wired and wireless networks by integrating with ClearPass Policy Manager. This ensures consistent policy regardless of user role and device type, and eliminates the need to configure unnecessary SSIDs, ACLs, VLANs and subnets at every node in the network.

Policy Enforcement Firewall

Enabled by the PEF license, wired and wireless user and application traffic can be tunneled to a stateful firewall on the 7200 Series through GRE tunnels for inspection. Policies are then enforced based on user role, device type, application and location - as described in Dynamic Segmentation.

Application visibility and control

Enabled by the PEF license, application visibility with Deep Packet Inspection (DPI) technology evaluates and optimizes performance and Quality of Service policies for over 3,000 applications - even for encrypted or hidden traffic.

Web content filtering

WebCC is an add-on subscription-based feature that classifies websites by content category and rates them by reputation. It can also block, apply QoS, bandwidth-limit, mirror, and log web content.



Unified Communications and Collaboration (UCC)

Visualize and troubleshoot networks based on call quality metrics such as MOS, latency, jitter and packet loss. Supported applications include: Teams, Skype for Business, Wi-Fi Calling, Facetime, SIP, Jabber, Spark and more.

Zero Touch Provisioning

The 7200 Series can be factory-shipped and deployed onsite with cloud-based Aruba Activate. For network-specific requirements, settings can be applied based on hierarchical configuration.

Integrated VPN services

With support for IPSec/SSL VPNs, Aruba Remote APs (RAPs) and Aruba VIA VPN users can establish encrypted sessions without any additional hardware required.

Third-party security integration

For advanced malware or antivirus protection, the 7200 Series can assume the role of an on-premises agent of centrally-hosted firewalls such as those provided by Palo Alto Networks and Check Point Software.

PERFORMANCE AND CAPACITY					
Features	7205	7210	7220	7240XM	7280
Maximum campus or remote AP licenses	256	512	1,024	2,048	2,048
Maximum concurrent users/devices	8,192	16,384	24,576	32,768	32,768
Maximum VLANs	4,096	4,096	4,096	4,096	4,096
Active firewall sessions	1 million (M)	2M	2M	2M	2M
Concurrent GRE tunnels	4,096	8,192	16,384	32,768	32,768
Concurrent IPsec sessions	8,192	16,384	24,576	32,768	32,768
Concurrent SSL sessions	4,096	8,192	8,192	8,192	8,192
Firewall throughput (Gbps)	12	20	40	40	100
Wired Bridged Throughput (Gbps)	12	20	40	40	100
Encrypted throughput 3DES (Gbps)	5	7	25	28	57
Encrypted throughput AES-CBC-256 (Gbps)	5	7	22	30	46
Encrypted throughput AES-CCM (Gbps)	5	7	20	29	75
Encrypted throughput AES-GCM-256 (Gbps)	5	7	26	35	70

INTERFACES AND INDICATORS					
Features	7205	7210	7220	7240XM	7280
Form factor/footprint	1xRU	1xRU	1xRU	1xRU	1xRU
10/100/1000BASE-T	4xCombo	2xCombo	2xCombo	2xCombo	-
1000BASE-X					
10G Ports (10G or 1G supported)	2xSFP+	4xSFP+	4xSFP+	4xSFP+	8xSFP+
40G Ports	-	-	-	-	2xQSFP+
USB 2.0	2	1	1	1	1
Management/status LEDs	Yes	Yes	Yes	Yes	Yes
LINK/ACT and status LEDs	Yes	Yes	Yes	Yes	Yes
LCD panel and navigation buttons	Yes	Yes	Yes	Yes	Yes
Console port	Micro USB, RJ-45	Mini USB, RJ-45	Mini USB, RJ-45	Mini USB, RJ-45	Micro USB, RJ-45
Out-of-band management port	Yes	No	No	No	Yes



PHYSICAL					
Features	7205	7210	7220	7240XM	7280
Dimensions (HxWxD)	(H) 4.4 cm x (W) 44.2 cm x (D) 33.4 cm (1.75" x 17.38" x 13.13")	(H) 4.4 cm x (W) 44.5 cm x (D) 44.5 cm (1.75" x 17.5" x 17.5")			(H) 4.4 cm x (W) 44.2 cm x (D) 40.1 cm (1.73" x 17.40" x 15.79")
Weight	4.95 kg (10.19 lbs.)	7.45 kg (16.43 lbs.)			7.9 kg (17.41 lbs)
MTBF (Hours)	129,597 (@40C)	106,536 (@40C)	113,751 (@40C)	116,590 (@40C)	281,896 (@45C)

ENVIRONMENTAL RANGE					
Features	7205	7210	7220	7240XM	7280
Operating Temperature	0° C to 40° C				
Storage Temperature	-40° C to 70° C				
Humidity/Storage Humidity	10% to 95%, NC	5% to 95%, NC	5% to 95%, NC	5% to 95%, NC	5% to 95%, NC
Operating Altitude	10,000 feet				
Acoustic Noise ¹	49 dBA	52.9 dBA			47.1 dBA
Maximum Heat Dissipation (BTU/hour)	260	375	427	563	819
Maximum Power Consumption	75.2W	110W	125W	165W	240W
Power Source	Internal power supply	350-watt AC or DC power supply			550-watt power supply

¹Sound power per ETSI 300 753 in accordance with ISO 7779

POWER ADAPTER AND SUPPLY SPECIFICATIONS			
Features	350-watt AC	350-watt DC	550-watt
Input voltage range	100 VAC to 240 VAC	DC -48V to DC -60V	100 VAC to 240 VAC
Output Voltage	+12VDC, 29.16A	+12VDC, 29.16A	+12VDC, 29.16A
Input frequency	50-60 Hz	50-60 Hz	50-60 Hz
AC line input current (steady state)	5 - 2.5A	5 - 2.5A	7.1 - 3.4A
Operating Temperature	-5o to +55o C	-5o to +55o C	-5o to +55o C
Cooling	Internal fan (Air flow rear to front)	Internal fan (Air flow rear to front)	819 Internal fan (Air flow rear to front)
Weight	1.3 kg (2.8 lbs)	1.3 kg (2.8 lbs)	0.87 kg (1.9 lbs)



REGULATORY AND SAFETY COMPLIANCE					
Features	7205	7210	7220	7240XM	7280
Regulatory SKU information	ARCN7205	ARCN0100	ARCN0101	ARCN0102	ARCN7280
Minimum ArubaOS Release	6.4.3.0	6.2.0.0	6.2.0.0	6.4.4.0	6.5.4.0 or 8.3.0.0
	802.11ax (Wi-Fi 6), AOS 8.4; WI-FI CERTIFIED WPA3™, AOS 8.4; WI-FI CERTIFIED Enhanced Open™, AOS 8.4				
Regulatory and Safety Compliance	FCC Part 15 Class A CE				
	Industry Canada Class A				
	VCCI Class A (Japan)				
	EN 55022 Class A (CISPR 22 Class A), EN 61000-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, EN 55024, AS/NZS 3548				
	UL 60950, EN60950				
	CAN/CSA 22.2 #60950				
	CE mark, cTUVus, CB, C-tick, Anatel, NOM, MIC				
Telco	Common Language Equipment Identifier (CLEI) Code				

SERVICE AND WARRANTY INFORMATION

- Hardware: 1 year parts/labor, can be extended with support contract
- Software: 90 days, can be extended with support contract

ORDERING INFORMATION	
Part Number	Description
Aruba 7205 Series Mobility Controllers	
JW735A	Aruba 7205 (RW) 2-port 10GBASE-X (SFP+) Controller
JW736A	Aruba 7205 (US) 2-port 10GBASE-X (SFP+) Controller
JW737A	Aruba 7205 (JP) 2-port 10GBASE-X (SFP+) Controller
JY852A	Aruba 7205 (EG) 2x 10GBASE-X SFP+ Controller
JW738A	Aruba 7205 (IL) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW739A	Aruba 7205 (RW) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW740A	Aruba 7205 (US) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW741A	Aruba 7205 (JP) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller
JW742A	Aruba 7205 (IL) FIPS/TAA-compliant 2-port 10GBASE-X (SFP+) Controller



ORDERING INFORMATION

Part Number	Description
Aruba 7210 Series Mobility Controllers	
JW743A	Aruba 7210 (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW744A	Aruba 7210 (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JY853A	Aruba 7210 (EG) 4x 10GBase-x SFP/SFP+ Controller
JW645A	Aruba 7210DC (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW646A	Aruba 7210DC (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW745A	Aruba 7210 (RW) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW746A	Aruba 7210 (US) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW747A	Aruba 7210 (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW647A	Aruba 7210DC (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW748A	Aruba 7210 (IL) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)
JW749A	Aruba 7210 (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW648A	Aruba 7210DC (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW750A	Aruba 7210 (JP) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
R6M40A	Aruba 7210 (RU) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000 BASE-T or SFP) Gateway
Aruba 7220 Series Mobility Controllers	
JW751A	Aruba 7220 (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW752A	Aruba 7220 (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW649A	Aruba 7220DC (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW650A	Aruba 7220DC (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW753A	Aruba 7220 (RW) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW754A	Aruba 7220 (US) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)
JW755A	Aruba 7220 (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW651A	Aruba 7220DC (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW756A	Aruba 7220 (IL) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)
JW757A	Aruba 7220 (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW652A	Aruba 7220DC (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) 350W DC Pwr Cntrlr
JW758A	Aruba 7220 (JP) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP)



ORDERING INFORMATION

Part Number	Description
Aruba 7240XM Series Mobility Controllers	
JW784A	Aruba 7240XM (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW830A	Aruba 7240XM (US) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JY854A	Aruba 7240XM (EG) 4x 10GBase-x SFP/SFP+ Controller
JW675A	Aruba 7240XMDC (US) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
JW783A	Aruba 7240XM (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW829A	Aruba 7240XM (RW) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW674A	Aruba 7240XMDC (RW) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
JW786A	Aruba 7240XM (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW832A	Aruba 7240XM (IL) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW677A	Aruba 7240XMDC (IL) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
JW785A	Aruba 7240XM (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW831A	Aruba 7240XM (JP) FIPS/TAA 16GB DRAM 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Controller
JW676A	Aruba 7240XMDC (JP) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
R8W28A	Aruba 7240XMDC (EG) 16GB DRAM 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr
Aruba 7240 to 7240XM Series Upgrades	
JW834A	Aruba 7240XM (US) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW838A	Aruba 7240XM (US) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW842A	Aruba 7240XMDC (US) 4p 10GBase-X/SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade
JW833A	Aruba 7240XM (RW) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW837A	Aruba 7240XM (RW) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW841A	Aruba 7240XMDC (RW) 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade
JW836A	Aruba 7240XM (IL) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW840A	Aruba 7240XM (IL) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW844A	Aruba 7240XMDC (IL) 4p 10GBase-X /SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade
JW835A	Aruba 7240XM (JP) 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW839A	Aruba 7240XM (JP) FIPS/TAA 4p 10GBase-X (SFP+) 2p Dual Pers (10/100/1000BASE-T or SFP) Cntrlr 16GB Upgrade
JW843A	Aruba 7240XMDC (JP) 4p 10GBase-X/SFP+ 2p Dual Pers (10/100/1000 or SFP) DC Pwr Cntrlr 16GB Upgrade



ORDERING INFORMATION	
Part Number	Description
Aruba 7280 Series Mobility Controllers	
JX910A	Aruba 7280 (US) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX911A	Aruba 7280 (RW) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX912A	Aruba 7280 (JP) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX913A	Aruba 7280 (IL) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX914A	Aruba 7280 (US) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX915A	Aruba 7280 (RW) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX916A	Aruba 7280 (JP) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JX917A	Aruba 7280 (IL) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
JZ077A	Aruba 7280 (EG) 2x40GbE and 8x10GBASE-X (SFP+) Controller
JZ078A	Aruba 7280 (EG) FIPS/TAA-compliant 2x40GbE and 8x10GBASE-X (SFP+) Controller
Controller Accessories	
<i>Aruba 7205/7280 Series Wall/Rack Mount</i>	
JW083A	Aruba SPR-WL2-MNT 7205/7280 - Wall/Rack Mount
<i>Aruba 7210/7220/7240/7240XM Series Wall/Rack Mount</i>	
JW109A	Aruba SPR-WL-MNT 7210/7220/7240/7240XM - Wall/Rack Mount
<i>Aruba 7210/7220/7240/7240XM Redundant Power Supplies and Fan Tray</i>	
JW657A	Aruba PSU-350-AC 7200 Series S3500-24T S3500-48T and S3500-24F 350W AC Power Supply
JW658A	Aruba PSU-350-DC 7200 Series Mobility Controllers 350W DC (-48V DC) Power Supply
JW111A	Aruba HW-7200-FT 7200 Series Fan Tray
<i>Aruba 7280 Redundant Power Supply and Fan Tray</i>	
JZ012A	PSU-550-AC 550W AC Power Supply
JZ013A	Aruba HW-7280-FT 7280 Series Fan Tray

ORDERING INFORMATION						
Part Number		7205	7210	7220	7240XM	7280
Transceivers						
JW149A	SFP-EX 1000BASE-EX LC SFP XCVR	X	X	X	X	X
JW150A	SFP-ZX 1000BASE-ZX LC SFP XCVR	X	X	X	X	
J4859D	Aruba 1G SFP LC LX 10km SMF Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹
J4858D	Aruba 1G SFP LC SX 500m OM2 MMF Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹
J4860D	Aruba 1G SFP LC LH 70km SMF Transceiver	X ²	X ²	X ²	X ²	X ²
J8177D	Aruba 1G SFP RJ45 T 100m Cat5e Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹

X: Supported transceiver

¹Default minimum ArubaOS software version is 6.5.3.0 and 8.1.0.0

²Minimum ArubaOS software version is 6.5.4.7 and 8.4.0.0

³Minimum ArubaOS software version is 8.1.0.0



ORDERING INFORMATION

Part Number		7205	7210	7220	7240XM	7280
Transceivers						
JW148A	SFP-10GE-ZR 10G LC Cnctr SFP+ XCVR	X	X	X	X	X
J9150D	Aruba 10G SFP+ LC SR 300m OM3 MMF Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹
J9151E	Aruba 10G SFP+ LC LR 10km SMF Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹
J9152D	Aruba 10G SFP+ LC LRM 220m OM2 MMF Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹
J9153D	Aruba 10G SFP+ LC ER 40km SMF Transceiver	X ¹	X ¹	X ¹	X ¹	X ¹
JL745A	Aruba 1G SFP LC SX 500m MMFTAA XCVR	X ³	X ³	X ³	X ³	X ³
JL746A	Aruba 1G SFP LC LX 10km SMF TAA XCVR	X ³	X ³	X ³	X ³	X ³
JL747A	Aruba 1G SFP RJ45 T 100m Cat5e TAA XCVR	X ³	X ³	X ³	X ³	X ³
JL748A	Aruba 10G SFP+ LC SR 300m MMFTAA XCVR	X ³	X ³	X ³	X ³	X ³
JL749A	Aruba 10G SFP+ LC LR 10km SMF TAA XCVR	X ³	X ³	X ³	X ³	X ³
J9281D	Aruba 10G SFP+ to SFP+ 1m DAC Cable	X ¹	X ¹	X ¹	X ¹	X ¹
J9283D	Aruba 10G SFP+ to SFP+ 3m DAC Cable	X ¹	X ¹	X ¹	X ¹	X ¹
J9285D	Aruba 10G SFP+ to SFP+ 7m DAC Cable	X ¹	X ¹	X ¹	X ¹	X ¹
JH231A	HPE X142 40G QSFP+ MPO SR4 Transceiver					X ¹
JH232A	HPE X142 40G QSFP+ LC LR4 SM Transceiver					X ¹
JH233A	HPE X142 40G QSFP+ MPO eSR4 300M XCVR					X ¹
JH234A	HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable					X ¹
JH235A	HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable					X ¹
JH236A	HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable					X ¹
JH678A	HPE X140 40G QSFP+ LC BiDi 150m MM C-TRX					X ¹
JH700A	HPE X240 QSFP+ 4x10G SFP+DAC Reman C-Cbl					X ¹
JG329A	HPE X240 QSFP+ 4x10G SFP+ 1m DAC Cable					X ¹
JG331A	HPE X240 QSFP+ 4x10G SFP+ 5m DAC Cable					X ¹
JH231A	HPE X142 40G QSFP+ MPO SR4 Transceiver					X ¹
JH232A	HPE X142 40G QSFP+ LC LR4 SM Transceiver					X ¹
JH233A	HPE X142 40G QSFP+ MPO eSR4 300M XCVR					X ¹
JH234A	HPE X242 40G QSFP+ to QSFP+ 1m DAC Cable					X ¹
JH235A	HPE X242 40G QSFP+ to QSFP+ 3m DAC Cable					X ¹
JH236A	HPE X242 40G QSFP+ to QSFP+ 5m DAC Cable					X ¹
JL308A	Aruba 40G QSFP+ LC BiDi 150m MMFXCVR					X ¹

X: Supported transceiver

¹Default minimum ArubaOS software version is 6.5.3.0 and 8.1.0.0

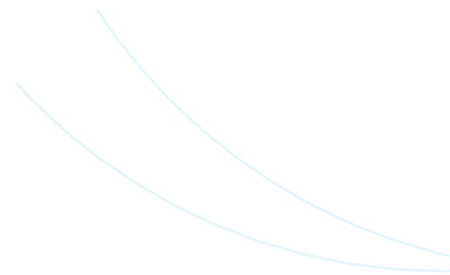
²Minimum ArubaOS software version is 6.5.4.7 and 8.4.0.0

³Minimum ArubaOS software version is 8.1.0.0



For additional information on the Aruba 7200 Series Mobility Controllers please refer to:

- ArubaOS Network Operating System Data Sheet (and licenses)
- 7200 Series Data Sheet
- 7200 Series Ordering Guide
- SD-WAN Data Sheet (and licenses)



DATA SHEET

ARUBA 500H SERIES HOSPITALITY ACCESS POINTS

High performance and cost-effective Wi-Fi 6 (802.11ax) for hospitality, branch, and teleworker deployments

These economical Wi-Fi 6 access points provide high-performance connectivity for any organization experiencing growing mobile, cloud and IoT requirements. With a wireless aggregate data rate of up to 1.5 Gbps and gigabit local wired ports, they deliver the range of connectivity options needed for venues such as hotels, residence halls, and remote offices alike.

INCREDIBLE EFFICIENCY

The 500H Series APs are designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.

Features include Orthogonal frequency-division multiple access (OFDMA), and cellular optimization. With up to 2 spatial streams (2SS) and 80MHz channel bandwidth, the 500H Series provides groundbreaking wireless capabilities for budget-conscious deployments.

Read the [Multi-User 802.11ax white paper](#) for further information.

Advantages of OFDMA

This capability allows Aruba's APs to handle multiple Wi-Fi 6 capable clients on each channel simultaneously, regardless of device or traffic type. Channel utilization is optimized by handling each transaction via smaller sub-carriers or resource units (RUs), which means that clients are sharing a channel and not competing for airtime and bandwidth.

Wi-Fi 6 aware client optimization

Aruba's patented AI-powered ClientMatch technology eliminates sticky client issues by placing Wi-Fi 6 capable devices on the best available AP. Session metrics are used to steer mobile devices to the best AP based on available bandwidth, types of applications being used and traffic type – even as users roam.

aruba

KEY FEATURES

- Combine wireless and wired access in a single compact form factor
- Ideal for organizations with work from home or teleworker initiatives
- Up to 1.5 Gbps of maximum wireless throughput
- 4 wired network ports and 1 Smart Rate uplink port
- WPA3 and Enhanced Open security
- Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices
- OFDMA for enhanced multi-user efficiency
- IoT-ready Bluetooth 5 and Zigbee support
- Aruba Fiber Media Converter optional add-on for seamless fiber backhaul

Advanced Cellular Coexistence (ACC)

This feature uses built-in filtering to automatically minimize the impact of interference from cellular networks, distributed antenna systems (DAS), and commercial small cell or femtocell equipment.

Intelligent Power Monitoring (IPM)

Aruba APs continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget (AP-505H).



IoT PLATFORM CAPABILITIES

Like all Aruba Wi-Fi 6 APs, the 500H Series includes an integrated Bluetooth 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors. This allows organizations to leverage the 500H Series as an IoT platform, which eliminates the need for an overlay infrastructure and additional IT resources.

Target Wake Time (TWT)

Ideal for IoTs that communicate infrequently, TWT establishes a schedule for when clients need to communicate with an AP. This helps improve client power savings and reduces airtime contention with other clients.

Advanced IoT Coexistence (AIC)

This feature uses built-in filtering to allow Wi-Fi and BLE/ Zigbee radios to operate at maximum capacity without the impact of interference

ARUBA SECURE INFRASTRUCTURE

The Aruba 500H Series includes security components to help protect user authentication and wireless traffic. Select capabilities include:

WPA3 and Enhanced Open

Support for stronger encryption and authentication is provided via the latest version of WPA for enterprise protected networks. Enhanced Open offers seamless new protection for users connecting to open networks where each session is automatically encrypted to protect user passwords and data on guest networks.

WPA2-MPSK

MPSK enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device or device type change, no additional changes are needed for other devices. This requires ClearPass Policy Manager.

VPN Tunnels

In Remote AP (RAP) and IAP-VPN deployments, the Aruba 500H Series can be used to establish a secure SSL/IPSec VPN tunnel to a Gateway or Mobility Controller that is acting as a VPN concentrator.

Trusted Platform Module (TPM)

For enhanced device assurance, all Aruba APs have an installed TPM for secure storage of credentials, keys and boot code.

SIMPLE AND SECURE ACCESS

To simplify policy enforcement, the Aruba 500H Series uses Aruba's Policy Enforcement Firewall (PEF) to encapsulate all traffic from the AP to the Mobility Controller (or gateway) for end-to-end encryption and inspection. Policies are applied based on user role, device type, applications, and location. This reduces the manual configuration of SSIDs, VLANs and ACLs. PEF also serves as the underlying technology for Aruba Dynamic Segmentation.

HIGH-DENSITY CONNECTIVITY

Each 500H Series AP provides connectivity for a maximum of 256 associated clients per radio (512 in total). In real-world scenarios, the maximum recommended client density is dependent on environmental conditions.

VERSATILE INSTALLATION OPTIONS

The APs can be deployed as a wall-mount or for remote teleworker environments, they can be converted to a desk-mount by using an optional accessory stand.

Aruba also offers a Fiber Media Converter that fits snugly alongside Aruba 500H Series Hospitality APs. It can transparently convert fiber to copper Ethernet, convert DC power to POE, and extend the reach of the AP.

FLEXIBLE OPERATION AND MANAGEMENT

Our unified APs can operate as standalone access points or with a gateway for greater scalability, security, and manageability. APs can be deployed using zero touch provisioning – without on-site technical expertise – for ease of implementation in branch offices and for remote work. Aruba APs can be managed using cloud-based or on-premises solutions for any campus, branch, or remote work environment.

As the management and orchestration console for Aruba ESP (Edge Services Platform), Aruba Central provides a single pane of glass for overseeing every aspect of wired and wireless LANs, WANs, and VPNs. AI-powered analytics, end-to-end orchestration and automation, and advanced security features are built natively into the solution.

SMALL OFFICE/HOME OFFICE FOR HYBRID WORK

For hybrid environments, EdgeConnect Microbranch extends the WAN to the small office/home office to deliver a consistent employee experience no matter where users



are located. EdgeConnect Microbranch offers a suite of SD-WAN capabilities to optimize performance, security, and manageability via cloud-based Aruba Central and the Aruba AP itself. With EdgeConnect Microbranch, organizations can extend existing remote access point (RAP) capabilities to benefit from policy-based routing, tunnel and route orchestration, and SASE integration to cloud security services such as Zscaler.

For large installations across multiple sites, APs can be factory-shipped and can be activated with Zero Touch Provisioning through Aruba Central or AirWave. This reduces deployment time, centralizes configuration, and helps manage inventory.

500H Remote AP bundles

To simplify the ordering and distribution of 500H access points, we offer a number of AP bundles that combine an AP variant a desk stand, power adapter, and North American or European power cord. This makes it easier to get remote workers and small branches up and running quickly.



Access point with optional stand shown



TECHNICAL SPECIFICATIONS	
Hardware variants	
AP type	<ul style="list-style-type: none"> AP-503H: Mid-range dual radio Wi-Fi 6 Hospitality AP with 1+2 Ethernet ports AP-505H: High-end dual radio Wi-Fi 6 Hospitality AP with 1+4 Ethernet ports, PSE, USB
Wi-Fi radio and platform specifications	
5GHz radio	Two spatial stream (SU) MIMO for up to 1.2Gbps wireless data rate (HE80)
2.4GHz radio	Two spatial stream (SU) MIMO for up to 287Mbps wireless data rate (HE20) Note: HE40 operation is supported in 2.4GHz, but uncommon and not recommended for enterprise deployments
Maximum number of associated client devices	Up to 256 associated client devices per radio
Maximum number of BSSIDs	16 BSSIDs per radio
Supported frequency bands (country-specific restrictions apply)	<ul style="list-style-type: none"> 2.400 to 2.4835GHz ISM 5.150 to 5.250GHz U-NII-1 5.250 to 5.350GHz U-NII-2A 5.470 to 5.725GHz U-NII-2C 5.725 to 5.850GHz U-NII-3/ISM 5.850 to 5.895GHz U-NII-4
Dynamic frequency selection (DFS) optimizes the use of available RF spectrum	
Supported radio technologies	<ul style="list-style-type: none"> 802.11b: Direct-sequence spread-spectrum (DSSS) 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM) 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 8 resource units
Supported modulation types:	<ul style="list-style-type: none"> 802.11b: BPSK, QPSK, CCK 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension) 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (proprietary extension) 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
802.11n high-throughput (HT) support	HT20/40
802.11ac very high throughput (VHT) support:	VHT20/40/80
802.11ax high efficiency (HE) support:	HE20/40/80
Supported data rates (Mbps):	<ul style="list-style-type: none"> 802.11b: 1, 2, 5.5, 11 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40), 400 with 256-QAM 802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS = 1 to 2, VHT20 to VHT80), 1,083 with 1024-QAM 802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40) 802.11ax (5GHz): 3.6 to 1,201 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE80)
802.11n/ac/ax packet aggregation:	A-MPDU, A-MSDU
Transmit power	Configurable in increments of 0.5 dBm
Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements):	<ul style="list-style-type: none"> 2.4 GHz band: +20 dBm (17 dBm per chain) 5 GHz band: +21 dBm (18 dBm per chain) Note: conducted transmit power levels exclude antenna gain. For total (EIRP) transmit power, add antenna gain
Minimum configurable transmit power level	0dBm (conducted, per chain)
VPN IPsec throughput performance	100 Mbps (AP-503H) and 500 Mbps or better (AP-505H)



- Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks
- Advanced IOT Coexistence (AIC) allows concurrent operation of multiple radios in the 2.4GHz band (AP-505H)
- Maximum ratio combining (MRC) for improved receiver performance
- Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance
- Space-time block coding (STBC) for increased range and improved reception
- Low-density parity check (LDPC) for high-efficiency error correction and increased throughput
- Transmit beam-forming (TxBF) for increased signal reliability and range
- 802.11ax Target Wait Time (TWT) to support low-power client devices

WI-FI ANTENNAS

AP-503H

- Two integrated semi-directional antennas for 2x2 MIMO with peak single antenna gain of 2.5dBi in 2.4GHz and 5.6dBi in 5GHz. Built-in antennas are optimized for vertical wall or desk mounted orientation of the AP.
 - Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 1.7dBi in 2.4GHz and 5.0dBi in 5GHz.

AP-505H

- Two integrated semi-directional antennas for 2x2 MIMO with peak single antenna gain of 5.2dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for vertical wall or desk mounted orientation of the AP.
 - Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 3.3dBi in 2.4GHz and 2.9dBi in 5GHz.

OTHER INTERFACES

Uplink (E0)

- AP-503H: Ethernet wired network port (RJ45)
- Auto-sensing link speed (10/100/1000BASE-T) and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
 - POE-PD: 802.3af POE (class 3)
- AP-505H: Smart Rate Ethernet wired network port (RJ45)
- Auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDX
 - 2.5Gbps speed complies with NBase-T and 802.3bz specifications
 - 802.3az Energy Efficient Ethernet (EEE)
 - POE-PD: 48Vdc (nominal) 802.3af/at/bt POE (class 3, 4 or 6)

Local

- AP-503H (E1-E2): Two Ethernet wired network ports (RJ45)
- Auto-sensing link speed (10/100/1000BASE-T) and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
- AP-505H (E1-E4): Four Ethernet wired network ports (RJ45)
- Auto-sensing link speed (10/100/1000BASE-T) and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
 - E1 & E2: POE-PSE: 802.3af/at POE output; dual 802.3af (both ports) or single 802.3at (E1 only)



OTHER INTERFACES	
DC power interface	<p>AP-503H:</p> <ul style="list-style-type: none"> • 12Vdc (nominal, +/- 5%), accepts 2.1mm/5.5mm center-positive circular plug with 9.5mm length <p>AP-505H</p> <ul style="list-style-type: none"> • 48Vdc (nominal, +/- 5%), accepts 1.35mm/3.5mm center-positive circular plug with 9.5mm length
USB 2.0 host interface (Type A connector)	<p>AP-505H</p> <ul style="list-style-type: none"> • Cellular modems • IOT or other plug-in accessories • Device battery charging port • Capable of sourcing up to 1A / 5W to an attached device
Bluetooth Low Energy (BLE5.0) and Zigbee (802.15.4) radio	<ul style="list-style-type: none"> • BLE: up to 7dBm transmit power (class 1) and -100dBm receive sensitivity (125kbps) • Zigbee: up to 7dBm transmit power and -97dBm receive sensitivity (250kbps) • Integrated semi-directional antenna with peak gain of 2.5dBi (AP-503H) or 1.2dBi (AP-505H)
Visual indicators (two multi-color LEDs):	<ul style="list-style-type: none"> • Power/System status • Radio status • Local network port status (2x on AP-503H, 4x on AP-505H) • POE-PSE status (2x) (applies to AP-505H only)
Reset button:	Factory reset, LED mode control (normal/off)
Serial console interface	Proprietary, micro-B USB physical jack
Crypto performance	<ul style="list-style-type: none"> • Up to 500Mbps



POWER SOURCES AND POWER CONSUMPTION	
Power Sources: The AP supports direct DC power and Power over Ethernet	<ul style="list-style-type: none"> The AP supports direct DC power and Power over Ethernet When both DC and POE power sources are available, DC power takes priority over POE¹ Power sources are sold separately; see the 500H Series Ordering Guide for details <p>AP-505H</p> <ul style="list-style-type: none"> When powered by DC or 802.3bt (class 6) POE, the AP will operate without restrictions When powered by 802.3at (class 4) POE and with the IPM feature disabled, the AP will disable the USB port (only) if POE-PSE is enabled, and support (802.3af) POE-PSE power on E1 only (no PSE on E2) When powered by 802.3af (class 3) POE with the IPM feature disabled, the AP will disable the USB port and POE-PSE capability With IPM enabled, the AP will start up without restrictions, but may dynamically apply additional restrictions depending on the POE budget and actual power consumption. The feature specific restrictions and order in which they are applied can be configured
Maximum (worst-case) power consumption (without USB or PSE / max):	<p>AP-503H</p> <ul style="list-style-type: none"> DC powered: 10.0W POE powered (802.3af): 11.4W <p>AP-505H</p> <ul style="list-style-type: none"> DC powered: 14W / 50W POE powered (802.3bt): 14W / 51W POE powered (802.3at): 14W / 25.5W POE powered (802.3af): 13.5W / 13.5W
Maximum (worst-case) power consumption in idle mode (without USB or PSE)	<p>AP-503H: 4.5W (POE)</p> <p>AP-505H: 6.2W (POE)</p>
Maximum (worst-case) power consumption in deep-sleep mode (without USB or PSE)	<p>AP-503H: 2.7W (POE)</p> <p>AP-505H: 3.5W (POE)</p>

MECHANICAL SPECIFICATIONS	
Dimensions/weight (unit, excluding mount bracket):	<p>AP-503H:</p> <ul style="list-style-type: none"> 86mm (W) x 40mm (D) x 150mm (H) 290g <p>AP-505H:</p> <ul style="list-style-type: none"> 86mm (W) x 47mm (D) x 150mm (H) 360g
Dimensions/weight (shipping):	<p>AP-503H:</p> <ul style="list-style-type: none"> 111mm (W) x 54mm (D) x 167mm (H) 380g <p>AP-505H:</p> <ul style="list-style-type: none"> 111mm (W) x 54mm (D) x 167mm (H) 450g
Mounting details	Using one of the (separate orderable) mount kits, the AP can be attached to a single or dual gang wall-box, directly to a wall, or desk mounted. See the 500H Series Ordering Guide for details.

¹ AP-505H only. AP-503H does not support simultaneous connection of POE and DC power sources.



ENVIRONMENTAL SPECIFICATIONS

Operating conditions	<ul style="list-style-type: none"> • Temperature: 0C to +40C / +32F to +104F • Humidity: 5% to 93% non-condensing • ETS 300 019 class 3.2 environments
Storage and transportation conditions	<ul style="list-style-type: none"> • Temperature: -40C to +70C / -40F to +158F • Humidity: 5% to 93% non-condensing • ETS 300 019 classes 1.2 and 2.3 environments

RELIABILITY

Mean Time Between Failure (MTBF):	<p>AP-503H: 1,360 khrs (155 yrs) at +25C operating temperature AP-505H: 780khrs (88yrs) at +25C operating temperature.</p>
-----------------------------------	---

REGULATORY AND SAFETY COMPLIANCE

Regulatory model numbers	<ul style="list-style-type: none"> • AP-503H (all variants): APINH503 • AP-505H (all variants): APINH505
Minimum Software Release	<ul style="list-style-type: none"> • ArubaOS and Aruba InstantOS 8.7.1.0 (AP-503H) and 8.7.0.0 (AP-505H)
Regulatory compliance (For more country-specific regulatory information and approvals, please see your Aruba representative.)	<ul style="list-style-type: none"> • FCC/ISED • CE Marked • RED Directive 2014/53/EU • EMC Directive 2014/30/EU • Low Voltage Directive 2014/35/EU • IEC/EN 60950 • EN 60601-1-1, EN60601-1-2 • IEC/EN 62368-1
Certifications	<ul style="list-style-type: none"> • Wi-Fi Alliance: <ul style="list-style-type: none"> - Wi-Fi CERTIFIED a, b, g, n, ac - Wi-Fi CERTIFIED 6 (ax) - WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) - WMM, WMM-PS, Wi-Fi Agile Multiband - Passpoint (release 2) • Bluetooth SIG (AP-505H only) • Ethernet Alliance (POE)

For more and country-specific regulatory information and approvals, please see your Aruba representative.
 Aruba's hardware limited lifetime warranty.



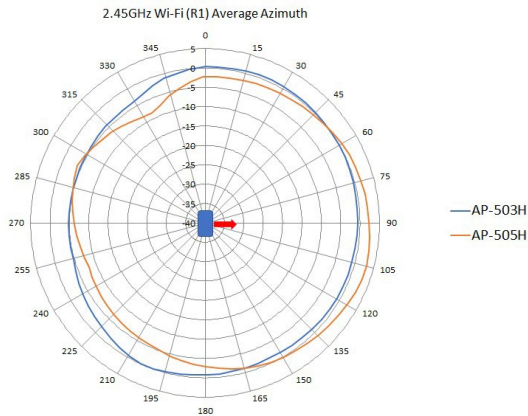
RF PERFORMANCE TABLE		
	Maximum transmit power (dBm) per transmit chain	Receiver sensitivity (dBm) per receive chain
2.4GHz, 802.11b		
1Mbps	17	-94
11Mbps	17	-86
2.4GHz, 802.11g		
6Mbps	17	-89
54Mbps	17	-73
2.4GHz, 802.11n HT20		
MCS0	17	-89
MCS7	15	-69
2.4GHz, 802.11ax HE20		
MCS0	17	-89
MCS11	11	-60
5GHz, 802.11a		
6Mbps	18	-92
54Mbps	18	-74
5GHz, 802.11n HT20		
MCS0	18	-91
MCS7	16	-71
5GHz, 802.11n HT40		
MCS0	18	-88
MCS7	16	-78
5GHz, 802.11ac VHT20		
MCS0	18	-91
MCS9	14	-67
5GHz, 802.11ac VHT40		
MCS0	18	-90
MCS9	14	-64
5GHz, 802.11ac VHT80		
MCS0	18	-86
MCS9	14	-63
5GHz, 802.11ax HE20		
MCS0	18	-91
MCS11	12	-62
5GHz, 802.11ax HE40		
MCS0	18	-90
MCS11	12	-59
5GHz, 802.11ax HE80		
MCS0	18	-87
MCS11	12	-56



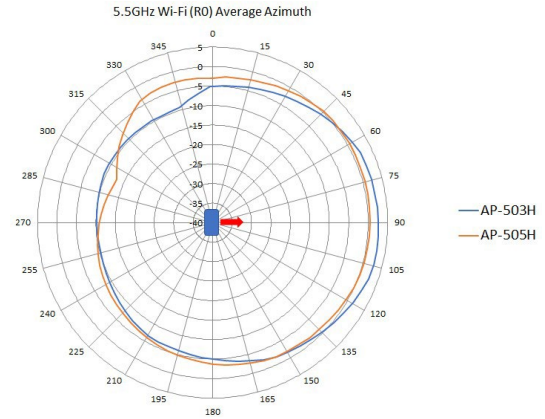
ANTENNA PATTERNS

Horizontal or azimuth plane (looking at the top of the AP, front facing to the right)

(averaged patterns for all applicable antennas)



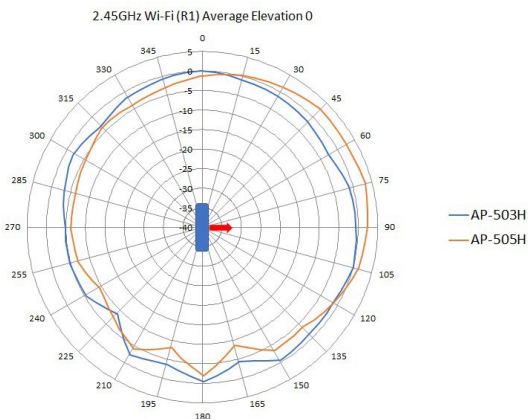
2.45GHz Wi-Fi (antennas 0, 1)



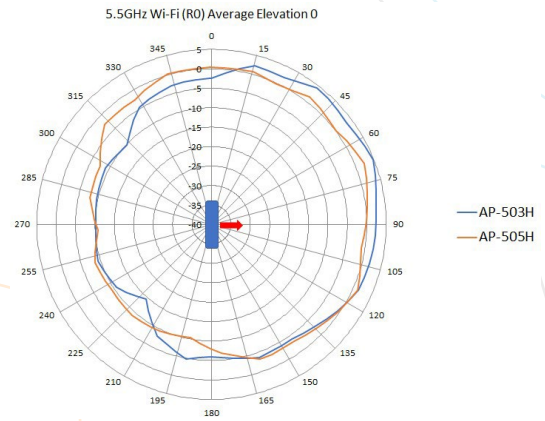
5.5GHz Wi-Fi (antennas 0, 1)

Vertical (elevation) plane 0 (looking at the side of the AP, front facing to the right)

(averaged patterns for all applicable antennas)



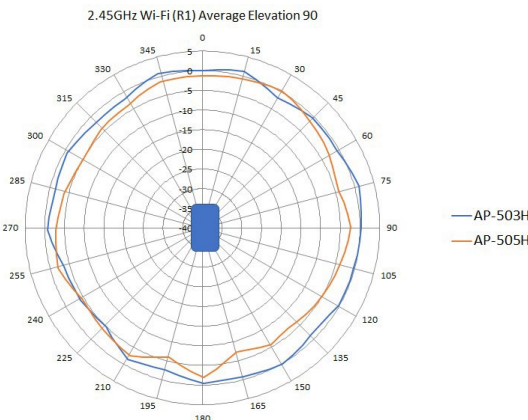
2.45GHz Wi-Fi (antennas 0, 1)



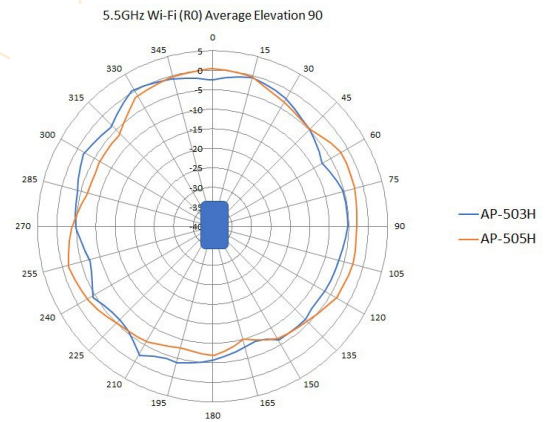
5.5GHz Wi-Fi (antennas 0, 1)

Vertical (elevation) plane 90 (looking at the front of the AP)

(averaged patterns for all applicable antennas)



2.45GHz Wi-Fi (antennas 0, 1)



5.5GHz Wi-Fi (antennas 0, 1)



ORDERING INFORMATION

Part Number	Description
Aruba 500H Series Hospitality Access Points	
AP-503H access points	
R3V44A	Aruba AP-503H (EG) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V42A	Aruba AP-503H (IL) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V40A	Aruba AP-503H (JP) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V36A	Aruba AP-503H (RW) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V38A	Aruba AP-503H (US) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R7G96A	Aruba AP-503HR (EU) Remote AP bundle with AP-503H (RW) + desk mount + power adapter + EU power cord
R7G97A	Aruba AP-503HR (US) Remote AP bundle with AP-503H (US) + desk mount + power adapter + NA power cord
AP-505H access points	
R3V54A	Aruba AP-505H (EG) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V52A	Aruba AP-505H (IL) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V50A	Aruba AP-505H (JP) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V46A	Aruba AP-505H (RW) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V48A	Aruba AP-505H (US) Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V56A	Aruba AP-505HR (EU) Remote AP bundle with AP-505H (RW) + desk mount + power adapter + EU power cord
R3V57A	Aruba AP-505HR (US) Remote AP bundle with AP-505H (US) + desk mount + power adapter + NA power cord
AP-503H access points – TAA models	
R3V45A	Aruba AP-503H (EG) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V43A	Aruba AP-503H (IL) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V41A	Aruba AP-503H (JP) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V37A	Aruba AP-503H (RW) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
R3V39A	Aruba AP-503H (US) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+2 Ethernet
AP-505H access points – TAA models	
R3V55A	Aruba AP-505H (EG) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V53A	Aruba AP-505H (IL) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V51A	Aruba AP-505H (JP) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V47A	Aruba AP-505H (RW) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB
R3V49A	Aruba AP-505H (US) TAA Dual-radio 802.11ax 2x2 Unified Hospitality AP with 1+4 Ethernet, PSE, USB

For compatible accessories and spares, see the 500H Series Ordering Guide.



© Copyright 2022 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

DS_Aruba500HSeries_RVK_120222 a00096366enw

Contact us at www.arubanetworks.com/contact

DATA SHEET

ARUBA 500 SERIES CAMPUS ACCESS POINTS

Cost-effective Wi-Fi 6 (802.11ax) for medium-density indoor environments

These affordable Wi-Fi 6 access points provide high-performance connectivity for any organization experiencing growing numbers of mobile, IoT and mobility requirements. With a maximum real-world aggregate data rate of 1.49 Gbps (HE80/HE20), they deliver the speed and reliability needed for venues and workplaces such as schools, midsize offices and retailers.

INCREDIBLE EFFICIENCY

The 500 Series APs are also designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.

Features include Orthogonal frequency-division multiple access (OFDMA), and cellular optimization. With up to 2 spatial streams (2SS) and 80MHz channel bandwidth (HE80), the 500 Series provides groundbreaking wireless capabilities for budget-conscious deployments.

Read the [Wi-Fi 6 Reference Guide](#) for further information.

Advantages of OFDMA

This capability allows Aruba's APs to handle multiple Wi-Fi 6 capable clients on each channel simultaneously, regardless of device or traffic type. Channel utilization is optimized by handling each transaction via smaller sub-carriers or resource units (RUs), which means that clients are sharing a channel and not competing for airtime and bandwidth.

Aruba Air Slice™ for Extended Application Assurance

Initially, APs in controller-less mode (Instant) can provide SLA-grade performance by allocating radio resources, such as time, frequency, and spatial streams, to specific traffic



KEY FEATURES

- 1.49 Gbps maximum real-world speed (HE80/HE20)
- WPA3 and Enhanced Open security
- Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices
- OFDMA for enhanced multi-user efficiency
- IoT-ready Bluetooth 5 and Zigbee support

types. By combining Aruba's Policy Enforcement Firewall (PEF) and Layer 7 deep packet inspection (DPI) to identify user roles and applications, the APs will dynamically allocate the bandwidth needed. Non-Wi-Fi 6 clients can also benefit.

Air Slice™ for APs uses Aruba Central for management. Controller-based APs will be supported in a future software release.



Wi-Fi 6 aware client optimization

Aruba's patented AI-powered ClientMatch technology eliminates sticky client issues by placing Wi-Fi 6 capable devices on the best available AP. Session metrics are used to steer mobile devices to the best AP based on available bandwidth, types of applications being used and traffic type – even as users roam.

Aruba Advanced Cellular Coexistence (ACC)

This feature uses built-in filtering to automatically minimize the impact of interference from cellular networks, distributed antenna systems (DAS), and commercial small cell or femtocell equipment.

Intelligent Power Monitoring (IPM)

Aruba APs continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.

IOT PLATFORM CAPABILITIES

Like all Aruba Wi-Fi 6 APs, the 500 Series includes an integrated Bluetooth 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors. This allows organizations to leverage the 500 Series as an IoT platform, which eliminates the need for an overlay infrastructure and additional IT resources.

Target Wake Time (TWT)

Ideal for IoTs that communicate infrequently, TWT establishes a schedule for when clients need to communicate with an AP. This helps improve client power savings and reduces airtime contention with other clients.

ARUBA SECURE INFRASTRUCTURE

The Aruba 500 Series includes components of Aruba's 360 Secure Fabric to help protect user authentication and wireless traffic. Select capabilities include:

WPA3 and Enhanced Open

Support for stronger encryption and authentication is provided via the latest version of WPA for enterprise protected networks.

Enhanced Open offers seamless new protection for users connecting to open networks where each session is automatically encrypted to protect user passwords and data on guest networks.

WPA2-MPSK

MPSK enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device or device type change, no additional changes are needed for other devices. Requires ClearPass Policy Manager.

VPN Tunnels

In Remote AP (RAP) and IAP-VPN deployments, the Aruba 500 Series can be used to establish a secure SSL/IPSec VPN tunnel to a Mobility Controller that is acting as a VPN concentrator.

Trusted Platform Module (TPM)

For enhanced device assurance, all Aruba APs have an installed TPM for secure storage of credentials and keys, and boot code.

SIMPLE AND SECURE ACCESS

To simplify policy enforcement, the Aruba 500 Series uses Aruba's policy enforcement firewall (PEF) feature to encapsulate all traffic from the AP to the Mobility Controller (or Gateway) for end-to-end encryption and inspection. Policies are applied based on user role, device type, applications, and location. This reduces the manual configuration of SSIDs, VLANs and ACLs. PEF also serves as the underlying technology for Aruba Dynamic Segmentation.

HIGH-DENSITY CONNECTIVITY

Each 500 Series AP provides connectivity for a maximum of 256 associated clients per radio (512 in total). In real-world scenarios, the maximum recommended client density is dependent on environmental conditions.



FLEXIBLE OPERATION AND MANAGEMENT

Our unified APs can operate as standalone access points or with a gateway for greater scalability, security, and manageability. APs can be deployed using zero touch provisioning – without on-site technical expertise – for ease of implementation in branch offices and for remote work.

Aruba APs can be managed using cloud-based or on-premises solutions for any campus, branch, or remote work environment. As the management and orchestration console for Aruba ESP (Edge Services Platform), Aruba Central provides a single pane of glass for overseeing every aspect of wired and wireless LANs, WANs, and VPNs. AI-powered analytics, end-to-end orchestration and automation, and advanced security features are built natively into the solution.

ADDITIONAL WI-FI FEATURES

Each AP also includes the following standards-based technologies:

Transmit beamforming (TxBF)	Increased signal reliability and range
Passpoint Wi-Fi (Release 2) (Hotspot 2.0)	Seamless cellular-to-Wi-Fi carryover for guests
Dynamic Frequency Selection (DFS)	Optimized use of available RF spectrum
Maximum Ratio Combining (MRC)	Improved receiver performance
Cyclic Delay/Shift Diversity (CDD/CSD)	Greater downlink RF performance
Space-Time Block Coding	Increased range and improved reception
Low-Density Parity Check (LDPC)	High-efficiency error correction for increased throughput



TECHNICAL SPECIFICATIONS		
Model	AP-504	AP-505
AP type	Indoor, dual radio, 5GHz and 2.4GHz 802.11ax 2x2 MIMO	
5GHz radio	Two spatial stream Single User (SU) MIMO for up to 1.2Gbps wireless data rate with 2SS HE80 802.11ax client devices	
2.4GHz radio	Two spatial stream Single User (SU) MIMO for up to 574Mbps (287 Mbps) wireless data rate with 2SS HE40 (HE20) 802.11ax client devices	
Maximum number of associated client devices	Up to 256 associated client devices per radio	
Maximum number of BSSIDs	16 BSSIDs per radio	
Supported frequency bands (country-specific restrictions apply)	<ul style="list-style-type: none"> • 2.400 to 2.4835GHz ISM • 5.150 to 5.250GHz U-NII-1 • 5.250 to 5.350GHz U-NII-2A • 5.470 to 5.725GHz U-NII-2C • 5.725 to 5.850GHz U-NII-3/ISM • 5.850 to 5.895GHz U-NII-4 	
Available channels	Dependent on configured regulatory domain	
Supported radio technologies	<ul style="list-style-type: none"> • 802.11b: Direct-sequence spread-spectrum (DSSS) • 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM) • 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 8 resource units 	
Supported modulation types:	<ul style="list-style-type: none"> • 802.11b: BPSK, QPSK, CCK • 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension) • 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (proprietary extension) • 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM 	
802.11n high-throughput (HT) support:	HT20/40	
802.11ac very high throughput (VHT) support:	VHT20/40/80	
802.11ax high efficiency (HE) support:	HE20/40/80	
Supported data rates (Mbps):	<ul style="list-style-type: none"> • 802.11b: 1, 2, 5.5, 11 • 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 • 802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40), 400 with 256-QAM • 802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS = 1 to 2, VHT20 to VHT80), 1,083 with 1024-QAM • 802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40) • 802.11ax (5GHz): 3.6 to 1,201 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE80) 	
802.11n/ac/ax packet aggregation:	A-MPDU, A-MSDU	
Transmit power:	Configurable in increments of 0.5 dBm	
Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements):	2.4 GHz band: +21 dBm (18dBm per chain) 5 GHz band: +21 dBm (18 dBm per chain) Note: conducted transmit power levels exclude antenna gain. For total (EIRP) transmit power, add antenna gain.	



WI-FI ANTENNAS

AP-504	AP-505
Two (female) RP-SMA connectors for external dual band antennas (A0 and A1, corresponding with radio chains 0 and 1). Worst-case internal loss between radio interface and external antenna connectors (due to diplexing circuitry): 0.7dB in 2.4GHz and 1.3dB in 5GHz.	Two integrated dual-band downtilt omni-directional antennas for 2x2 MIMO with peak antenna gain of 4.9dBi in 2.4GHz and 5.7dBi in 5GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees. <ul style="list-style-type: none"> Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 4.3dBi in 2.4GHz and 5.6dBi in 5GHz.

OTHER INTERFACES

Model	AP-504	AP-505
E0: Ethernet wired network port (RJ-45)	<ul style="list-style-type: none"> Auto-sensing link speed (10/100/1000BASE-T) and MDI/MDX POE-PD: 48Vdc (nominal) 802.3af/at POE (class 3 or 4) 802.3az Energy Efficient Ethernet (EEE) 	
DC power interface	12Vdc (nominal, +/- 5%), accepts 2.1mm/5.5mm center-positive circular plug with 9.5mm length	
USB 2.0 host interface (Type A connector)	Capable of sourcing up to 1A / 5W to an attached device	
Bluetooth Low Energy (BLE5.0) and Zigbee (802.15.4) radio	<ul style="list-style-type: none"> BLE: up to 7dBm transmit power (class 1) and -93dBm receive sensitivity (1Mbps) Zigbee: up to 6dBm transmit power and -96dBm receive sensitivity Integrated vertically polarized omnidirectional antenna with roughly 30 degrees downtilt and peak gain of 3.3dBi	
Visual indicators (two multi-color LEDs):	For System and Radio status	
Reset button:	Factory reset, LED mode control (normal/off)	
Serial console interface	Proprietary, micro-B USB physical jack	
Security slot	Kensington security slot	

POWER SOURCES AND POWER CONSUMPTION

Model	AP-504	AP-505
Power Sources: The AP supports direct DC power and Power over Ethernet	<ul style="list-style-type: none"> The AP supports direct DC power and Power over Ethernet When both DC and POE power sources are available, DC power takes priority over POE Power sources are sold separately; see the 500 Series Ordering Guide for details When powered by DC or 802.3at (class 4) POE, the AP will operate without restrictions. When powered by 802.3af (class 3) POE and with the IPM feature disabled, the AP will disable the USB port. In the same configuration but with IPM enabled, the AP will start up in unrestricted mode, but may dynamically apply restrictions depending on the POE budget and actual power. The feature restrictions and order can be programmed. 	
Maximum (worst-case) power consumption (without / with a USB device attached):	<ul style="list-style-type: none"> DC powered: 8.9W / 14.2W. POE powered (802.3at): 11.0W / 16.5W. POE powered (802.3af): 11.0W / 13.5W. This assumes that up to 5W is supplied to the attached USB device. 	
Maximum (worst-case) power consumption in idle mode:	4.3W (DC) or 6.2W (POE).	
Maximum (worst-case) power consumption in deep-sleep mode:	1.7W (DC) or 3.7W (POE).	



MECHANICAL SPECIFICATIONS	
Model	AP-505
Dimensions/weight (AP-505; unit, excluding mount bracket):	160mm (W) x 161mm (D) x 37mm (H) 500g
Dimensions/weight (AP-505; shipping):	193mm (W) x 183mm (D) x 63mm (H) 645g
Mounting details	A mounting bracket has been pre-installed on the back of the AP. This bracket is used to secure the AP to any of the mount kits (sold separately); see the 500 Series Ordering Guide for details.

ENVIRONMENTAL SPECIFICATIONS		
Model	AP-504	AP-505
Operating conditions	<ul style="list-style-type: none"> • Temperature: 0C to +50C / +32F to +122F • Humidity: 5% to 93% non-condensing • AP is plenum rated for use in air-handling spaces • ETS 300 019 class 3.2 environments 	
Storage and transportation conditions	<ul style="list-style-type: none"> • Temperature: -40C to +70C / -40F to +158F • Humidity: 5% to 93% non-condensing • ETS 300 019 classes 1.2 and 2.3 environments 	

RELIABILITY		
Model	AP-504	AP-505
Mean Time Between Failure (MTBF):	1.3Mhrs (148yrs) at +25C operating temperature.	

REGULATORY AND SAFETY COMPLIANCE		
Model	AP-504	AP-505
Regulatory model numbers	APIN0504	APIN0505
Minimum ArubaOS Release	ArubaOS and Aruba InstantOS 8.6.0.0	
Regulatory compliance (For more country-specific regulatory information and approvals, please see your Aruba representative.)	<ul style="list-style-type: none"> • FCC/ISED • CE Marked • RED Directive 2014/53/EU • EMC Directive 2014/30/EU • Low Voltage Directive 2014/35/EU • UL/IEC/EN 60950 • EN 60601-1-1, EN60601-1-2 	<ul style="list-style-type: none"> • Railway Certs (AP-505 Only): <ul style="list-style-type: none"> - EN 50155:2017 - Railway Applications - EN 50121-1:2017 – Railway EMC - EN 50121-3-2 – Railway EMC - EN 50121-4:2016 - Railway Immunity - IEC 61373 ed2:2008 - Railway Shock and Vibration
Certifications	<ul style="list-style-type: none"> • UL2043 plenum rating • Wi-Fi Alliance: <ul style="list-style-type: none"> - Wi-Fi CERTIFIED a, b, g, n, ac - Wi-Fi CERTIFIED 6 (ax) - WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) - WMM, WMM-PS, W-Fi Agile Multiband - Passpoint (release 2) - Wi-Fi Location • Bluetooth SIG • Ethernet Alliance (POE, PD device, class 4) 	



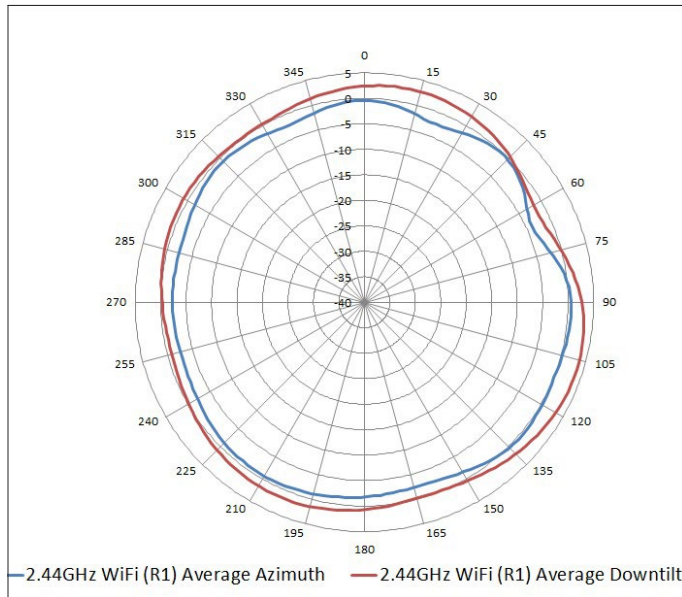
RF PERFORMANCE TABLE		
Band, rate	Maximum transmit power (dBm) per transmit chain	Receiver sensitivity (dBm) per receive chain
2.4GHz, 802.11b		
1Mbps	18	-98
11Mbps	18	-90
2.4GHz, 802.11g		
6Mbps	18	-93
54Mbps	18	-76
2.4GHz, 802.11n HT20		
MCS0	18	-93
MCS7	16	-75
2.4GHz, 802.11ax HE20		
MCS0	18	-93
MCS11	14	-62
5GHz, 802.11a		
6Mbps	18	-92
54Mbps	18	-75
5GHz, 802.11n HT20		
MCS0	18	-92
MCS7	16	-74
5GHz, 802.11n HT40		
MCS0	18	-90
MCS7	16	-71
5GHz, 802.11ac VHT20		
MCS0	18	-92
MCS9	16	-69
5GHz, 802.11ac VHT40		
MCS0	18	-90
MCS9	16	-65
5GHz, 802.11ac VHT80		
MCS0	18	-87
MCS9	16	-62
5GHz, 802.11ax HE20		
MCS0	18	-93
MCS11	14	-62
5GHz, 802.11ax HE40		
MCS0	18	-90
MCS11	14	-59
5GHz, 802.11ax HE80		
MCS0	18	-87
MCS11	14	-56



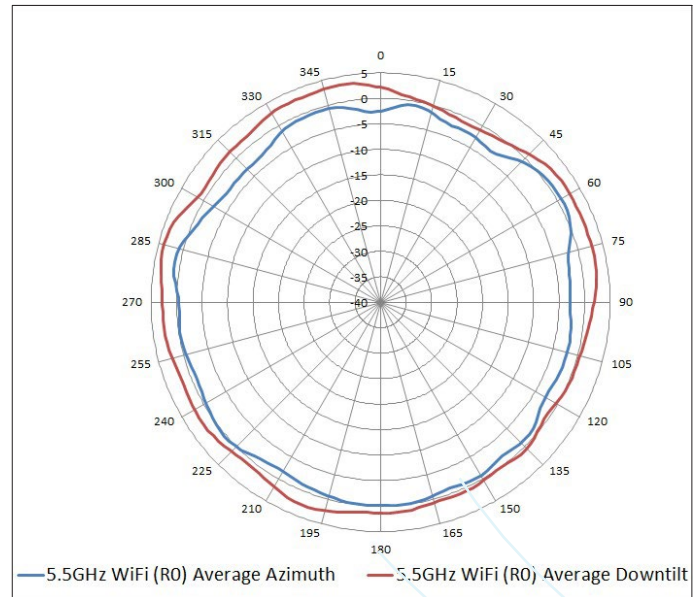
ANTENNA PATTERNS

Horizontal planes (top view)

Showing azimuth (0 degrees) and 30 degrees downtilt patterns (averaged patterns for all applicable antennas)



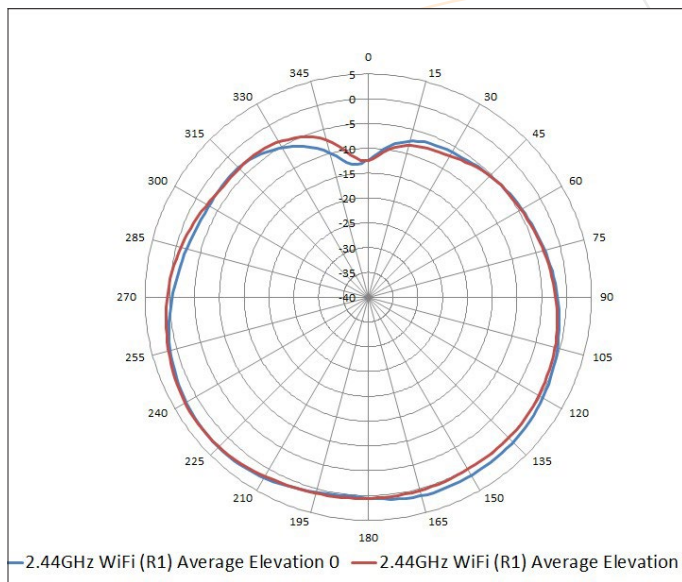
2.44GHz Wi-Fi (antennas 1, 2)



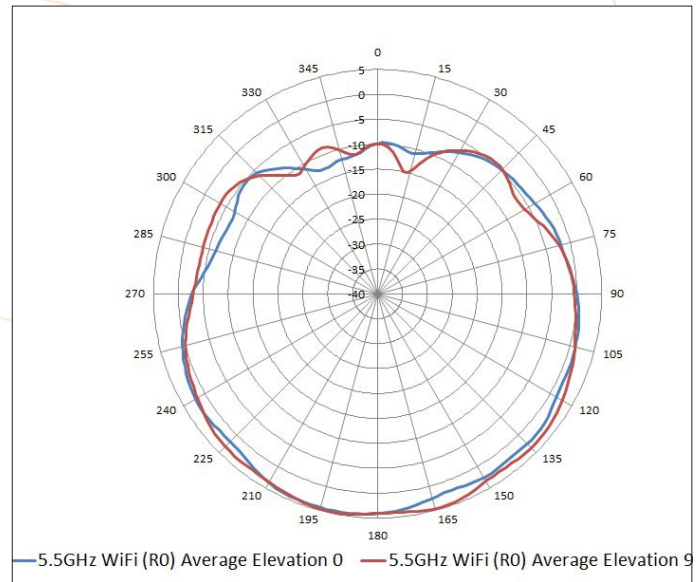
5.5GHz Wi-Fi (antennas 1, 2)

Vertical (elevation) planes (side view, AP facing down)

Showing side view with AP rotated 0 and 90 degrees (averaged patterns for all applicable antennas)



2.44GHz Wi-Fi (antennas 1, 2)



5.5GHz Wi-Fi (antennas 1, 2)



ORDERING INFORMATION

Part number	Description
Aruba 500 Series Campus Access Points	
Internal antenna access points	
R2H25A	Aruba AP-505 (EG) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H26A	Aruba AP-505 (IL) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H27A	Aruba AP-505 (JP) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H28A	Aruba AP-505 (RW) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H28ACM	Aruba CM AP-505 (RW) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H29ACM	Aruba CM AP-505 (US) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H29A	Aruba AP-505 (US) Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
External antenna access points	
R2H19A	Aruba AP-504 (EG) Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H20A	Aruba AP-504 (IL) Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H21A	Aruba AP-504 (JP) Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H22A	Aruba AP-504 (RW) Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H23A	Aruba AP-504 (US) Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
Internal antenna access points – TAA models	
R2H35A	Aruba AP-505 (EG) TAA Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H36A	Aruba AP-505 (IL) TAA Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H37A	Aruba AP-505 (JP) TAA Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H38A	Aruba AP-505 (RW) TAA Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
R2H39A	Aruba AP-505 (US) TAA Dual Radio 2x2:2 802.11ax Internal Antennas Unified Campus AP
External antenna access points – TAA models	
R2H30A	Aruba AP-504 (EG) TAA Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H31A	Aruba AP-504 (IL) TAA Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H32A	Aruba AP-504 (JP) TAA Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H33A	Aruba AP-504 (RW) TAA Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
R2H34A	Aruba AP-504 (US) TAA Dual Radio 2x2:2 802.11ax External Antennas Unified Campus AP
For compatible accessories, see the 500 Series Ordering Guide	

Note: All hardware SKUs can be managed by Aruba Central. Central Managed (CM) SKUs are used for simplified ordering within US and Canada only.

Resources:

500 Series Ordering Guide

DATA SHEET

ARUBA 510 SERIES CAMPUS ACCESS POINTS

Very high Wi-Fi 6 (802.11ax) performance with dual radios

Aruba Wi-Fi 6 access points provide high-performance connectivity for any organization experiencing growing numbers of IoT and mobility requirements. With a combined peak data rate of up to 2.69Gbps, they deliver the speed and reliability needed for any enterprise environment.

INCREDIBLE EFFICIENCY

The 510 Series APs are also designed to optimize user experience by maximizing Wi-Fi efficiency and dramatically reducing airtime contention between clients.

Features include Orthogonal frequency-division multiple access (OFDMA), multi-user MIMO and cellular optimization. With up to 4 spatial streams (4SS) and 160MHz channel bandwidth (VHT160), the 510 Series provides groundbreaking wireless capabilities for any enterprise.

Read the Multi-User 802.11ax white paper for further information.

Advantages of OFDMA

This capability allows Aruba's APs to handle multiple Wi-Fi 6 capable clients on each channel simultaneously, regardless of device or traffic type. Channel utilization is optimized by handling each transaction via smaller sub-carriers or resource units (RUs), which means that clients are sharing a channel and not competing for airtime and bandwidth.

Multi-user MIMO (MU-MIMO)

The 510 Series APs support downlink MU-MIMO (5GHz radio) to maximize the use of its MIMO radio capabilities by simultaneously exchanging data with multiple single or dual stream client devices.



KEY FEATURES

- Up to 2.69Gbps combined peak data rate
- WPA3 and Enhanced Open security
- Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices
- OFDMA and MU-MIMO for enhanced multi-user efficiency
- IoT-ready Bluetooth 5 and Zigbee support
- Embedded ranging technology for accurate indoor location measurements

WI-FI OPTIMIZATION

Client optimization

Aruba's patented AI-powered ClientMatch technology eliminates sticky client issues by steering a client to the AP where it receives the best radio signal. Client Match steers traffic from the noisy 2.4 GHz band to the preferred 5 GHz or 6 GHz band depending on client capabilities. ClientMatch also dynamically steers traffic to load balance APs to improve the user experience.



Automated Wi-Fi radio frequency management

To optimize the user experience and provide greater stability, Aruba AirMatch allows organization to automate network optimization using machine learning. AirMatch provides dynamic bandwidth adjustments to support changing device density, enhanced roaming using an even distribution of Effective Isotropic Radiated Power (EIRP) to radios, and real-time channel assignments to mitigate co-channel interference.

Application Assurance

With Air Slice, organizations can provide application assurance to their users that goes beyond the traditional capabilities of airtime fairness. After the SLAs are configured, Air Slice monitors network usage, automatically allocates radio resources, and dynamically adjusts radio resources as new users connect. and applications sessions begin or end.

Aruba Advanced Cellular Coexistence (ACC)

This feature uses built-in filtering to automatically minimize the impact of interference from cellular networks, distributed antenna systems (DAS), and commercial small cell or femtocell equipment.

Intelligent Power Monitoring (IPM)

Aruba APs continuously monitor and report hardware energy consumption. They can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.

IOT READY

The 510 Series includes an integrated Bluetooth 5 and 802.15.4 radio (for Zigbee support) to simplify deploying and managing IoT-based location services, asset tracking services, security solutions and IoT sensors. This allows organizations to leverage the 510 Series as an IoT platform, which eliminates the need for an overlay infrastructure and additional IT resources.

Target Wake Time (TWT)

Ideal for IoTs that communicate infrequently, TWT establishes a schedule for when clients need to communicate with an AP. This helps improve client power savings and reduces airtime contention with other clients.

FOUNDATION FOR ACCURATE INDOOR LOCATION

Aruba APs act as a foundation for accurate indoor location so that location-aware services can be deployed at scale. Using embedded GPS receivers, Aruba Wi-Fi 6E APs are able to self-locate and work with Wi-Fi 6 APs to establish reference points that can be used to accurately determine indoor client location.

Because they use universal latitude and longitude coordinates, there is no need for custom map development or to create separate applications for indoor and outdoor environments.

ARUBA SECURE INFR ASTRUCTURE

The Aruba 510 Series includes components of Aruba's Zero Trust and SASE framework to help protect user authentication and wireless traffic. Select capabilities include:

WPA3 and Enhanced Open

Support for stronger encryption and authentication is provided via the latest version of WPA for enterprise protected networks.

Enhanced Open offers seamless new protection for users connecting to open networks where each session is automatically encrypted to protect user passwords and data on guest networks.

WPA2-MPSK

MPSK enables simpler passkey management for WPA2 devices – should the Wi-Fi password on one device or device type change, no additional changes are needed for other devices. Requires ClearPass Policy Manager.

VPN Tunnels

In Remote AP (RAP) and IAP-VPN deployments, the Aruba 510 Series can be used to establish a secure SSL/IPSec VPN tunnel to a Mobility Controller that is acting as a VPN concentrator.

Trusted Platform Module (TPM)

For enhanced device assurance, all Aruba APs have an installed TPM for secure storage of credentials and keys, and boot code.



SIMPLE AND SECURE ACCESS

To simplify policy enforcement, the Aruba 510 Series uses Aruba's policy enforcement firewall (PEF) feature to encapsulate all traffic from the AP to the Mobility Controller (or Gateway) for end-to-end encryption and inspection. Policies are applied based on user role, device type, applications, and location. This reduces the manual configuration of SSIDs, VLANs and ACLs. PEF also serves as the underlying technology for Aruba Dynamic Segmentation.

FLEXIBLE OPERATION AND MANAGEMENT

Our unified APs can operate as standalone access points or with a gateway for greater scalability, security, and manageability. APs can be deployed using zero touch provisioning – without on-site technical expertise – for ease of implementation in branch offices and for remote work.

Aruba APs can be managed using cloud-based or on-premises solutions for any campus, branch, or remote work environment. As the management and orchestration console for Aruba ESP (Edge Services Platform), Aruba Central provides a single pane of glass for overseeing every aspect of wired and wireless LANs, WANs, and VPNs. AI-powered analytics, end-to-end orchestration and automation, and advanced security features are built natively into the solution.

ADDITIONAL WI-FI FEATURES

Each AP also includes the following standards-based technologies:

Transmit beamforming (TxBF)

Increased signal reliability and range

Passpoint Wi-Fi (Release 2) (Hotspot 2.0)

Seamless cellular-to-Wi-Fi carryover for guests

Dynamic Frequency Selection (DFS)

Optimized use of available RF spectrum

Maximum Ratio Combining (MRC)

Improved receiver performance

Cyclic Delay/Shift Diversity (CDD/CSD)

Greater downlink RF performance

Space-Time Block Coding

Increased range and improved reception

Low-Density Parity Check (LDPC)

High-efficiency error correction for increased throughput

SPECIFICATIONS

Hardware variants

- AP-514: External antenna models
- AP-515: Internal antenna models

Wi-Fi radio specifications

- AP type: Indoor, dual radio, 5GHz 802.11ax 4x4 MIMO and 2.4GHz 802.11ax 2x2 MIMO
- 5GHz radio:
 - Four spatial stream Single User (SU) MIMO for up to 4.8Gbps wireless data rate to individual 4SS HE160 802.11ax client devices (max)
 - Two spatial stream Single User (SU) MIMO for up to 1.2Gbps wireless data rate to individual 2SS HE80 802.11ax client devices (typical)
 - Four spatial stream Multi User (MU) MIMO for up to 4.8Gbps wireless data rate to up to four 1SS or two 2SS HE160 802.11ax DL-MU-MIMO capable client devices simultaneously (max)
 - Four spatial stream Multi User (MU) MIMO for up to 2.4Gbps wireless data rate to up to four 1SS or two 2SS HE80 802.11ax DL-MU-MIMO capable client devices simultaneously (typical)
- 2.4GHz radio:
 - Two spatial stream Single User (SU) MIMO for up to 574Mbps wireless data rate to 2SS HE40 802.11ax client devices (max)
 - Two spatial stream Single User (SU) MIMO for up to 287Mbps wireless data rate to 2SS HE20 802.11ax client devices (typical)
- Support for up to 512 associated client devices per radio, and up to 16 BSSIDs per radio
- Supported frequency bands (country-specific restrictions apply):

- 2.400 to 2.4835GHz	ISM
- 5.150 to 5.250GHz	U-NII-1
- 5.250 to 5.350GHz	U-NII-2A
- 5.470 to 5.725GHz	U-NII-2C
- 5.725 to 5.850GHz	U-NII-3/ISM
- 5.850 to 5.895GHz	U-NII-4
- Available channels: Dependent on configured regulatory domain
- Dynamic frequency selection (DFS) optimizes the use of available RF spectrum



- Including Zero-Wait DFS (ZWDFS) to accelerate channel changes
- Supported radio technologies:
 - 802.11b: Direct-sequence spread-spectrum (DSSS)
 - 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)
 - 802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 16 resource units (for an 80MHz channel)
- Supported modulation types:
 - 802.11b: BPSK, QPSK, CCK
 - 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM (proprietary extension)
 - 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (proprietary extension)
 - 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
- 802.11n high-throughput (HT) support: HT20/40
- 802.11ac very high throughput (VHT) support: VHT20/40/80/160
- 802.11ax high efficiency (HE) support: HE20/40/80/160
- Supported data rates (Mbps) :
 - 802.11b: 1, 2, 5.5, 11
 - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
 - 802.11n (2.4GHz): 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)
 - 802.11n (5GHz): 6.5 to 600 (MCS0 to MVC31, HT20 to HT40)
 - 802.11ac: 6.5 to 3,467 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT160)
 - 802.11ax (2.4GHz): 3.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)
 - 802.11ax (5GHz): 3.6 to 4,803 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160)
- 802.11n/ac/ax packet aggregation: A-MPDU, A-MSDU
- Transmit power: Configurable in increments of 0.5 dBm
- Maximum (aggregate, conducted total) transmit power (limited by local regulatory requirements):
 - 2.4 GHz band: +21 dBm (18dBm per chain)
 - 5 GHz band: +24 dBm (18 dBm per chain)
 - Note: conducted transmit power levels exclude antenna gain. For total (EIRP) transmit power, add antenna gain.
- Advanced Cellular Coexistence (ACC) minimizes the impact of interference from cellular networks
- Maximum ratio combining (MRC) for improved receiver performance

- Cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance
- Space-time block coding (STBC) for increased range and improved reception
- Low-density parity check (LDPC) for high-efficiency error correction and increased throughput
- Transmit beam-forming (TxBF) for increased signal reliability and range
- 802.11ax Target Wait Time (TWT) to support low-power client devices

Wi-Fi antennas

- AP-514: Four (female) RP-SMA connectors for external dual band antennas (A0 through A3, corresponding with radio chains 0 through 3). Worst-case internal loss between radio interface and external antenna connectors (due to diplexing circuitry): 1.3dB in 2.4GHz and 1.7dB in 5GHz.
- AP-515: Four integrated dual-band downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 4.2dBi in 2.4GHz and 7.5dBi in 5GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees.
 - Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the effective per-antenna pattern is 3.8dBi in 2.4GHz and 4.6dBi in 5GHz.

Additional interfaces

- E0: HPE SmartRate port (RJ-45, maximum negotiated speed 2.5Gbps)
 - Auto-sensing link speed (100/1000/2500BASE-T) and MDI/MDX
 - 2.5Gbps speed complies with NBase-T and 802.3bz specifications
 - PoE-PD: 48Vdc (nominal) 802.3af/at/bt (class 3 or higher)
 - 802.3az Energy Efficient Ethernet (EEE)
- E1: 10/100/1000BASE-T Ethernet network interface (RJ-45)
 - Auto-sensing link speed and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
- Link aggregation (LACP) support between both network ports for redundancy and increased capacity
- DC power interface: 12Vdc (nominal, +/- 5%), accepts 2.1mm/5.5mm center-positive circular plug with 9.5mm length
- USB 2.0 host interface (Type A connector)
 - Capable of sourcing up to 1A / 5W to an attached device



- Bluetooth 5 and Zigbee (802.15.4) radio (2.4GHz)
 - Bluetooth 5: up to 8dBm transmit power (class 1) and -95dBm receive sensitivity
 - Zigbee: up to 8dBm transmit power and -97dBm receive sensitivity
 - Integrated vertically polarized omnidirectional antenna with roughly 30 degrees downtilt and peak gain of 3.5dBi (AP-515) or 4.9dBi (AP-514)
- Visual indicators (two multi-color LEDs): for System and Radio status
- Reset button: factory reset, LED mode control (normal/off)
- Serial console interface (proprietary, micro-B USB physical jack)
- Kensington security slot

Power sources and power consumption

- The AP supports direct DC power and Power over Ethernet (PoE; on port E0)
- When both power sources are available, DC power takes priority over PoE
- Power sources are sold separately; see the ordering Information section below for details
- When powered by DC or 802.3at (class 4) / 802.3bt (class 5) PoE, the AP will operate without restrictions.
- When powered by 802.3af (class 3) PoE and with the IPM feature enabled, the AP will start up in unrestricted mode, but it may apply restrictions depending on the PoE budget and actual power. What IPM restrictions to apply, and in what order, is programmable.
- Operating the AP with an 802.3af (class 3 or lower) PoE source and IPM disabled is not supported (except for AP staging; no radios will be enabled).
- Maximum (worst-case) power consumption:
 - DC powered: 16.0W
 - PoE powered (802.3af, IPM enabled): 13.5W
 - PoE powered (802.3at/bt): 20.8W
 - All numbers above are without an external USB device connected. When sourcing the full 5W power budget to such a device, the incremental (worst-case) power consumption for the AP is up to 5.7W (PoE powered) or 5.5W (DC powered).
- Maximum (worst-case) power consumption in idle mode: 12.6W (PoE) or 9.7W (DC)
- Maximum (worst-case) power consumption in deep-sleep mode: 5.9W (PoE) or 1.5W (DC)

Mounting details

A mounting bracket has been pre-installed on the back of the AP. This bracket is used to secure the AP to any of the (sold separately) mount kits; see the ordering Information section below for details.

Mechanical specifications

- Dimensions/weight (AP-515; unit, excluding mount bracket):
 - 200mm (W) x 200mm (D) x 46mm (H)/ 7.9" (W) x 7.9" (D) x 1.8" (H)
 - 810g/28.5oz
- Dimensions/weight (AP-515; shipping):
 - 230mm (W) x 220mm (D) x 72mm (H)/ 9.1" (W) x 8.7" (D) x 2.8" (H)
 - 1010g/35.5oz

Environmental specifications

- Operating conditions
 - Temperature: 0C to +50C/+32F to +122F
 - Humidity: 5% to 93% non-condensing
 - AP is plenum rated for use in air-handling spaces
 - ETS 300 019 class 3.2 environments
- Storage and transportation conditions
 - Temperature: -40C to +70C/-40F to +158F
 - Humidity: 5% to 93% non-condensing
 - ETS 300 019 classes 1.2 and 2.3 environments

Reliability

Mean Time Between Failure (MTBF): 560,000hrs (64yrs) at +25C operating temperature.

Regulatory compliance

- FCC/ISED
- CE Marked
- RED Directive 2014/53/EU
- EMC Directive 2014/30/EU
- Low Voltage Directive 2014/35/EU
- UL/IEC/EN 60950
- EN 60601-1-1, EN60601-1-2
- Railway Certs (AP-515 Only):
 - EN 50155:2017 – Railway Applications
 - EN 50121-1:2017 – Railway EMC
 - EN 50121-3-2 – Railway EMC
 - EN 50121-4:2016 – Railway Immunity
 - IEC 61373 ed2:2008 – Railway Shock and Vibration

For more country-specific regulatory information and approvals, please see your Aruba representative.



Regulatory model numbers

- AP-514: APIN0514
- AP-515: APIN0515

Certifications

- UL2043 plenum rating
- Wi-Fi Alliance:
 - Wi-Fi CERTIFIED a, b, g, n, ac, ax
 - WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal(SAE), Enhanced Open (OWE)
 - WMM, WMM-PS, W-Fi Agile Multiband
 - Passpoint (release 2)
 - Wi-Fi Location
- Bluetooth SIG

WARRANTY

Aruba’s hardware limited lifetime warranty.

MINIMUM OPERATING SYSTEM SOFTWARE VERSIONS

ArubaOS and Aruba InstantOS 8.4.0.0 (with some restrictions). For unrestricted operation, use 8.6.0.0 or later.

RF PERFORMANCE TABLE		
Band, rate	Maximum transmit power (dBm) per transmit chain	Receiver sensitivity (dBm) per receive chain
2.4GHz, 802.11b		
1Mbps	18	-96
11Mbps	18	-88
2.4GHz, 802.11g		
6Mbps	18	-93
54Mbps	17	-75
2.4GHz, 802.11n HT20		
MCS0	18	-93
MCS7	16	-75
2.4GHz, 802.11ax HE20		
MCS0	18	-92
MCS11	14	-62
5GHz, 802.11a		
6Mbps	18	-93
54Mbps	17	-75
5GHz, 802.11n HT20		
MCS0	18	-93
MCS7	16	-73
5GHz, 802.11n HT40		
MCS0	18	-90
MCS7	16	-70



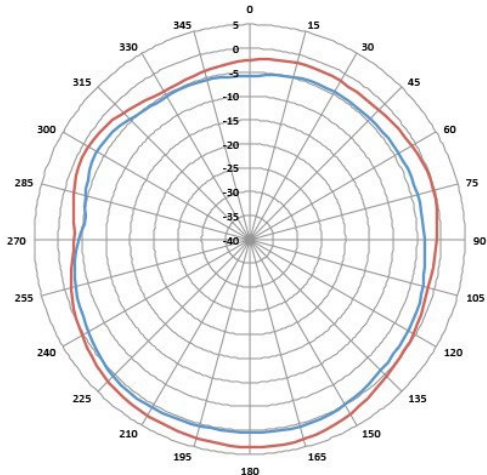
RF PERFORMANCE TABLE		
Band, rate	Maximum transmit power (dBm) per transmit chain	Receiver sensitivity (dBm) per receive chain
5GHz, 802.11ac VHT20		
MCS0	18	-93
MCS9	16	-68
5GHz, 802.11ac VHT40		
MCS0	18	-90
MCS9	16	-65
5GHz, 802.11ac VHT80		
MCS0	18	-87
MCS9	16	-62
5GHz, 802.11ac VHT160		
MCS0	18	-84
MCS9	16	-59
5GHz, 802.11ax HE20		
MCS0	18	-90
MCS11	14	-60
5GHz, 802.11ax HE40		
MCS0	18	-87
MCS11	14	-57
5GHz, 802.11ax HE80		
MCS0	18	-84
MCS11	14	-54
5GHz, 802.11ax HE160		
MCS0	18	-81
MCS11	13	-51



ANTENNA PATTERN PLOTS

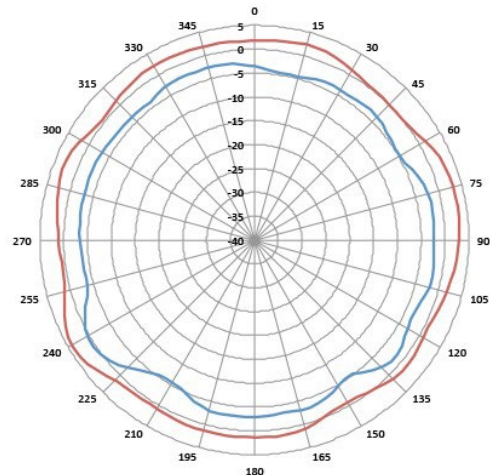
Horizontal planes (top view)

Showing azimuth (0 degrees) and 30 degrees downtilt patterns (averaged patterns for all applicable antennas)



— 2.44GHz WiFi (R1) Average Azimuth — 2.44GHz WiFi (R1) Average Downtilt

2.44GHz Wi-Fi (antennas 1, 2)

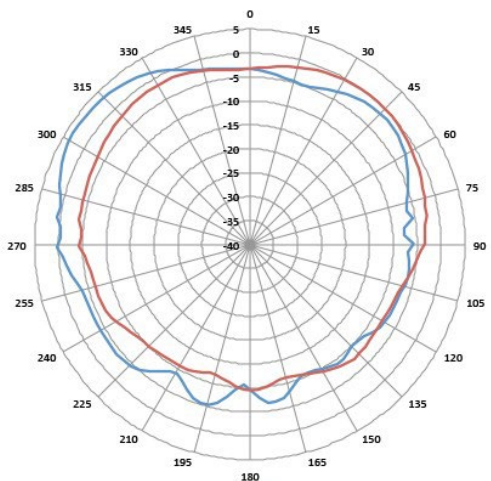


— 5.5GHz WiFi (R0) Average Azimuth — 5.5GHz WiFi (R0) Average Downtilt

5.5GHz Wi-Fi (antennas 1, 2, 3, 4)

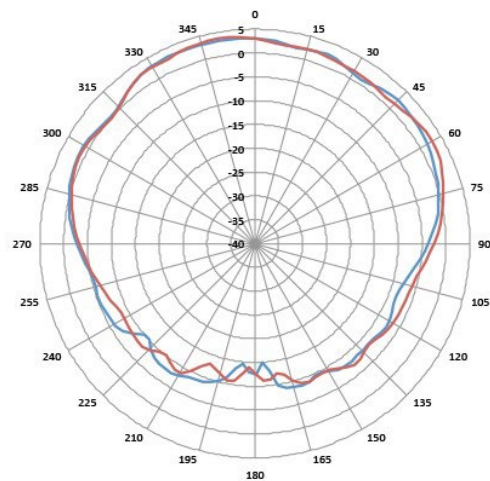
Vertical (elevation) planes (side view, AP facing up)

Showing side view with AP rotated 0 and 90 degrees (averaged patterns for all applicable antennas)



— 2.44GHz WiFi (R1) Average Elevation 0 — 2.44GHz WiFi (R1) Average Elevation 90

2.44GHz Wi-Fi (antennas 1, 2)



— 5.5GHz WiFi (R0) Average Elevation 0 — 5.5GHz WiFi (R0) Average Elevation 90

5.5GHz Wi-Fi (antennas 1, 2, 3, 4)



ORDERING INFORMATION

Part Number	Description
Aruba 510 Series Campus Access Points	
Q9H54A	Aruba AP-514 (EG) Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H55A	Aruba AP-514 (IL) Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H56A	Aruba AP-514 (JP) Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H57A	Aruba AP-514 (RW) Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H58A	Aruba AP-514 (US) Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H59A	Aruba AP-515 (EG) Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H60A	Aruba AP-515 (IL) Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H61A	Aruba AP-515 (JP) Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H62A	Aruba AP-515 (RW) Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H63A	Aruba AP-515 (US) Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H64A	Aruba AP-514 (EG) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H65A	Aruba AP-514 (IL) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H66A	Aruba AP-514 (JP) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H67A	Aruba AP-514 (RW) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H68A	Aruba AP-514 (US) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax External Antennas Unified Campus AP
Q9H69A	Aruba AP-515 (EG) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H70A	Aruba AP-515 (IL) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H71A	Aruba AP-515 (JP) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H72A	Aruba AP-515 (RW) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP
Q9H73A	Aruba AP-515 (US) TAA Dual Radio 4x4:4 + 2x2:2 802.11ax Internal Antennas Unified Campus AP

For more ordering information and compatible accessories, please refer to the [ordering guide](#).

DATA SHEET

ARUBA AIRWAVE

Multivendor, on-premises campus network management

Aruba AirWave is a versatile network management system (NMS) for enterprise campus wired, wireless, and remote connectivity. Supporting a wide range of features such as zero-touch provisioning, enhanced client visibility, traffic analysis, reporting and multivendor integration, AirWave is ideally suited to manage Aruba and third-party network devices.

Deployed as a purpose-built hardware or virtual machine image, each AirWave server supports up to 4,000 network devices (access points, switches, and controllers).

For organizations with the need for more flexible services, higher scale and performance, learn about the next generation management capabilities of Aruba Central, an AI-powered network operations, analytics and security solution that can be deployed in the cloud or on-premises.

STREAMLINED CONFIGURATION AND DEPLOYMENT

AirWave utilizes configuration groups, assigned templates, and step by step workflows to simplify device configuration. Entire config files can be imported, compared, assigned and archived. Modifying and using smaller segments of configuration files across groups of devices is also supported.

These capabilities allow IT to quickly add, modify and deploy devices across distributed locations, while saving time and minimizing mistakes. Aruba's Zero-Touch Provisioning (ZTP) can be used to automatically push configuration files to devices to further simplify the deployment process. Integrated auditing is also provided for security and change management.

CONTACT TRACING AND LOCATION TRACING

Historical Wi-Fi location data from AirWave can be exported, analyzed, and displayed using Aruba Central or a third-party data analysis tool. This includes simple search queries can be run on a per-client basis to identify nearby clients and contact duration. This is intended to expediently provide data for appropriate enterprise and public health entities to manage and counteract potential COVID-19 outbreaks.

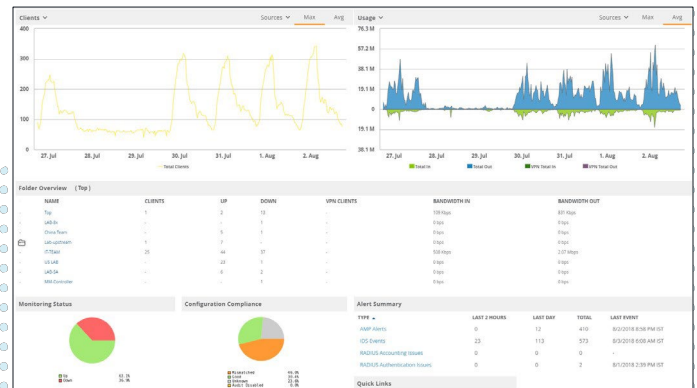


Figure 1: Aruba AirWave Dashboard

KEY FEATURES

- WLAN, wired LAN, and VPN management
- Zero touch provisioning
- Contact tracing and location tracing
- User and application visibility and control
- Wi-Fi connectivity health analytics
- Physical and virtual appliance options
- Multivendor and 3rd party integration

To expand location accuracy, the Bluetooth radio within Aruba APs can be used as Bluetooth tags or as Bluetooth hubs when deployed as part of Aruba Meridian. For more details, please learn about Hybrid Workplace solutions.

This feature is available as an extension through Aruba Central, and is included as part of Aruba's business continuity and recovery special program offers. Please contact your Aruba sales representative for consultation and support.

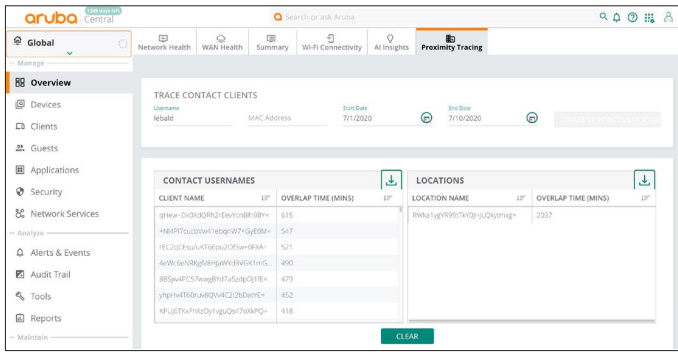


Figure 2: Proximity Tracing

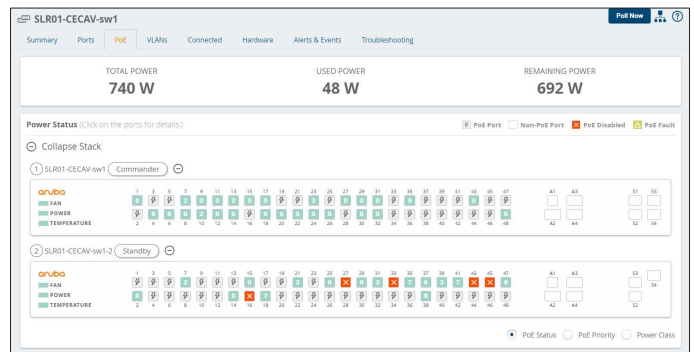


Figure 3: Aruba AirWave Switch Faceplate View

REAL-TIME VISIBILITY AND CONTROL

AirWave provides detailed health and analytics dashboards to monitor critical applications and services, including:

- **Network Health** – used to view client usage, monitoring and configuration compliance, alert summaries and other selected statistics.
- **Traffic Analysis** – helps to monitor application usage and policy enforcement across the entire network. Tracks web categories, client destinations and relative trust levels. Details are displayed by network, roles, device type and users.
- **UCC Analytics** – a consolidated view of how VoIP applications are performing displays MOS scores, and potential RF performance and capacity issues.

For detailed device visibility, simply click a chart or graph to drill-down from any network level view, or locate and select a device for a configuration summary and details on connected clients, neighbors, alerts and related events.

When looking at switch information, additional visibility into key values of individual and stacked switches is provided. This includes port status, PoE consumption, VLAN assignment, device and neighbor connections, power status and trends, alerts and events and which troubleshooting actions can be performed.

COMPREHENSIVE MANAGEMENT AND TROUBLESHOOTING

Role-Based Access, Discovery and Topology

AirWave utilizes a role-based model for administrative access.

Multiple combinations of access and management rights can be assigned as needed. AirWave allows IT to protect the environment and provides the ability to tailor administrative access based on assigned scope and responsibilities.

AirWave also discovers and maps devices across the entire environment, including those with distributed locations. The resulting topology map shows upstream relationships between APs, controllers and switches in order to assess the impact on related devices and clients, and to isolate root cause of issues.

Stage-based Connectivity Health

A reliable connection is the foundation of a successful user experience. AirWave monitors the connectivity of clients, to proactively help identify and resolve issues. Data points

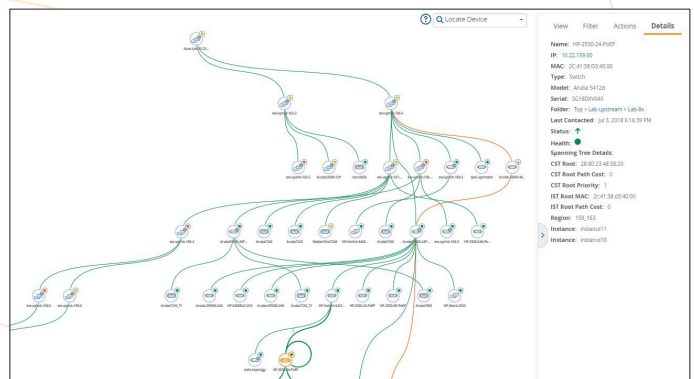


Figure 4: Aruba AirWave Topology View

include client association, as well as network authentication and DHCP metrics.

VisualRF for Wi-Fi Visibility & Management

Real-time views of actual floorplan maps make it easy to see RF coverage issues, location of all access points, and possible

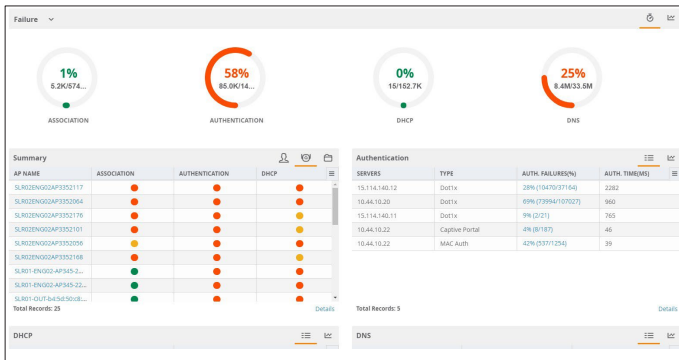


Figure 5: Aruba AirWave Connectivity Health

split download images, and schedule updates during off hours to minimize the impact during peak operations.

The AirWave Central Ready appliance is designed for investment protection. Providing the enhanced performance, storage, and interface requirements to support either AirWave or the planned Aruba Central on-premises deployment option.

AirWave virtual deployments are supported on VMware and Microsoft Hyper-V host hyper visors.

GOVERNMENT-GRADE CERTIFICATIONS

AirWave is highly secure, and has achieved the Federal Information Processing Standard (FIPS) Publication 140-2 validation, a government level computer security standard for cryptographic modules (Certificate #2577). See [detailed security documentation](#) for more information.

interference points. The result is a comprehensive view of how the network is performing, and potential trouble spots.

Selectable overlays show client health, traffic thresholds, UCC performance and channel utilization to quickly diagnose client, building, floor or location specific issues.

VisualRF also provides the ability to capture and playback physical movement of devices and clients within locations to isolate and troubleshoot those challenging intermittent mobility issues.

RAPIDS for Intrusion Detection

AirWave utilizes Aruba's Rogue AP Intrusion Detection Service (RAPIDS), to identify and resolve issues caused by rogue access points, and clients.

Wired and wireless data is correlated to identify relevant threats, while reducing false positives to strengthen network security. RAPIDS includes:

- Summary Data – percentage of device classification and acknowledgments, and device counts by type.
- Lists & Events – concise summaries of devices by type and events by severity, category and scope.
- Rules Engine - easily define and edit wireless, wired, and controller properties to detect rogues, classifications and threat levels.

Firmware Upgrade & Compliance

An advanced image upgrade and compliance module, makes it easy to update firmware by device type or version group,



Category	Pro Appliance	Pro Appliance (Gen10)	Central Ready Appliance
Appliance Specifications			
CPU	8-core 2.6 Ghz HPE DL360 Gen9 E5-2640v3	8 Core Intel Xeon-S 4110 @ 2.10 Ghz - HPE DL360 Gen10	2 20-core Intel Xeon-G 6138 @ 2.0 GHz - HPE DL360 Gen10
Memory	48GB	48GB	512GB
Storage	6 300GB 12G SAS 15K 2.5in SC ENT HDD	6 300GB SAS 15K SFF SC DS HDD	4 1TB SSD HDD (2 TB in RAID 10)
Appliance Scalability			
Maximum Managed Devices	1,500	1,500	4,000
Power			
Power	500W FS Plat Hot Plug Power Supply	500W FS Plat Hot Plug Power Supply	500W FS Plat Hot Plug Power Supply
Power Supply	Optional redundant power supply	Optional redundant power supply	Optional redundant power supply
AC Input Voltage	110/220 VAC Auto-Selecting	110/220 VAC Auto-Selecting	110/220 VAC Auto-Selecting
AC Input Frequency	50/60 Hz Auto-Selecting	50/60 Hz Auto-Selecting	50/60 Hz Auto-Selecting
Physical			
Rackmount	1U SFF Easy Install Rail 1U Cable Management Arm	1U SFF Easy Install Rail 1U Cable Management Arm	1U SFF Easy Install Rail 1U Cable Management Arm
Dimensions (H x W x D)	1.7 x 17.1 x 27.5 inches (4.32 x 43.47 x 69.85 cm)	1.7 x 17.1 x 27.5 inches (4.32 x 43.47 x 69.85 cm)	1.7 x 17.1 x 27.8 inches (4.29 x 43.46 x 70.7 cm)
Weight	33.3 lb. (15.31 kg) max	33.3 lb. (15.31 kg) max	35.9 lb. (16.27 kg) max
HP SmartDrives	8 + 2 SFF/4 LFF max, HDD/SSD	8 + 2 SFF/4 LFF max, HDD/SSD	4 LFF SAS/SATA/SSD 8 or 10 SFF SAS/SATA/SSD
Networking	4 x 1GbE embedded + FlexibleLOM slot	4 x 1GbE embedded + Flexible LOM slot or HPE FlexFabric 10Gb 4-Port 536FLR-T Adapter	2 x 10GbE and 4 x 1GbE embedded + Flexible-LOM slot
VGA/serial/USB ports	Front VGA opt, rear VGA standard, and serial opt., 5 USB 3.0	Front VGA opt, rear VGA standard, and serial opt., 5 USB 3.0	Front VGA opt, rear VGA standard, and serial opt., 5 USB 3.0, iLO Remote Mgmt, MicroSD Slot
Industry compliance	ASHRAE A3 and A4, lower idle power	ASHRAE A3 and A4, lower idle power	ASHRAE A3 and A4, lower idle power
Warranty			
Hardware	1 year parts	1 year parts	1 year parts
Software	90 days	90 days	90 days

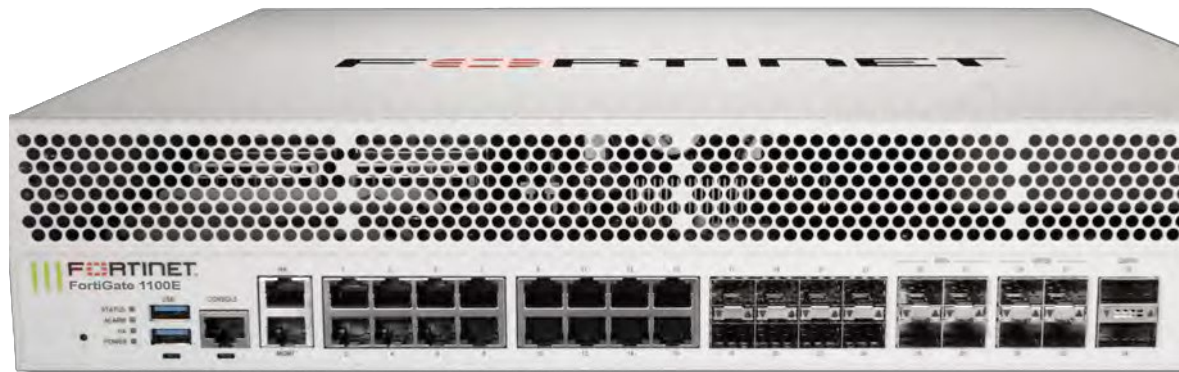


ORDERING INFORMATION

Part Number	Description
JW546AAE	Aruba LIC-AW Aruba AirWave with RAPIDS and VisualRF 1 Device License E-LTU
JW558AAE	Aruba AW-25-FR AirWave 25 Device Failover License E-LTU
JW559AAE	Aruba AW-50-FR AirWave 50 Device Failover License E-LTU
JW560AAE	Aruba AW-100-FR AirWave 100 Device Failover License E-LTU
JW561AAE	Aruba AW-200-FR AirWave 200 Device Failover License E-LTU
JW562AAE	Aruba AW-500-FR AirWave 500 Device Failover License E-LTU
JW563AAE	Aruba AW-1000-FR 1000 AirWave Device Failover License E-LTU
JW564AAE	Aruba AW-2500-FR 2500 AirWave Device Failover License E-LTU
JW565AAE	Aruba AW-EXF1-50 AirWave 50 Device Failover Expansion License E-LTU
JW566AAE	Aruba AW-EXF1-2500 AirWave 2500 Volume Failover Expansion License E-LTU
JW567AAE	Aruba AW-CONDUCTOR AirWave Conductor Console License E-LTU
JX918A	Aruba AirWave DL360 Professional Edition Hardware Appliance
R3W19A	Aruba AirWave Pro Gen 10 Hardware Appliance
R1Q04B	Aruba Central Ready AirWave 8 Appliance
JZ075A	Aruba AW-HW-GLASS AirWave Hardware Appliance for Centralized Monitoring
R1T38A	Aruba DL360 Gen10 500W Spare PSU
JZ076AAE	Aruba AW-VA-GLASS AirWave Virtual Appliance for Centralized Monitoring E-LTU

FortiGate 1100E Series

FG-1100E/-DC and FG-1101E



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Hyperscale Security to secure any edge at any scale.

High performance with flexibility

The FortiGate 1100E Series enables organizations to build security-driven networks that can weave security deep into their datacenter and across their hybrid IT architecture to protect any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 1100E Series delivers coordinated, automated, end-to-end threat protection across all use cases.

The industry's first integrated Zero Trust Network Access (ZTNA) enforcement within an NGFW solution, FortiGate 1100E automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
12.5 Gbps	9.8 Gbps	7.1 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP, and 40 GE QSFP+ slots



Available in



Appliance



Virtual



Hosted



Cloud



Container

FortiOS Everywhere

FortiOS, Fortinet's advanced operating system

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations



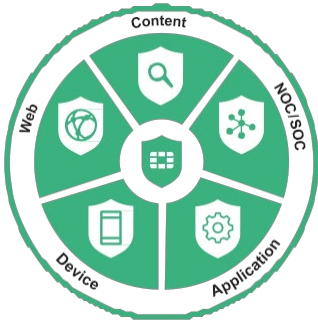
Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.



FortiGuard Services

FortiGuard AI-Powered Security

FortiGuard's rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance.

Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC

Advanced NAC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service

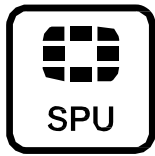
Includes tier-one hunting and automation, log location, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices

Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.



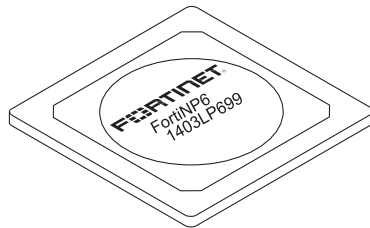
Secure Any Edge at Any Scale



Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



Network Processor 6 NP6

Fortinet's new breakthrough SPU NP6 network processor works in line with FortiOS functions delivering:

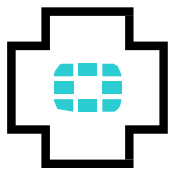
- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing



Content Processor 9 CP9

Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing



FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.



Use Cases



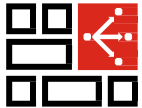
Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
 - Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
 - Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection
-



Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
 - Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
 - Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks
-



Secure SD-WAN

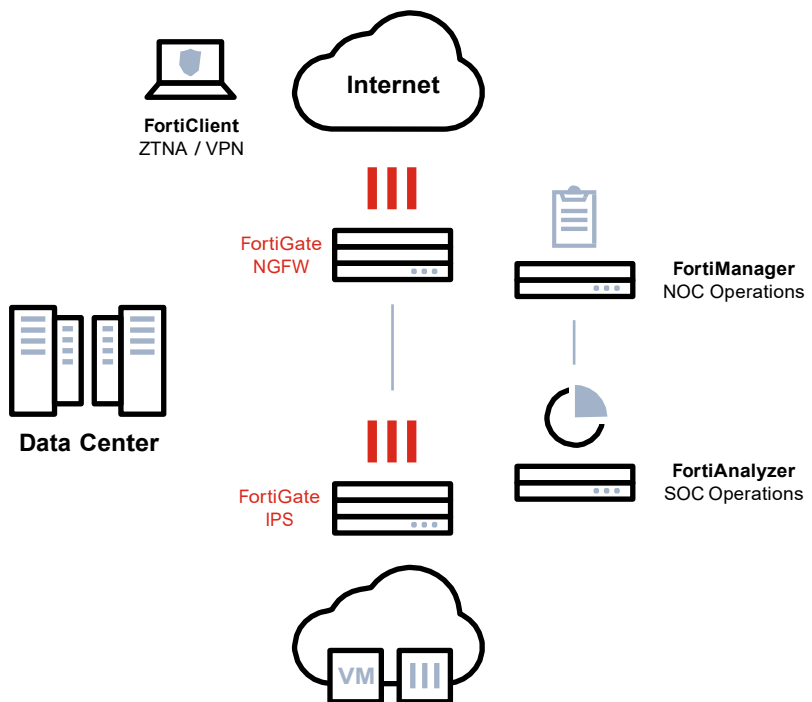
- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
 - Delivers superior quality of experience and effective security posture for work-from-anywhere models, SD-Branch, and cloud-first WAN use cases
 - Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing
-



Mobile Security for 4G, 5G, and IoT

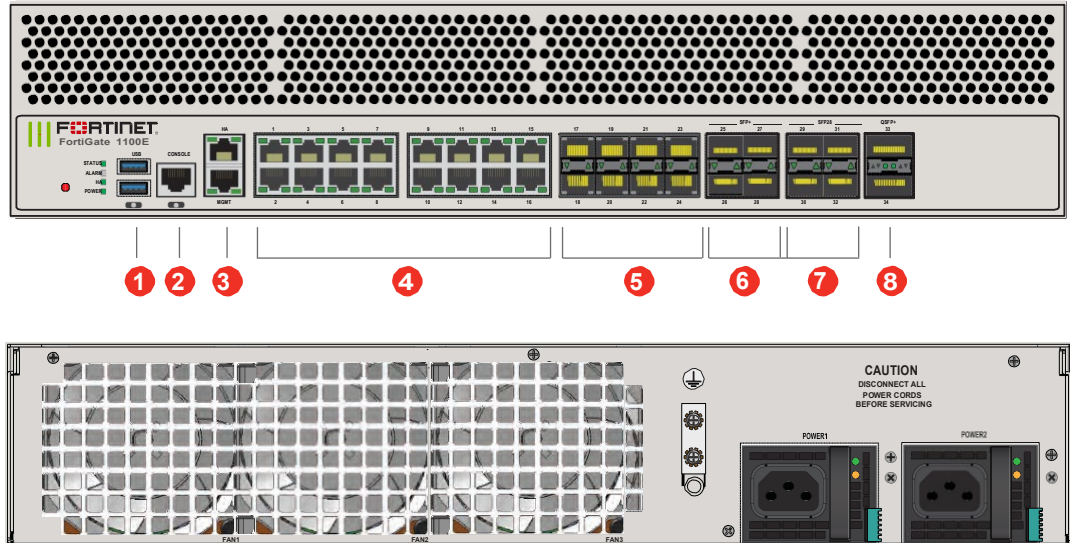
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane security enabled by full threat protection and visibility into GTP-U inspection

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

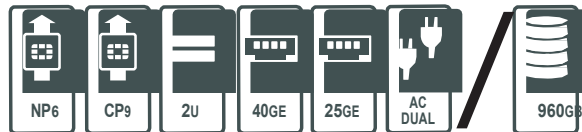
FortiGate 1100E Series



Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Ports
5. 8 x GE SFP Slots
6. 4 x 10 GE SFP+ Slots / GE SFP Slots
7. 4 x 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots
8. 2 x 40 GE QSFP+ Slots

Hardware Features



Specifications

	FG-1100E/-DC	FG-1101E
Interfaces and Modules		
Hardware Accelerated 40 GE QSFP+ Slots		2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots		4
Hardware Accelerated 10 GE SFP+ Slots / GE SFP Slots		4
Hardware Accelerated GE SFP Slots		8
Hardware Accelerated GE RJ45 Ports		16
GE RJ45 Management/ HA Ports		2
USB Ports (Client / Server)		1 / 2
Console Port		1
Onboard Storage	0	2x 480 GB SSD
Included Transceivers		2x SFP (SX 1 GE)
System Performance — Enterprise Traffic Mix		
IPS Throughput ²		12.5 Gbps
NGFW Throughput ^{2,4}		9.8 Gbps
Threat Protection Throughput ^{2,5}		7.11 Gbps
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		80 / 80 / 45 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)		80 / 80 / 45 Gbps
Firewall Latency (64 byte, UDP)		2.76 µs
Firewall Throughput (Packet per Second)		67.5 Mpps
Concurrent Sessions (TCP)		8 Million
New Sessions/Second (TCP)		500 000
Firewall Policies		100 000
IPsec VPN Throughput (512 byte) ¹		48 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		20 000
Client-to-Gateway IPsec VPN Tunnels		100 000
SSL-VPN Throughput		8.4 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		10 000
SSL Inspection Throughput (IPS, avg. HTTPS) ³		10 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³		6500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³		780 000
Application Control Throughput (HTTP 64K) ²		26 Gbps
CAPWAP Throughput (HTTP 64K)		43 Gbps
Virtual Domains (Default / Maximum)		10 / 250
Maximum Number of FortiSwitches Supported		196
Maximum Number of FortiAPs (Total / Tunnel)		4096 / 2048
Maximum Number of FortiTokens		20 000
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-1100E/-DC	FG-1101E
Dimensions and Power		
Height x Width x Length (inches)	3.5 x 17.44 x 17.62	
Height x Width x Length (mm)	88.9 x 443 x 447.4	
Weight	24.9 lbs (11.3kg)	25.4 lbs (11.55 kg)
Form Factor (supports EIA/ non-EIA standards)	Rack Mount, 2 RU	
AC Power Input	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	217 W / 336 W	222 W / 346 W
AC Current (Maximum)	6A@120V, 3A@240V	
Heat Dissipation	1147 BTU/h	1181 BTU/h
DC Power Input (FG-1100E-DC)	-48V DC	-- DC
Current (Maximum)	11.5A	--
Redundant Power Supplies (Hot Swappable)	Yes (Default dual AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	
Storage Temperature	-31°–158°F (-35°–70°C)	
Humidity	10%–90% non-condensing	
Noise Level	66.7 dBA Forced	
Airflow	Front to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6	

Note: All performance values are "up to" and vary depending on system configuration.

¹ IPsec VPN performance test uses AES256-SHA256.

² IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

³ SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

⁴ NGFW performance is measured with Firewall, IPS and Application Control enabled.

⁵ Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



Ordering Information

Product	SKU	Description
FortiGate 1100E	FG-1100E	2x 40 GE QSFP+ slots, 4x 25 GE SFP28 slots, 4x 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, and 2 AC power supplies.
FortiGate 1101E	FG-1101E	2x 40 GE QSFP+ slots, 4x 25 GE SFP28 slots, 4x 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, 960 GB SSD onboard storage, and 2 AC power supplies.
FortiGate 1100E-DC	FG-1100E-DC	2x 40 GE QSFP+ slots, 4x 25 GE SFP28 slots, 4x 10 GE SFP+ slots, 8x GE SFP slots, 18x GE RJ45 ports (including 16x ports, 2x management/HA ports) SPU NP6 and CP9 hardware accelerated, and 2 DC power supplies.
Optional Accessories	SKU	Description
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Active Direct Attach Cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE SFP28 transceiver module, short range for all systems with SFP28 slots.
25 GE SFP28 Transceiver Module, Long Range	FG-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
40 GE QSFP+ Transceiver Module, Short Range	FN-TRAN-QSFP+SR	40 GE QSFP+ transceiver module, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Short Range, BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceivers, short range BiDi for systems with QSFP+ slots.
40 GE QSFP+ Transceiver Module, Long Range	FN-TRAN-QSFP+LR	40 GE QSFP+ transceiver module, long range for all systems with QSFP+ slots.
40 GE QSFP+ to 4x 10 GE SFP+ Optical Breakout	FG-TRAN-QSFP+4XSFP	40 GE QSFP+ Parallel Breakout Active Optical Cable with 1m length for all systems with QSFP+ slots.
QSFP+ to 4xSFP+ Optical breakout 5m	FG-TRAN-QSFP+4SFP-5	40 GE QSFP+ Parallel Breakout MPO to 4xLC connectors, 5m reach, transceivers not included.
Rack Mount Sliding Rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-2000E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC Power Supply	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FG-1100/1101E, FAZ-200F/FAZ-300F/FMG-200F and FAZ-800F/FMG-300F.
DC Power Supply	SP-FG300E-DC-PS	DC power supply for FG-1100E-DC



Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
Security Services	FortiGuard IPS Service	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering	•	•	•	
	FortiGuard Anti-Spam		•	•	
	FortiGuard IoT Detection Service	•	•		
	FortiGuard Industrial Security Service	•	•		
	FortiCloud AI-based Inline Sandbox Service ¹	•			
NOC Services	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiGuard Security Fabric Rating & Compliance Monitoring Service	•	•		
	FortiConverter Service	•	•		
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
SOC Services	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	FortiGuard Application Control				
	FortiCloud ZTNA Inline CASB Service ¹				
	Internet Service (SaaS) DB Updates				included with FortiCare Subscription
	GeoIP DB Updates				included with FortiCare Subscription
	Device/OS Detection Signatures				included with FortiCare Subscription
	Trusted Certificate DB Updates				included with FortiCare Subscription
	DDNS (v4/v6) Service				included with FortiCare Subscription

¹. Available when running FortiOS 7.2



FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

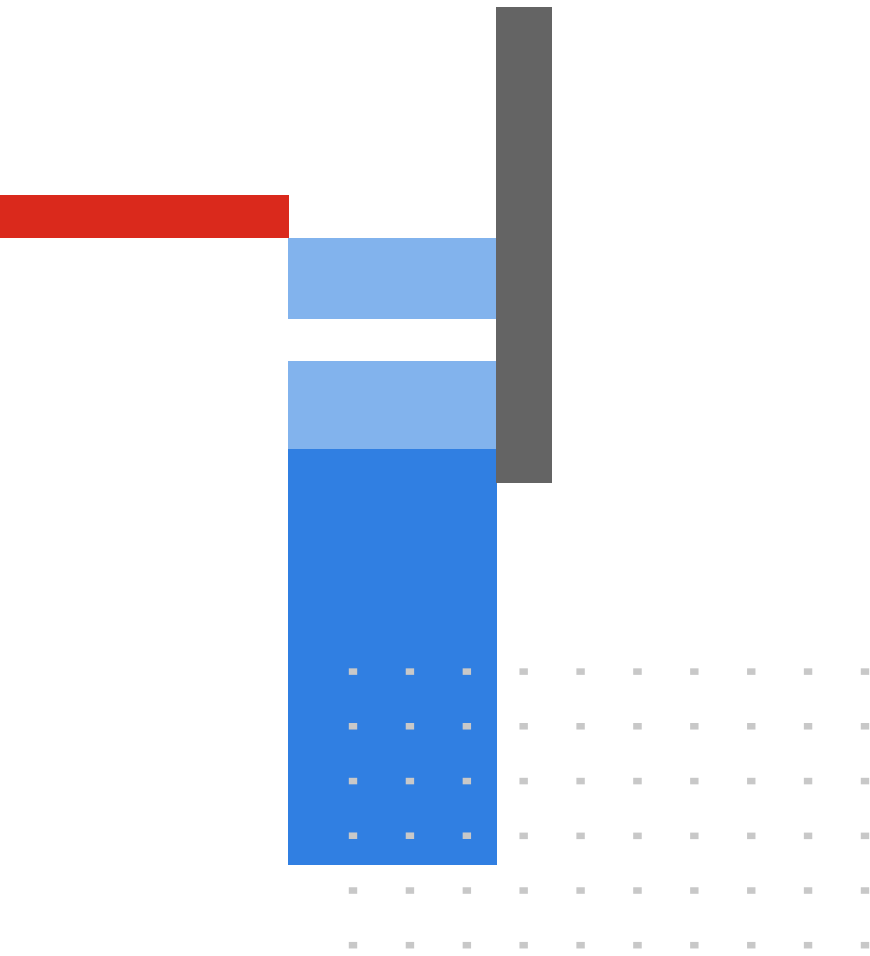
FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).





FORTINET

www.fortinet.com

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

November 15, 2022

FG-1100E-DAT-R22-20221115



**Hewlett Packard
Enterprise**

HPE IMC STANDARD SOFTWARE PLATFORM WITH 50-NODE E-LTU (JG747AAE)

Intelligent Management Software



WHAT'S NEW

- Integration with Aruba AirWave, ClearPass and HPE OneView.
- Cisco Nexus support.
- VXLAN support.
- API enhancements.

OVERVIEW

The HPE Intelligent Management Center Standard Software Platform is a comprehensive wired and wireless network management tool supporting the FCAPS model, providing for end-to-end business management of IT, scalability of system architecture, and accommodation of new technology and infrastructure.

Intelligent Management Center Standard Software Platform supports the management of Hewlett Packard Enterprise and

third-party devices and comes with a base license for 50 managed devices with available additional node licenses. Includes the eAPI library enabling programmatic extensions.

FEATURES

Comprehensive Network Management for Medium-Sized Networks

The HPE Intelligent Management Center Standard Software Platform is aimed at enterprises and business with branches, and integrates fault management, element configuration, and network monitoring from a central vantage point with third-party device support.

Contains license support for 50 managed devices with available additional licenses for purchase.

Delivers an extensive RESTful eAPI library that can be integrated with third-party software for additional functionality.

Collect data on archived information about the network, device, or Intelligent Management Center (IMC) optional software to appropriate Hewlett Packard Enterprise support organizations in a single step.

Gather data about network, resource, and administrator performance with a flexible, centralized reporting deliverable on a singular or periodic basis.

Resource Management for Easy Device Management

The HPE Intelligent Management Center Standard Software Platform offers management capabilities for a wide range of devices from routers and switches to desktops and servers.

View and monitor devices in a variety of visual methodologies, by device, IP, network topology, or through a custom view. Use the Security Control Center to enforce device settings consistently and sound alarms when they become non-compliant.

Ascertain the health of a particular device through the device details page containing the summary, connectivity testing, real-time data, and the option to Telnet/SSH into the device to fix any issues.

The Configuration Center can be used to track device changes.

Detailed Performance Monitoring with Real-time Notifications

The HPE Intelligent Management Center Standard Software Platform provides the ability to monitor device performance for report generation, performance information, and alarm notification.

Individually or collectively monitor devices for threshold settings, which when exceeded, sound an alarm.

Be alerted with integrated alarm notifications and easily fix issues from the console or by utilizing the Telnet/SSH proxy.

Virtualization Management for VLANs, Virtual and Physical Networks

The HPE Intelligent Management Center Enterprise Software Platform is one of the first management tools to integrate and monitor both virtual and physical networks.



Supports a variety of hypervisors including VMware vSphere, Microsoft Hyper-V, Citrix Xen and KVM.

Manages VLANs on a global or on a per device basis and create standardized VLANs one-by-one or in a batch operation.

You can view the status of all the VLANs through a network topology view, with the ability to monitor and manage devices from the same view.

Technical specifications

HPE IMC Standard Software Platform with 50-node E-LTU

Product Number	JG747AAE
Differentiator	Electronic delivery of license for HPE IMC Standard Edition Software Platform with 50-node E-LTU
Browser supported	IE 10 or 11 Firefox 30 or later Chrome 35 or later.
Software (required)	Database: Microsoft SQL Server 2008 Service Pack 3 (Windows only) Microsoft SQL Server 2008 R2 Service Pack 2 (Windows only) Microsoft SQL Server 2012 Service Pack 2 (Windows only) Microsoft SQL Server 2014 (Windows only) Oracle 11g Release 1 (Linux only) Oracle 11g Release 2 (Linux only) MySQL Enterprise Server 5.5 (Linux and Windows) (Up to 1000 devices are supported) MySQL Enterprise Server 5.6 (Linux and Windows) (Up to 1000 devices are supported).
Software (recommended)	Client: Windows XP SP3 or later.
Minimum system requirements	Server: Intel® Pentium® 4 3.0 GHz, 4 GB RAM memory, 50 GB storage, 10/100 Mbps NIC Client: Intel® Pentium® 4 2.0 GHz, 2 GB RAM memory, 50 GB storage, 10/100 Mbps NIC.
System requirements, recommended	Server: 3.0 GHz Intel® Xeon® or Intel® Core™ 2 Duo processor or equivalent 4 GB RAM 100 GB 10/100 Mbps.
Technical notes	Operating systems marked X64 are recommended. Client: JRE 1.6.0_update 27 or later is recommended. For fewer than 500 nodes, 1 CPU is sufficient From 500 to 2,000 nodes, there should be 2 CPUs or 1 dual-core CPU For more than 2,000 nodes, there should be 4 CPUs or 2 dual-core CPUs.



[For additional technical information, available models and options, please reference the QuickSpecs](#)

HPE POINTNEXT SERVICES

HPE Pointnext Services brings together technology and expertise to help you drive your business forward and prepare for whatever is next.

Operational Services from HPE Pointnext Services

HPE Pointnext Tech Care provides fast access to product-specific experts, an AI-driven digital experience, and general technical guidance to help enable constant innovation. We have reimagined IT support from the ground up to deliver faster answers and greater value. By continuously searching for better ways to do things—as opposed to just fixing things that break—HPE Pointnext Tech Care helps you focus on achieving your business goals.

HPE Pointnext Complete Care is a modular, edge-to-cloud IT environment service that provides a holistic approach to optimizing your entire IT environment, and achieving agreed upon IT outcomes and business goals through a personalized and customer-centric experience. All delivered by an assigned team of HPE Pointnext Services experts.

HPE Integration and Performance Services help you customize your experience at any stage of your product lifecycle with a menu of services based on individual needs, workloads, and technologies.

- Advise, design, and transform
- Deploy
- Integrate and migrate
- Operate and improve
- Financial Services
- GreenLake Management Services
- Retire and sanitize
- IT Training and personal development

Other related services

HPE Education Services delivers a comprehensive range of services to support your people as they expand their skills required for a digital transformation. Consult your HPE Sales Representative or Authorized Channel Partner of choice for any additional questions and support options.

Defective Media Retention is optional and allows you to retain Disk or eligible SSD/Flash Drives replaced by HPE due to malfunction.

HPE GREENLAKE

HPE GreenLake is HPE's market-leading IT as-a-Service offering that brings the cloud experience to apps and data everywhere – data centers, multi-clouds, and edges – with one unified operating model. HPE GreenLake delivers public cloud services and infrastructure for workloads on premises, fully managed in a pay per use model.

If you are looking for more services, like **IT financing solutions**, please [explore them here](#).

Make the right purchase decision.
Contact our presales specialists.



© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Parts and Materials: HPE will provide HPE-supported replacement parts and materials required to maintain the covered hardware.

Parts and components that have reached their maximum supported lifetime and/or the maximum usage limitations as set forth in the manufacturer's operating manual, product quick-specs, or the technical product data sheet will not be provided, repaired, or replaced as part of these services.

Image may differ from the actual product
[PSN5443908CZEN](#), January, 2023.

Overview

HPE Intelligent Management Center Standard Software Platform

Models

HPE IMC Standard Software Platform with 50-node E-LTU

JG747AAE

Aruba IMC Standard Software Platform with 50-node E-LTU

JH704AAE

Key features

- Highly flexible and scalable deployment options
 - Powerful administration control
 - Rich resource management
 - Detailed performance monitoring and management, flexible centralized reporting
 - Fault, Configuration, Accounting, Performance and Security (FCAPS) capabilities
 - Integration with Aruba AirWave, ClearPass and HPE OneView
 - Cisco Nexus support
 - VxLAN support and API Enhancements
-

Product overview

The HPE Intelligent Management Center (IMC) Standard Software Platform is a comprehensive management platform that was built from the ground up to support the Fault, Configuration, Accounting, Performance, Security (FCAPS) model. It provides features and functions that are designed for comprehensive management of the network infrastructure. IMC was designed to provide the following functions:

- Supports the ITIL operational center of excellence IT practices model
- Uses a single-pane management paradigm to enable end-to-end business management of IT services
- Provides scalability by supporting distributed and hierarchical system architectures, through additional operating system and database support.
- Uses an SOA model to provide full resource, service, and user management.
- Enables the integration of traditionally separate management tools using a modular design.
- Enables enterprises to expand their infrastructure management in scale and to seamlessly accommodate new technologies at the same time.

IMC software supports the management of Hewlett Packard Enterprise and third-party devices, and is compatible with Microsoft® Windows® and Linux operating systems. IMC Standard software comes with an initial license for 50 managed devices. Additional node licenses are available to extend the node limit.

Features and Benefits

Management

- Integration with Aruba AirWave, ClearPass, and HPE OneView allows administrators from IMC to use AirWave for "user centric" wired management and wireless management while IMC provides edge to core infrastructure management, monitoring, and troubleshooting. Integration with ClearPass ensures IMC has the user context, allowing the administrator to easily associate an IP address to the logged on user. OneView integration automates the provisioning of ToR switches when VLANs are added.
- Role-based administrative controls provides administrators with both the tools and the ability to grant access to only those features and resources operators need. IMC also provides controls and audit trails to support IT management best practices. IN IMC, management rights

Overview

and access to all resources are granted through operator and device groups or custom views of the devices. Operator groups grant and restrict access to specific parts of IMC.

- **Resource management**
provides comprehensive element management for multi-vendor devices via single Web portal. Administrators can access resources for managing and monitoring a device, add devices to the network, and view devices in a network topology, IP, or custom view. Administrators can see device health through the device details page, revealing real-time data, summary information, connectivity testing, and more; supports End-of-Life Notifications available as well
- **Virtualization management**
 - HPE IMC Software integrates management and the capability to integrate, discover, map, manage and monitor virtualized environments, helping to identify VM sprawl.
 - Provides insight and management of virtual networks, and reduces migration complexity by aligning as well as automating network policies with virtual images.
 - Supports VMware®, Hyper-V, and KVM; IMC Virtual Network Management Software; and automatic tracking of the network access port of virtual machines
- **Flexible, centralized reporting**
offers administrator performance, operator performance, and resource reporting options for network assets, configuration and configuration changes, network device and link status, alarms, and network device health. Report types offered are in real-time and quick-custom. Device data is offered for status, label, IP address, MAC address, device type, model, vendor, location, and many more.
- **Global ACL management**
provides operators with a comprehensive feature set for managing ACLs including viewing and configuring ACLs on devices managed by IMC, and importing ACLs. The ACL Manager supports basic, advanced, link, and user-defined ACLs. The ACL Assistant facilitates ACL template rule creation and easier management. The ACL Resource List provides a portal for viewing and managing ACLs with a Rule Set List. The ACL Deployment Wizard assists in the deployment of ACLs.
- **Configuration and change management**
combines the tasks of network device change and configuration management to effectively manage devices and audit changes. Like the IMC Resource Management feature, the Configuration Center has a portal for accessing most of IMC change and configuration management features. Operators can view and deploy software to devices, access configuration templates, utilize a system software library, clean the device for new deployments, and back the system up.
- **Compliance center**
supports organization adherence to compliance policies and standards. This feature enables operators to create compliance policies and rules that check the configuration of devices.
- **Network asset management**
tracks assets as well as changes to assets. This feature provides operators with a list of asset and drilldown capabilities into individual device details or device audit details. Operators can also query IMC for specific audit records and manage the device auditing process.
- **Real time fault management**
integrates network management system of fault, performance, auditing, security, and configuration reduces the effort required to manage complex network infrastructures, allowing network managers to have one database of network devices in IMC that drives various tasks of network management. The database integrates with all IMC functions. The alarm or event management system in IMC uses the existing device database and generates alarms in events of interest.
- **Global VLAN management**
gives administrators the ability to create standardized VLANs across all devices in the infrastructure that support VLANs. They can create VLANs, then add, configure, or remove them from all devices that support this feature. VLANs can be deployed in batch or individually for devices configuring VLANs. Administrators can also see VLANs on a topology view.
- **Customized functions and third-party device support**
extends device management and configuration functions; users can either extend an existing function to support third-party devices by compiling interactive scripts and XML files, or customize a function by compiling interactive scripts, XML files, and UI configuration files.
- **Performance monitoring and management**
provides the ability to monitor the performance of devices managed by IMC. The Performance Management features provide the ability to customize the collection, alarming, and presentation of performance data. IMC enables real-time and historical performance management for managed devices like routers and switches on data like IPSec VPNs, WSM, and QoS. Also customizable are threshold settings, performance views and data, and global monitors; real-time viewing.

Overview

- **Security Control Center**
defines policies and enforces device settings consistently on selected devices; you can also use policies to manage VLANs and VLAN port settings or automatically apply a configuration template on newly discovered devices. Configure policies to send alarms when device configurations become noncompliant.
- **Network data collection**
generates, packages, and sends archived information about your network, device, or IMC Software to the appropriate Hewlett Packard Enterprise support or sales organizations in one simple step; this feature gathers the data you selected and generates reports and data files containing the relevant information; it delivers the reports to your selected destination by email, FTP, SFTP, or to a file location.
- **Intuitive user interface**
desktop UI provides up to eight customizable icon-based screen interfaces that can be organized along specific tasks. Includes many features enabling administrators and operators to manage the network infrastructure. IMC also provides operators with many paths to the same destination. Operators are provided with quick start guides. With the My Favorites feature, operators can create links to the IMC features they use most often.
- **eAPI library and third-party applications**
the IMC eAPI library utilizes a RESTful implementation for simplified integration with HPE and third-party applications; eAPI calls are available in the library, which is included with IMC Standard software.
- **Highly flexible and scalable deployment models**
helps deliver an extensive set of capabilities for managing large heterogeneous networks, and provides scalability and high availability through a flexible distributed deployment model. With its modular design, IMC software can be deployed across multiple servers to provide increased scalability and resilience.
- **Rich Resource management**
provides network discovery and topology, including detailed inventory of the network and accurate depictions of how it is configured. Supported views include Layer 2 and 3 as well as VLAN topology and the ability to create custom views like a dashboard homepage. Customization enables administrators to organize and control the network infrastructure. Supports multidevice context, Intelligent Resilient Fabric, and End-of-Life Notifications via device discovery
- **Telnet/SSH proxy**
with the Telnet/SSH proxy, an administrator can use a browser to remotely access and manage devices through Telnet/SSH without installing a Telnet/SSH tool on the PC client used to access the device. This promotes secure and controlled access to devices while providing auditing of changes on any device; supports SSH v1/v2
- **Service Monitor**
monitors the availability and responsiveness of common network services via probes that you configure; the probes reside on local and remote IMC software agents and test services from servers and devices that you select when configuring the probes; monitor these protocols: DNS, FTP, HTTP, TCP, UDP, VoIP (using NTA module), SMTP, DHCP, ICMP, Radius, TACACS+
- **High availability (Optional add-on license)**
Provides high availability (HA) for the IMC system by offering one or multiple standby IMC servers for redundancy. IMC HA can be implemented using a deployment with a remote database or shared storage.

Warranty and support

- **Electronic and telephone support**
Limited electronic and business-hours telephone support is available from Hewlett Packard Enterprise; to reach our support centers, refer to <http://www.hpe.com/networking/contact-support>; for details on the duration of support provided with your product purchase, refer to <http://www.hpe.com/networking/warrantysummary>
- **Software releases**
to find software for your product, refer to <http://www.hpe.com/networking/support>; for details on the software releases available with your product purchase, refer to <http://www.hpe.com/networking/warrantysummary>

Technical Specifications

HPE IMC Standard Software Platform with 50-node E-LTU (JG747AAE)

Aruba IMC Standard Software Platform with 50-node E-LTU (JH704AAE)

Minimum system hardware Server:

Intel® Pentium® 4 3.0 GHz
 4 GB RAM memory
 50 GB storage
 10/100 Mbps NIC
 Video card supporting 1024 x 768 resolution and sound card

Client:

Intel® Pentium® 4 2.0 GHz
 2 GB RAM memory
 50 GB storage
 10/100 Mbps NIC
 Video card supporting 1024 x 768 resolution and sound card

System requirements,
 recommended

Server:

3.0 GHz Intel® Xeon® or Intel® Core™ 2 Duo processor or equivalent
 4 GB RAM memory
 100 GB storage
 10/100 Mbps NIC
 Video card supporting 1024 x 768 resolution and sound card

Software (required)

Server:

Operating system: Red Hat Enterprise Linux 5.5 (Enterprise and Standard versions only)
 Red Hat Enterprise Linux 5.5 X64 (Enterprise and Standard versions only)
 Red Hat Enterprise Linux 5.9 (Enterprise and Standard versions only)
 Red Hat Enterprise Linux 5.9 X64 (Enterprise and Standard versions only)
 Red Hat Enterprise Linux 6.x X64 (Enterprise and Standard versions only)
 Windows Server 2008 R2 with Service Pack 1
 Windows Server 2008 R2 X64 with Service Pack 1
 Windows Server 2008 with Service Pack 2
 Windows Server 2008 X64 with Service Pack 2
 Windows Server 2012 R2 X64
 Windows Server 2012 X64 with KB2836988

Database:

Microsoft SQL Server 2008 Service Pack 3 (Windows only)
 Microsoft SQL Server 2008 R2 Service Pack 2 (Windows only)
 Microsoft SQL Server 2012 Service Pack 2 (Windows only)
 Microsoft SQL Server 2014 (Windows only)
 Oracle 11g Release 1 (Linux only)
 Oracle 11g Release 2 (Linux only)
 MySQL Enterprise Server 5.5 (Linux and Windows) (Up to 1000 devices are supported)
 MySQL Enterprise Server 5.6 (Linux and Windows) (Up to 1000 devices are supported)

Recommended software

Client:

Windows XP SP3 or later

Browser supported

IE 10 or 11
 Firefox 30 or later
 Chrome 35 or later

Hypervisor

VMware Workstation 6.5.x
 VMware Workstation 9.0.x
 VMware ESX Server 4.x
 VMware ESX Server 5.x

Technical Specifications

	Windows Server 2008 R2 Hyper-V Windows Server 2012 Hyper-V
Notes	Operating systems marked X64 are recommended. Client: JRE 1.6.0_update 27 or later is recommended. For fewer than 500 nodes, 1 CPU is sufficient; From 500 to 2,000 nodes, there should be 2 CPUs or 1 dual-core CPU; For more than 2,000 nodes, there should be 4 CPUs or 2 dual-core CPUs.
Services	Refer to the Hewlett Packard Enterprise website at http://www.hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, please contact your local Hewlett Packard Enterprise sales office.

HPE Intelligent Management Center Standard Software Platform accessories

License

HPE IMC Standard and Enterprise Additional 50-node E-LTU	JG749AAE
Aruba IMC Standard and Enterprise Additional 50-node E-LTU	JH714AAE
HPE PCM+ to IMC Standard Software Platform Upgrade with 200-node E-LTU	JG768AAE
HPE Intelligent Management Center High Availability Software E-LTU	JG771AAE
Aruba IMC High Availability Software E-LTU	JH711AAE

Software

HPE IMC Wireless Service Manager Software Module 50 Access Point E-LTU	JF414AAE
HPE IMC User Access Manager Software Module with 50-user E-LTU	JG752AAE
HPE IMC Endpoint Admission Defense Software Module with 50-user E-LTU	JG754AAE
HPE IMC TACACS+ Authentication Manager Software Module with 50-node E-LTU	JG764AAE
HPE IMC Network Traffic Analyzer Software Module with 5-node E-LTU	JG750AAE
Aruba IMC Network Traffic Analyzer Software Module with 5-node E-LTU	JH706AAE
HPE Intelligent Management Center QoS Manager E-LTU	JF408AAE
HPE IMC MPLS VPN Software Module with 50-node E-LTU	JF410AAE
HPE IMC Intelligent Analysis Reporter Software E-LTU	JG138AAE
HPE IMC Service Operation Management Software Module E-LTU	JG139AAE
HP IMC IPSec VPN Manager Software Module with 25-node E-LTU	JG144AAE
HP IMC Branch Intelligent Management System Software Module with 50-node E-LTU	JG265AAE
Aruba IMC Branch Intelligent Management System Software Module with 50-node E-LTU	JH708AAE
HPE IMC Service Health Manager Software Module E-LTU	JG398AAE
Aruba IMC Service Health Manager Software Module E-LTU	JH710AAE
HPE IMC Application Performance Manager Software Module 25-monitor E-LTU	JG489AAE
Aruba IMC Application Performance Manager Software Module with 25-monitor E-LTU	JH712AAE
HPE IMC VAN Connection Manager Software Module with E-LTU	JG494AAE
HPE IMC Remote Site Manager Software Module with E-LTU	JG495AAE
HPE IMC User Behavior Auditor Software Module with 50-user E-LTU	JG760AAE
HPE IMC Virtual Application Networking Fabric Manager Software E-LTU	JG770AAE
HPE IMC Virtual Application Networking Resource Automation Manager Software E-LTU	JG826AAE
HPE IMC Virtual Application Networking Software Defined Network Manager Software E-LTU	JG827AAE
HPE IMC Unified Communications Health Manager SW Module 2-monitor E-LTU	JG930AAE
HPE IMC Business Service Performance Software Module E-LTU	JH320AAE

Summary of Changes

Date	Version History	Action	Description of Change
06-Feb-2017	From Version 13 to 14	Added	Model added: JH704AAE SKUs added: JH714AAE, JH711AAE, JH706AAE, JH708AAE, JH710AAE, JH712AAE
05-Dec-2016	From Version 12 to 13	Changed	Software feature update
17-June-2016	From Version 11 to 12	Changed	Product description updated.
11-Dec-2015	From Version 10 to 11	Removed	SKU removed: JG399AAE
01-Dec-2015	From Version 9 to 10	Changed	QuickSpecs name changed to HPE Intelligent Management Center Standard Software Platform Product overview, Features and benefits and Technical Specifications were updated
29-Sep-2014	From Version 8 to 9	Changed	The QuickSpecs was completely revised
18-Sep-2014	From Version 7 to 8	Changed	Changes made on Features and Benefits
30-Sep-2013	From Version 6 to 7	Changed	The Product overview, Key Features, Features and Benefits, model specifications and Options were updated.
13-Jun-2013	From Version 5 to 6	Removed	License models were removed.
19-Feb-2013	From Version 4 to 5	Changed	The Product overview, Key Features, Features and Benefits, model specifications and Options were updated.
13-Feb-2012	From Version 3 to 4	Changed	The Features and Benefits, model names and Options were updated.
06-Apr-2011	From Version 2 to 3	Changed	The QuickSpecs was completely revised, including updating the title.
01-Mar-2011	From Version 1 to 2	Changed	An issue with the QuickSpecs PDF was corrected.

Summary of Changes



[Sign up for updates](#)

© Copyright 2017 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

To learn more, visit <http://www.hpe.com/networking>

Intel Pentium, Intel Core, and Intel Xeon are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft, Windows, and Windows Server are trademarks of the Microsoft Group of companies.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Oracle is a registered trademark of Oracle and/or its affiliates.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.



**Hewlett Packard
Enterprise**

c04111576 - 13834 - Worldwide - V14 - 6-February-2017

HPE FLEXFABRIC 5900 SWITCH SERIES



FIGURE 1. HPE FlexFabric 5901AF 48G
4XG 2QSFP+ Switch

KEY FEATURES

- New SKU JL864A with high performance, improved energy efficiency of 39–45% (Max./Idle 96W/70W in 5901AF vs. 175W/115W in 5900AF), and reduced heat dissipation of 83% (327 BTU/hr in 5901AF vs. 597 BTU/hr in 5900AF)
- High-density, high-performance Top-of-Rack (ToR) switch with 48 x 10/100/1000 Mbps RJ-45 ports, 4 x 1/10 SFP+ ports, and 2 x 40 QSFP ports that bridge the gap between legacy and modern networks
- HPE Intelligent Resilient Fabric (IRF) technology and software hot patch for greater resiliency and scalability
- Cut-through with low-latency and varying wirespeed performance
- Rich feature sets with IPv4 and IPv6 support with Layer 2, Layer 3, and QoS/ACL features
- OpenFlow and NETCONF for automating manual tasks and improving service delivery
- Dual, redundant hot-pluggable power supplies help in reduced power consumption

PRODUCT OVERVIEW

The HPE FlexFabric 5900 Switch Series are high-density, low-latency Top-of-Rack (ToR) networking switches suited for deployment at the access layer and management network of medium-sized and large enterprise data centers.

To meet the increased demand for virtualization, scalability, and programmability, these switches provide high-performance switching with low-latency and user-friendly OS (Comware v7). HPE Intelligent Resilient Fabric (IRF) helps in simpler, flatter, and agile networks by combining multiple physical switches into a logical device. Network and security features coupled with dual, redundant, hot-swappable power supplies ensure investment protection, reliability, and availability and allow advanced chassis power management.

These switches also provide multi-vendor network management with HPE Intelligent Management Center (IMC) for complete network visibility.

FEATURES AND BENEFITS

Low-latency and multiple wirespeed for demanding applications in data center environment

- The HPE FlexFabric 5900 Switch Series provide multiple wirespeed of 10/100/1000BASE-T and 1/10/40G fiber ports for high-performance and flexible deployments.

- All ports support full L2/L3 features, IPv4/IPv6 dual-stack, OpenFlow, and NETCONF for high scalability and software-defined network (SDN) support.
- HPE Intelligent Resilient Fabric (IRF) stacking enables uninterrupted L2 switching and L3 forwarding to eliminate operational complexity.

High-performance data center switching

- The HPE FlexFabric 5900 Switch Series delivers 336 Gbps switching capacity for the most demanding applications.
- It supports up to 250 Mpps throughput for data-intensive environments.
- With low latency (under a 1.5 μ s for 10GbE), this switch series delivers increased network throughput. It also includes two 40GbE QSFP+ ports for blazing fast uplinks.
- It supports Zero Touch Provisioning by eliminating human errors and automatically setting up network devices leading to accelerated ROI.

Simplicity and lower TCO

- The HPE FlexFabric 5900 Switch Series simplifies switch management by up to 88% (due to IRF stacking capability of nine switches resulting in 1/9th of overhead reduction)¹ with multiunit HPE Intelligent Resilient Fabric (IRF).
- Dual, redundant hot-swappable power supplies with reversible airflow (front to back/back to front) reduce power consumption.
- It supports centralized configuration, compliance and policy management, monitoring, and troubleshooting with HPE Intelligent Management Center (IMC) to provide a consistent network manageability experience.
- There are no extra hidden costs with a simple one license per switch for all OS features.
- All switch ports are active and ready to use without the need for activation licenses.

Business agility and resilience

- The HPE FlexFabric 5900 Switch Series delivers IRF < 50 ms convergence time allowing faster application response times.
- It provides In-Service Software Update (ISSU) enabling high availability with modular updates accomplished without any downtime.

Layer 2 switching and Layer 3 routing

- Supports a large number of Layer 2 devices with 32K MAC address table. Supports IEEE 802.1ad QinQ and selective QinQ that increase scalability by providing a hierarchical structure
- Supports jumbo frames with a frame size of up to 9216-byte, improving the performance of large data transfers
- Supports Device Link Detection Protocol (DLDP) that monitors link connectivity and shuts down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks

Warranty and support

- Limited lifetime warranty
See hpe.com/networking/warrantysummary for warranty and support information included with your product purchase.

- Software releases

To find software for your product, see hpe.com/networking/support; for details on the software releases available with your product purchase, see hpe.com/networking/warrantysummary.

¹ Because of stacking capability of nine switches, there is a management overhead reduction of 1/9th (11%).



HPE FLEXFABRIC 5900 SWITCH SERIES



Specifications	HPE FlexFabric 5901AF 48G 4XG 2QSFP+ Switch (JL864A)	HPE FlexFabric 5900AF 48G 4XG 2QSFP+ Switch (JG510A)
I/O ports and slots	48 x 10/100/1000 BASE-T ports support; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ 1000/10000, 2 QSFP+ 40GbE ports	48 x 10/100/1000 BASE-T ports support; Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only 4 SFP+ 1000/10000, 2 QSFP+ 40GbE ports
Additional ports and slots	1 x RJ-45 console port 1 x mini-USB port 1 x USB port 2 x out-of-band management ports (1 x SFP GbE port and one copper port)	1 x RJ-45 console port 1 x mini-USB port 1 x USB port 2 x out-of-band management ports (1 x SFP GbE port and one copper port)
Power supplies	2 power supply slots (AC/DC) 1 minimum power supply required (ordered separately)	2 power supply slots (AC/DC) 1 minimum power supply required (ordered separately)
Fan tray	2 fan tray slots Note: The customer must order fan trays, as they are not included with the switch. The system should not be operated without a fan tray for more than two minutes. The system should not be operated outside of the temperature range of 23°F (-5°C) to 113°F (45°C). Failure to comply with these operating requirements may void the product warranty.	2 fan tray slots Note: The customer must order fan trays, as fan trays are not included with the switch. This system requires two same-direction airflow fan trays to function properly. The system should not be operated with only one fan tray for more than 24 hours. The system should not be operated without a fan tray for more than two minutes. The system should not be operated outside of the temperature range of 32°F (0°C) to 113°F (45°C). Failure to comply with these operating requirements may void the product warranty.
Physical characteristics		
Dimensions	17.32 in. (w) x 14.17 in. (d) x 1.73 in. (h) 44 cm x 36 cm x 4.4 cm (1U height)	17.32 in. (w) x 18.11 in. (d) x 1.72 in. (h) 43.99 cm x 46.0 cm x 4.37 cm (1U height)
Weight	16.535 lb (< 7.5 kg)	< 10 kg
Memory and processor	1 GB flash; packet buffer size: 8 MB, 2 GB SDRAM	512 MB flash; packet buffer size: 9 MB, 2 GB SDRAM
Performance		
Latency	1GbE < 5 μs and 40GbE < 1.2 μs (64-byte packets)	10GbE: < 1.51 μs
Throughput	Up to 250 Mpps (64-byte packets)	Up to 250 Mpps (64-byte packets)
Routing/Switching capacity	336 Gbps	336 Gbps
Routing table size	16,000 entries (IPv4), 8,000 entries (IPv6)	16,000 entries (IPv4), 8,000 entries (IPv6)
MAC address table size	110,000 entries	128,000 entries
Environment		
Operating temperature	23°F to 113°F (-5°C to 45°C)	32°F to 113°F (0°C to 45°C)
Operating relative humidity	10% to 95%, noncondensing	10% to 90%, noncondensing
Acoustic	43.6/56.9 dB	Low-speed fan: 65.7 dB, high-speed fan: 70.6 dB



HPE FLEXFABRIC 5900 SWITCH SERIES (CONTINUED)

HPE FlexFabric 5901AF 48G 4XG 2QSFP+ Switch (JL864A)

Electrical characteristics																																														
Frequency	50/60 Hz	50/60 Hz																																												
Maximum heat dissipation	327.6 BTU/hr (345.63 kJ/hr)	597 BTU/hr (629.86 kJ/hr)																																												
AC voltage	100 to 240 VAC V rated	100 to 240 VAC V rated																																												
DC voltage	-48 VDC to -60 VDC V rated (depending on power supply chosen)	-48 VDC to -60 VDC V rated (depending on power supply chosen)																																												
Maximum power rating	96W (dual AC)	175W (dual AC)																																												
Idle power	70W (dual AC)	115W (dual AC)																																												
Notes	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with a fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.	Idle power is the actual power consumption of the device with no ports connected. Maximum power rating and maximum heat dissipation are the worst-case theoretical maximum numbers provided for planning the infrastructure with a fully loaded PoE (if equipped), 100% traffic, all ports plugged in, and all modules populated.																																												
Safety	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; Anatel; ULAR; GOST; EN 60950-1/A11; FDA 21 CFR Subchapter J; NOM; RoHS Compliance	UL 60950-1; EN 60825-1 Safety of Laser Products-Part 1; EN 60825-2 Safety of Laser Products-Part 2; IEC 60950-1; CAN/CSA-C22.2 No. 60950-1; Anatel; ULAR; GOST; EN 60950-1/A11; FDA 21 CFR Subchapter J; NOM; RoHS Compliance																																												
Emissions	CISPR 32:2015 Class A; VCCI Class A; EN 55032 Class A; ICES-003 Class A; AS/NZS CISPR 32 Class A; EN 61000-3-2:2014; EN 61000-3-3:2013; FCC (CFR 47, Part 15 B) Class A	VCCI Class A; EN 55022 Class A; ICES-003 Class A; ANSI C63.4 2003; AS/NZS CISPR 22 Class A; EN 61000-3-2:2006; EN 61000-3-3:1995+A1:2001+A2:2005; EMC Directive 2004/108/EC; FCC (CFR 47, Part 15) Class A																																												
Immunity	<table border="1"> <tr> <td>Generic</td> <td>ETSI EN 300 386 v1.6.1; ETSI EN 300 386 v2.1.1</td> </tr> <tr> <td>EN</td> <td>EN 55024:2010; EN55024:2010+A1:2015; CISPR 35:2016; EN55035:2017</td> </tr> <tr> <td>ESD</td> <td>EN 61000-4-2; IEC 61000-4-2</td> </tr> <tr> <td>Radiated</td> <td>EN 61000-4-3; IEC 61000-4-3</td> </tr> <tr> <td>EFT/Burst</td> <td>EN 61000-4-4; IEC 61000-4-4</td> </tr> <tr> <td>Surge</td> <td>EN 61000-4-5; IEC 61000-4-5</td> </tr> <tr> <td>Conducted</td> <td>EN 61000-4-6; IEC 61000-4-6</td> </tr> <tr> <td>Power frequency magnetic field</td> <td>IEC 61000-4-8; EN 61000-4-8</td> </tr> <tr> <td>Voltage dips and interruptions</td> <td>EN 61000-4-11; IEC 61000-4-11</td> </tr> <tr> <td>Harmonics</td> <td>EN 61000-3-2; IEC 61000-3-2</td> </tr> <tr> <td>Flicker</td> <td>EN 61000-3-3; IEC 61000-3-3</td> </tr> </table>	Generic	ETSI EN 300 386 v1.6.1; ETSI EN 300 386 v2.1.1	EN	EN 55024:2010; EN55024:2010+A1:2015; CISPR 35:2016; EN55035:2017	ESD	EN 61000-4-2; IEC 61000-4-2	Radiated	EN 61000-4-3; IEC 61000-4-3	EFT/Burst	EN 61000-4-4; IEC 61000-4-4	Surge	EN 61000-4-5; IEC 61000-4-5	Conducted	EN 61000-4-6; IEC 61000-4-6	Power frequency magnetic field	IEC 61000-4-8; EN 61000-4-8	Voltage dips and interruptions	EN 61000-4-11; IEC 61000-4-11	Harmonics	EN 61000-3-2; IEC 61000-3-2	Flicker	EN 61000-3-3; IEC 61000-3-3	<table border="1"> <tr> <td>Generic</td> <td>ETSI EN 300 386 v1.3.3</td> </tr> <tr> <td>EN</td> <td>EN 55024:1998+ A1:2001 + A2:2003</td> </tr> <tr> <td>ESD</td> <td>EN 61000-4-2; IEC 61000-4-2</td> </tr> <tr> <td>Radiated</td> <td>EN 61000-4-3; IEC 61000-4-3</td> </tr> <tr> <td>EFT/Burst</td> <td>EN 61000-4-4; IEC 61000-4-4</td> </tr> <tr> <td>Surge</td> <td>EN 61000-4-5; IEC 61000-4-5</td> </tr> <tr> <td>Conducted</td> <td>EN 61000-4-6; IEC 61000-4-6</td> </tr> <tr> <td>Power frequency magnetic field</td> <td>IEC 61000-4-8; EN 61000-4-8</td> </tr> <tr> <td>Voltage dips and interruptions</td> <td>EN 61000-4-11; IEC 61000-4-11</td> </tr> <tr> <td>Harmonics</td> <td>EN 61000-3-2; IEC 61000-3-2</td> </tr> <tr> <td>Flicker</td> <td>EN 61000-3-3; IEC 61000-3-3</td> </tr> </table>	Generic	ETSI EN 300 386 v1.3.3	EN	EN 55024:1998+ A1:2001 + A2:2003	ESD	EN 61000-4-2; IEC 61000-4-2	Radiated	EN 61000-4-3; IEC 61000-4-3	EFT/Burst	EN 61000-4-4; IEC 61000-4-4	Surge	EN 61000-4-5; IEC 61000-4-5	Conducted	EN 61000-4-6; IEC 61000-4-6	Power frequency magnetic field	IEC 61000-4-8; EN 61000-4-8	Voltage dips and interruptions	EN 61000-4-11; IEC 61000-4-11	Harmonics	EN 61000-3-2; IEC 61000-3-2	Flicker	EN 61000-3-3; IEC 61000-3-3
Generic	ETSI EN 300 386 v1.6.1; ETSI EN 300 386 v2.1.1																																													
EN	EN 55024:2010; EN55024:2010+A1:2015; CISPR 35:2016; EN55035:2017																																													
ESD	EN 61000-4-2; IEC 61000-4-2																																													
Radiated	EN 61000-4-3; IEC 61000-4-3																																													
EFT/Burst	EN 61000-4-4; IEC 61000-4-4																																													
Surge	EN 61000-4-5; IEC 61000-4-5																																													
Conducted	EN 61000-4-6; IEC 61000-4-6																																													
Power frequency magnetic field	IEC 61000-4-8; EN 61000-4-8																																													
Voltage dips and interruptions	EN 61000-4-11; IEC 61000-4-11																																													
Harmonics	EN 61000-3-2; IEC 61000-3-2																																													
Flicker	EN 61000-3-3; IEC 61000-3-3																																													
Generic	ETSI EN 300 386 v1.3.3																																													
EN	EN 55024:1998+ A1:2001 + A2:2003																																													
ESD	EN 61000-4-2; IEC 61000-4-2																																													
Radiated	EN 61000-4-3; IEC 61000-4-3																																													
EFT/Burst	EN 61000-4-4; IEC 61000-4-4																																													
Surge	EN 61000-4-5; IEC 61000-4-5																																													
Conducted	EN 61000-4-6; IEC 61000-4-6																																													
Power frequency magnetic field	IEC 61000-4-8; EN 61000-4-8																																													
Voltage dips and interruptions	EN 61000-4-11; IEC 61000-4-11																																													
Harmonics	EN 61000-3-2; IEC 61000-3-2																																													
Flicker	EN 61000-3-3; IEC 61000-3-3																																													
Management	HPE IMC; command-line interface; out-of-band management; SNMP manager; Telnet; FTP	HPE IMC; command-line interface; out-of-band management; SNMP manager; Telnet; FTP																																												
Services	Visit the Hewlett Packard Enterprise website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, contact your local HPE sales office.	Visit the HPE website at hpe.com/networking/services for details on the service-level descriptions and product numbers. For details about services and response times in your area, contact your local HPE sales office.																																												



STANDARDS AND PROTOCOLS APPLIES TO ALL PRODUCTS IN SERIES

BGP

- RFC 1163 Border Gateway Protocol (BGP)
- RFC 1771 BGPv4
- RFC 1997 BGP Communities Attribute
- RFC 2918 Route Refresh Capability
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4360 BGP Extended Communities Attribute
- RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4760 Multiprotocol Extensions for BGP-4

Device management

- RFC 1157 SNMP v1/v2c
- RFC 1305 NTPv3
- RFC 1591 DNS (client)
- RFC 1902 (SNMP v2)
- RFC 1908 (SNMP v1/2 coexistence)
- RFC 2573 (SNMP v3 applications)
- RFC 2576 (coexistence between SNMP v1, v2, v3)
- Multiple configuration files
- Multiple software images
- SSHv1/SSHv2
- TACACS/TACACS+

General protocols

- IEEE 802.1D MAC Bridges
- IEEE 802.1p Priority
- IEEE 802.1Q VLANs
- IEEE 802.1s Multiple Spanning Trees
- IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- IEEE 802.3ae 10-Gigabit Ethernet
- IEEE 802.3ag Ethernet OAM
- IEEE 802.3ah Ethernet in First Mile over Point-to-Point Fiber—EFMF
- IEEE 802.3x Flow Control



- RFC 768 UDP
- RFC 783 TFTP Protocol (revision 2)
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 826 ARP
- RFC 854 Telnet
- RFC 856 Telnet
- RFC 868 Time Protocol
- RFC 896 Congestion Control in IP/TCP Internetworks
- RFC 950 Internet Standard Subnetting Procedure
- RFC 1027 Proxy ARP
- RFC 1058 RIPv1
- RFC 1091 Telnet Terminal-Type Option
- RFC 1141 Incremental updating of the Internet checksum
- RFC 1142 OSI IS-IS Intra-domain Routing Protocol
- RFC 1191 Path MTU discovery
- RFC 1213 Management Information Base for Network Management of TCP/IP-based Internet
- RFC 1253 (OSPFv2)
- RFC 1531 Dynamic Host Configuration Protocol
- RFC 1533 DHCP Options and BOOTP Vendor Extensions
- RFC 1534 DHCP/BOOTP Interoperation
- RFC 1541 DHCP
- RFC 1591 DNS (client only)
- RFC 1624 Incremental Internet Checksum
- RFC 1723 RIPv2
- RFC 1812 IPv4 Routing
- RFC 2030 Simple Network Time Protocol (SNTP) v4
- RFC 2131 DHCP
- RFC 2236 IGMP Snooping
- RFC 2338 VRRP
- RFC 2453 RIPv2
- RFC 2581 TCP Congestion Control
- RFC 2644 Directed Broadcast Control
- RFC 2767 Dual Stacks IPv4 and IPv6
- RFC 3046 DHCP Relay Agent Information Option



- RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- RFC 4250 The SSH Protocol Assigned Numbers
- RFC 4251 SSH Protocol Architecture
- RFC 4252 SSH Authentication Protocol
- RFC 4253 SSH Transport Layer Protocol
- RFC 4254 SSH Connection Protocol
- RFC 4419 Diffie-Hellman Group Exchange for the SSH Transport Layer Protocol
- RFC 4594 Configuration Guidelines for DiffServ Service Classes
- RFC 4941 Privacy Extensions for Stateless Address Auto-configuration in IPv6

IPv6

- RFC 2080 RIPng for IPv6
- RFC 2460 IPv6 Specification
- RFC 2461 IPv6 Neighbor Discovery
- RFC 2462 IPv6 Stateless Address Auto-configuration
- RFC 2463 ICMPv6
- RFC 2464 Transmission of IPv6 over Ethernet Networks
- RFC 2473 Generic Packet Tunneling in IPv6
- RFC 2545 Use of MP-BGP-4 for IPv6
- RFC 2563 ICMPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2740 OSPFv3 for IPv6
- RFC 2767 Dual stacks IPv4 and IPv6
- RFC 3315 DHCPv6 (client and relay)
- RFC 4291 IPv6 Addressing Architecture
- RFC 4862 IPv6 Stateless Address Auto-configuration
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

MIBs

- RFC 1213 MIB II
- RFC 1907 SNMP v2 MIB
- RFC 2571 SNMP Framework MIB
- RFC 2572 SNMP-MPD MIB
- RFC 2573 SNMP-Notification MIB
- RFC 2573 SNMP-Target MIB
- RFC 2574 SNMP USM MIB
- RFC 2737 Entity MIB (version 2)



- RFC 3414 SNMP-User based-SM MIB
- RFC 3415 SNMP-View based-ACM MIB
- LLDP-EXT-DOT1-MIB
- LLDP-EXT-DOT3-MIB
- LLDP-MIB

Network management

- RFC 3164 BSD Syslog Protocol

OSPF

- RFC 1587 OSPF NSSA
- RFC 2328 OSPFv2
- RFC 3101 OSPF NSSA
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3623 Graceful OSPF Restart
- RFC 4577 OSPF as the Provider/Customer Edge
- RFC 4811 OSPF Out-of-Band LSDB
- Resynchronization
- RFC 4812 OSPF Restart Signaling
- RFC 4813 OSPF Link-Local Signaling

QoS/CoS

- IEEE 802.1p (CoS)
- RFC 2475 DiffServ Architecture
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 3247 Supplemental Information for the New Definition of the EF PHB (expedited forwarding per-hop behavior)
- RFC 3260 New Terminology and Clarifications for DiffServ

Security

- Access Control Lists (ACLs)
- SSHv2



HPE FLEXFABRIC 5900 SWITCH SERIES ACCESSORIES

Transceivers	<p>HPE X120 1G SFP LC LX Transceiver JD119B HPE X120 1G SFP RJ45 T Transceiver JD089B HPE X120 1G SFP LC SX Transceiver JD118B HPE X120 1G SFP LC BX 10-U Transceiver JD098B HPE X120 1G SFP LC BX 10-D Transceiver JD099B HPE X120 1G SFP LC LH100 Transceiver JD103A HPE X130 10G SFP+ LC SR Transceiver JD092B HPE X130 10G SFP+ LC LR Transceiver JD094B HPE X130 10G SFP+ LC BiDi 40km-Downlink Transceiver JL740A HPE X130 10G SFP+ LC ER 40km Transceiver JG234A HPE X130 10G SFP+ LC BiDi 40km-Uplink Transceiver JL739A HPE X130 10G SFP+ LC LH 80km XCVR JG915A HPE X130 10G SFP+ LC BiDi 10km-Uplink Transceiver JL737A HPE X130 10G SFP+ LC BiDi 10km-Downlink Transceiver JL738A HPE X140 40G QSFP+ LC BiDi 100m MM XCVR JL251A HPE X140 40G QSFP+ MPO SR4 XCVR JG325B HPE X140 40G QSFP+ CSR4 300m XCVR JG709A HPE X140 40G QSFP+ LC LR4 SM 10km 1310nm Transceiver JG661A HPE X140 40G QSFP+ MPO MM 850nm CSR4 300m Transceiver JG709A HPE X140 40G QSFP+ LC LR4L 2km SM Transceiver JL286A HPE X130 10G SFP+ LC LH80 tunable Transceiver JL250A</p>
Power supply	<p>HPE X361 150W 100–240VAC to 12VDC Power Supply JD362B HPE X361 150W 48–60VDC to 12VDC Power Supply JD366B HPE A58x0AF Back (Power Side) to Front (Port Side) Airflow 300W AC Power Supply JG900A (for JG510A only) HPE A58x0AF Back (Power Side) to Front (Port Side) Airflow 300W DC Power Supply JG901A (for JG510A only) HPE 58x0AF 650W AC Power Supply JC680A (for JG510A only)</p>
Fan	<p>HPE FlexFabric 5944 Power to Port Airflow (Back to Front) Fan Module JL838A HPE FlexFabric 5944 Port to Power Airflow (Front to Back) Fan Module JL837A HPE 58x0AF Back (Power Side) to Front (Port Side) Airflow Fan Tray JC682A (for JG510A only) HPE 58x0AF Front (Port Side) to Back (Power Side) Airflow Fan Tray JC683A (for JG510A only) HPE X711 Front (Port Side) to Back (Power Side) Airflow High Volume Fan Tray JG552A (for JG510A only) HPE X712 Back (Power Side) to Front (Port Side) Airflow High Volume Fan Tray JG553A (for JG510A only)</p>
Cables	<p>HPE X240 10G SFP+ 7m DAC Cable JC784C HPE FlexNetwork X240 10G SFP+ to SFP+ 0.65m Direct Attach Copper Cable JD095C HPE FlexNetwork X240 10G SFP+ to SFP+ 1.2m Direct Attach Copper Cable JD096C HPE FlexNetwork X240 10G SFP+ to SFP+ 3m Direct Attach Copper Cable JD097C HPE FlexNetwork X240 10G SFP+ to SFP+ 5m Direct Attach Copper Cable JG081C HPE FlexNetwork X240 40G QSFP+ QSFP+ 1m Direct Attach Copper Cable JG326A HPE FlexNetwork X240 40G QSFP+ QSFP+ 3m Direct Attach Copper Cable JG327A HPE FlexNetwork X240 40G QSFP+ QSFP+ 5m Direct Attach Copper Cable JG328A HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 1m Direct Attach Copper Splitter Cable JG329A HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 3m Direct Attach Copper Splitter Cable JG330A HPE FlexNetwork X240 40G QSFP+ to 4x10G SFP+ 5m Direct Attach Copper Splitter Cable JG331A HPE X2A0 40G QSFP+ 7m AOC Cable JL287A HPE X2A0 40G QSFP+ 10m AOC Cable JL288A HPE X2A0 40G QSFP+ 20m AOC Cable JL289A HPE X2A0 10G SFP+ 7m AOC Cable JL290A HPE X2A0 10G SFP+ 10m AOC Cable JL291A HPE X2A0 10G SFP+ 20m AOC Cable JL292A</p>



LEARN MORE AT
hpe.com/us/en/networking/comware.html

Make the right purchase decision.
Contact our presales specialists.



Chat

Email

Call



Get updates



SEZNAM PODDODAVATELŮ / ČESTNÉ PROHLÁŠENÍ

1. Název veřejné zakázky	
<u>Virtuální učebna pro FD ČVUT</u>	
2. Účastník zadávacího řízení	
Obchodní firma:	TECOM spol. s r. o.
Sídlo:	Praha 10, Štěrboholská 1421/37, PSČ 10200
IČO:	41196856
Právní forma:	Společnost s ručením omezeným

Účastník zadávacího řízení čestně prohlašuje, že nemá v úmyslu zadat určitou část výše uvedené veřejné zakázky poddodavateli.