



Présentation du commutateur

AT-DC2552XS/L3

Commutateur 10Gbs & 40 Gbs pour Dorsale et Datacenter

Cut Through pour une faible latence

Double alimentation

Double ventilation

Eco-Friendly



Présentation AT-DC2552XS/L3

Version 1.1 - Février 2016

© 2016 Allied Telesis International SAS. Tous droits réservés.

La reproduction de tout ou partie de ce document est strictement interdite sans l'autorisation écrite préalable d'Allied Telesis International SAS.

Allied Telesis International SAS se réserve le droit de modifier tout ou partie des spécifications techniques, ou tout autre type d'informations figurant dans ce document, sans avertissement préalable.

Les informations contenues dans ce document sont susceptibles de changer à tout instant. Allied Telesis International SAS ne saura être tenu pour responsable, en aucune circonstance, des conséquences résultant de l'utilisation des informations contenues dans ce document.

Sommaire

1.	PRESENTATION	4
2.	ACCESSOIRES.....	5
2.1.	ALIMENTATION	5
2.2.	VENTILATION	6
2.3.	MODULES OPTIQUES SUPPORTES	6
3.	ARCHITECTURE ET PERFORMANCES	8
4.	ALLIEDWARE PLUS	9
5.	FONCTIONNALITES	10
5.1.	ALLIED TELESIS MANAGEMENT FRAMEWORK (AMF)	10
5.2.	EMPILAGE : VCSTACK ET VCSTACK LD	13
5.3.	EPSR (ETHERNET PROTECTION SWITCHING RING)	18
5.4.	AGREGATION DE LIENS 802.3AD (LACP)	19
5.5.	VIRTUAL LOCAL AREA NETWORK (VLAN)	20
5.6.	AUTHENTIFICATION PAR PORT 802.1X ET NETWORK ACCESS CONTROL (NAC).....	20
5.7.	SPANNING TREE, RAPID SPANNING TREE ET MULTIPLE SPANNING TREE	22
5.8.	AUTO DETECTION DES EQUIPEMENTS TERMINAUX	22
5.9.	IGMP SNOOPING ET IGMP	22
5.10.	IPV4 ET IPV6.....	23
5.11.	JUMBO FRAMES	23
5.12.	SECURISATION DES PORTS.....	23
5.13.	FILTRAGE MATERIEL (ACLs)	24
5.14.	GESTION DE QUALITE DE SERVICE (QoS).....	24
5.15.	GESTION DES EVENEMENTS (TRIGGER)	25
5.16.	ADMINISTRATION ET SUPERVISION	25
6.	SPECIFICATIONS TECHNIQUES	26
7.	STANDARDS ET PROTOCOLES.....	29
8.	REFERENCES	34

1. Présentation

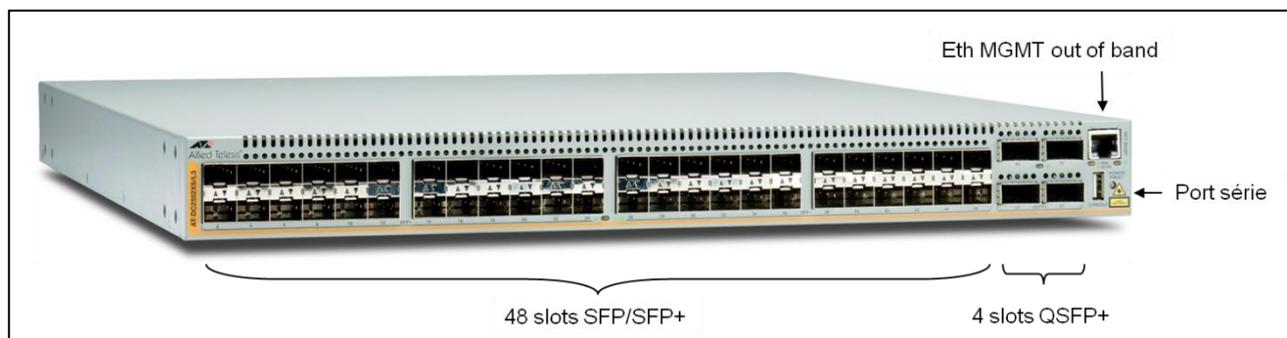
L'AT-DC2552XS/L3 est un commutateur présentant 48 emplacements 10 GbE (SFP +) et 4 emplacements 40 GbE (QSFP+). Sa densité d'interface et son fond de panier de 1280Gbps non bloquant le destine particulièrement aux environnements où transite un fort volume de données. Les interfaces 40 GbE peuvent être utilisées pour l'interconnexion traditionnelle à haut débit ou, grâce à la technologie VCStack, pour réaliser une pile de deux unités à haute performance. La distance entre les unités de la pile pouvant aller jusqu'à 10 Km, cette solution est, de part sa souplesse et les possibilités architecturales qu'elle permet, particulièrement intéressante pour réaliser un cœur de réseau résilient à haute capacité.

Outre son utilisation en tant qu'équipement de dorsale sur un réseau campus, l'AT-DC2552XS/L3 est également recommandé pour le centre de données (datacenter). En effet, son mode de commutation « Cut-Through » lui confère un temps de latence inférieur à 1 µs idéal pour connecter les serveurs et le stockage. De plus, le châssis 1U de ce commutateur peut intégrer deux alimentations et deux ventilations. Ces éléments étant extractible et insérable à chaud, L'AT-DC2552XS/L3 possède les caractéristiques indispensables dans les environnements les plus critiques nécessitant performance et haute disponibilité.

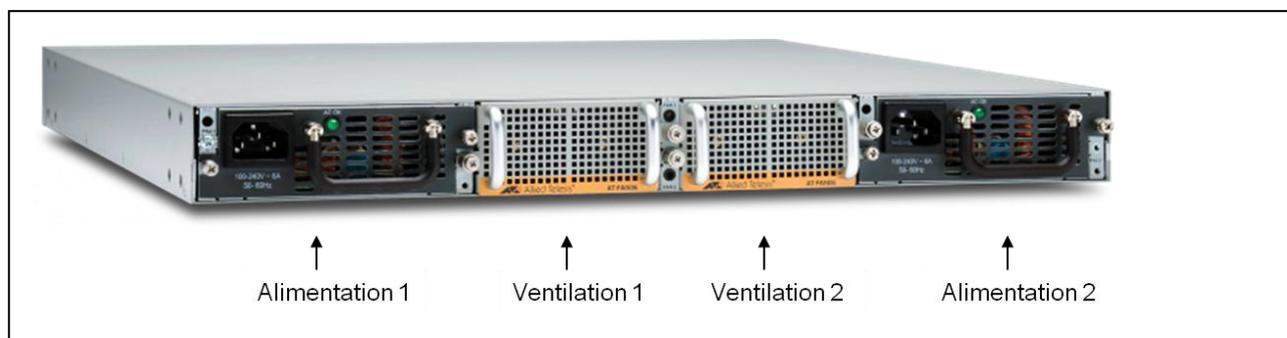
L'AT-DC2552XS/L3 embarque le système d'exploitation AlliedWare Plus commun à tous les commutateurs Entreprises, les routeurs, les firewalls ainsi que des solutions sans fil. Comme tous les équipements utilisant AlliedWare Plus, L'AT-DC2552XS/L3 supporte la technologie AMF (Allied Telesis Management Framework) qui permet de simplifier de manière spectaculaire tous les aspects opérationnels, à savoir le déploiement, la configuration, la maintenance, l'évolution du réseau ou remplacement d'unité.

Référence	Désignation
AT-DC2552XS/L3	Commutateur L3 empilable haute performance 48 x 10G SFP/SFP+ plus et 4 x 40G QSFP+ (livré sans alimentation et ventilation)
AT-PWR06-50	Alimentation 220VAC Hot Swap pour AT-DC2552XS
AT-FAN06	Module de ventilation Hot Swap pour AT-DC2552XS (deux modules sont nécessaires)
AT-FL-DC25-01	License Premium pour AT-DC2552XS/L3
AT-FL-DC25-AM20	Licence AMF master pour AT-DC2552XS/L3 jusqu'à 20 nœuds
AT-FL-DC25-AM40	Licence AMF master pour AT-DC2552XS/L3 jusqu'à 40 nœuds
AT-QSFP1CU	Quad SFP+ (QSFP+) Direct attach cable, Twinax, 1m (0 to 70°C) pour interconnexion ou empilage
AT-QSFP3CU	Quad SFP+ (QSFP+) Direct attach cable, Twinax, 1m (0 to 70°C) pour interconnexion ou empilage

AT-DC2552XS/L3 – Face avant



AT-DC2552XS/L3 – Face arrière



2. Accessoires

2.1. Alimentation

L'AT-DC2552XS/L3 est livré sans alimentation. Une seule alimentation suffit pour faire fonctionner le commutateur. Pour bénéficier d'une redondance, une deuxième alimentation peut être installée dans le boîtier, les deux alimentations fonctionnent alors en partage de charge.



- AT-PWR06-50 : alimentation Hot-Swap 100-240 VAC, 50/60 Hz
- Consommation typique 250 W
- Consommation maximale 280 W
- Chaleur dissipée : 900 BTU/hr

2.2. Ventilation

L'AT-DC2552XS/L3 est livré sans ventilation. Deux modules de ventilation doivent être installés pour un fonctionnement normal. Toutefois, la présence de deux modules permet de faire les opérations de maintenance sans interrompre la production.

- AT-FAN06 : module de ventilation pour ATDC2552XS/L3



2.3. Modules optiques supportés

2.3.1. Modules SFP 1 Gbs



Les 48 emplacements SFP/SFP+ acceptent les modules 1Gbs SFP suivants :

- AT-SPTX : 1000T 100 m sur cuivre Cat5e
- AT-SPSX : 1000SX GbE, 850 nm, jusqu'à 550 m sur fibre multimode
- AT-SPEX : 1000X GbE, 1310 nm, jusqu'à 2 km sur fibre multimode
- AT-SPLX10 : 1000LX GbE, 1310 nm, jusqu'à 10 km sur fibre monomode
- AT-SPLX40 : 1000Base-LX40, jusqu'à 40Km sur fibre monomode
- AT-SPZX80 : 1000Base-ZX, jusqu'à 80Km sur fibre monomode
- AT-SPBD10-13 : 1G sur 1 brin monomode 15 Km (à utiliser avec AT-SPBD10-14)
- AT-SPBD10-14 : 1G sur 1 brin monomode 15 Km (à utiliser avec AT-SPBD10-13)

2.3.2. Modules SFP+ 10Gbs



Les 48 emplacements SFP/SFP+ peuvent recevoir les modules 10Gbs SFP+ suivants :

- AT-SP10SR : 850 nm short-haul, 300 m sur fibre multimode 50/125µ
- AT-SP10LRM : 1310 nm short-haul, 220 m fibre multimode 62,5/125µ
- AT-SP10LR : 1310 nm medium-haul, 10 km sur fibre monomode
- AT-SP10ER40/I : 1310nm long-haul, 40 km sur fibre monomode

2.3.3. Câbles Direct Attach 1G/10Gbs (DAC 1G/10G)



Les emplacements SFP/SFP+ peuvent recevoir les câbles Direct Attach 1G/10G suivants :

- Câble Direct Attach de 1 m (SP10TW1)
- Câble Direct Attach de 3 m (SP10TW3)
- Câble Direct Attach de 7 m (SP10TW7)

2.3.4. Modules QSFP+ 40 Gbs et câbles Direct Attach 40Gbs (DAC 40G)

Les emplacements QSFP+ peuvent recevoir les modules et câbles Direct Attach suivants :

- AT-QSFPSR : 850 nm short-haul, jusqu'à 150 m sur fibre multimode
- AT-QSFPLR4 : 1310 nm medium-haul, jusqu'à 10 km sur fibre monomode
- AT-QSFP1CU câble cuivre Direct Attach QSFP+, 1 m
- AT-QSFP3CU câble cuivre Direct Attach QSFP+, 3 m
- AT-MTP12-1 : jarretière optique MTP pour AT-QSFPSR, 1 m
- AT-MTP12-5 : jarretière optique MTP pour AT-QSFPSR, 5 m

3. Architecture et performances

Grâce à leur architecture non bloquante, les AT-DC2552XS/L3 offrent des performances optimales quelque soit le volume de trafic traité. Les fonctionnalités de commutation de niveau 2 et de routage sont prises en charge de manière matérielle. C'est également le cas d'autres fonctions comme la gestion de qualité de service (QoS), le filtrage de trafic (ACL) et le traitement des flux multicast. L'utilisation de ces fonctions n'impacte donc pas les performances des commutateurs AT-DC2552XS/L3.

Référence	Matrice de commutation	Taux d'acheminement	Packet buffer
AT-DC2552XS/L3	1280 Gbps	952.32 Mpps	9 Mo

- Commutation « Cut Through »
- Temps de Latence 10GB : 800ns (trame de 64 octets)
- 16000 routes IPv4
- 8000 routes IPv6
- 128000 adresses MAC
- Jumbo frames maximum 12Kb
- CPU 1.2Ghz
- RAM 2 Go
- 128Mo de mémoire flash
- Wirespeed Switching (unicast et multicast) sur tous les ports Ethernet
- Jusqu'à 4094 VLAN
- Ports auto MDI/MDIX (port cuivre) et auto négociation
- Empilage jusqu'à 2 unités
- Empilage longue distance
- Double alimentation extractible à chaud
- Double ventilation extractible à chaud
- Refroidissement de l'arrière vers l'avant

4. AlliedWare Plus



Les commutateurs AT-DC2552XS/L3 embarquent le système d'exploitation AlliedWare Plus. Ce système d'exploitation s'appuie sur une syntaxe (CLI) conforme au standard de l'industrie. Un exemple de la syntaxe est présenté ci-dessous :

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2 name pedago
awplus(config-vlan)# vlan 3 name eleves
awplus(config-vlan)# exit
awplus(config)#interface port1.0.1-1.0.5
awplus(config-if)#switchport access vlan 2
awplus(config-if)#interface port1.0.10-1.0.15
awplus(config-if)#switchport access vlan 3
awplus(config-if)#interface port1.0.24
awplus(config-if)#switchport mode trunk
awplus(config-if)#switchport trunk allowed vlan add 2,3
awplus(config-if)#exit
```

AlliedWare Plus est commun à l'ensemble de nos commutateurs Campus, nos commutateurs Datacenter, nos commutateurs Industriels, nos routeurs, nos firewalls ainsi qu'à des solutions WiFi. D'une part l'interface en ligne de commande est identique entre ces différentes gammes de produits et, d'autre part, ils supportent la technologie AMF (Allied Telesis Management Framework) ce qui, associé à de puissantes possibilités de scripting, permet d'automatiser les tâches et, plus largement, de simplifier de manière conséquente tous les aspects opérationnelles. AMF est décrit plus en détail dans la suite de ce document.

Certaines fonctionnalités avancées nécessitent une licence optionnelle pour être utilisées. Se reporter à la fin de ce document pour en avoir la liste détaillée.

5. Fonctionnalités

5.1. Allied Telesis Management Framework (AMF)



Allied Telesis Management Framework (AMF) est un ensemble de fonctionnalités, simplifiant l'administration du réseau. En utilisant ces outils, la plupart des tâches courantes peuvent être automatisées et effectuées beaucoup plus rapidement. Grâce à AMF, les équipes informatiques sont déchargées de tâches indispensables mais répétitives et qui prennent beaucoup de temps. De même, AMF permet de limiter au maximum le temps nécessaire pour effectuer des opérations de maintenance. Par exemple, avec AMF, en cas de remplacement d'un commutateur, il suffit de connecter la nouvelle unité sortant de son emballage pour rétablir le service, la présence d'un expert n'est alors pas requise et la satisfaction des utilisateurs s'en trouve améliorée car le service est rétabli dans un temps record.

AMF est supporté par l'ensemble de nos commutateurs Campus, nos commutateurs Datacenter, nos commutateurs Industriels, nos routeurs, nos firewalls ainsi que certaines de nos solutions WiFi. Associé à de puissantes possibilités de scripting, AMF permet d'automatiser les tâches routinières et, plus largement, de simplifier de manière conséquente tous les aspects opérationnelles.

Aucun logiciel supplémentaire n'est nécessaire, AMF est inclus dans le système d'exploitation AlliedWare Plus qui est embarqué dans les équipements. Pour constituer un domaine AMF, au moins un équipement doit jouer le rôle de maître, cela peut être un x510, un x610, un x930, un DC2552XS/L3, un SBx908 ou un SBx8100. De base, un équipement pouvant être maître maître AMF peut gérer jusqu'à 3 nœuds, un nœud pouvant être un équipement isolé ou une pile. Il est possible d'augmenter le nombre de nœuds supportés par un maître par ajout d'une licence optionnelle.

Les licences AMF suivantes sont disponible pour l'AT-DC2552XS/L3 :

- Licence jusqu'à 20 nœuds
- Licence jusqu'à 40 nœuds

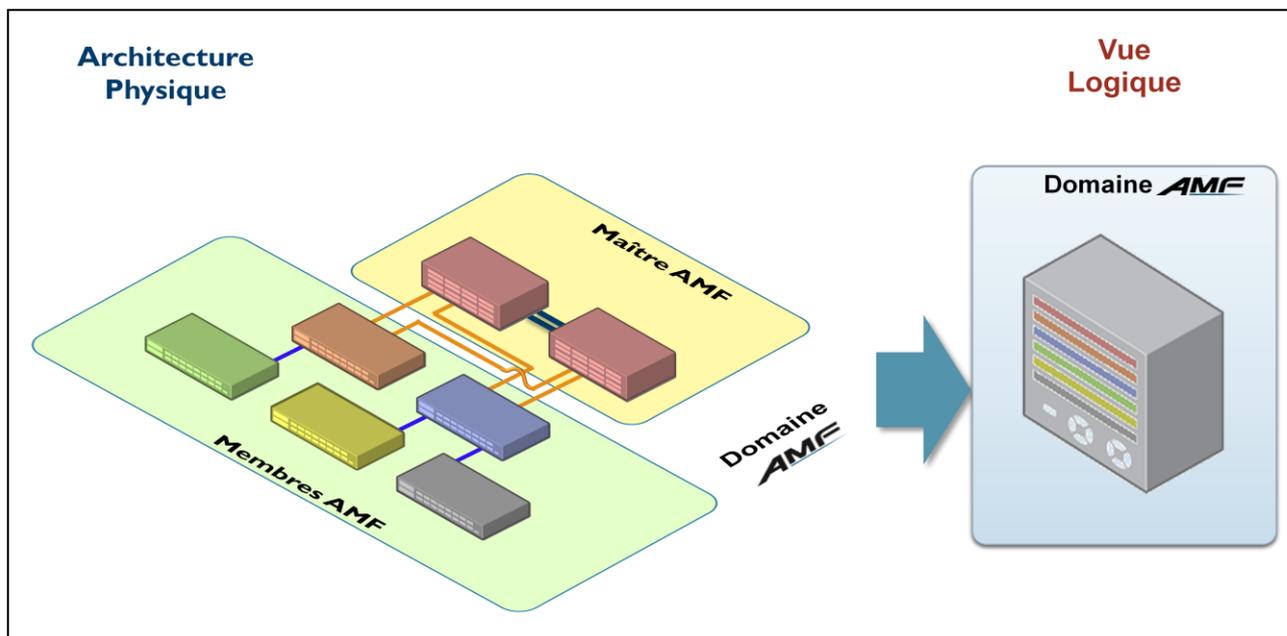
AMF permet de virtualiser le réseau afin de disposer de services que l'on a sur un châssis : CLI unifiée, sauvegarde automatique, restauration automatique, création de groupes, mise à jour automatique, provisioning...

Les fonctionnalités apportées par AMF sont décrites ci dessous :

Gestion centralisée des équipements (CLI unifiée)

L'ensemble des commutateurs d'un domaine AMF est présenté comme un commutateur unique. L'administrateur gère alors un châssis virtuel dont chaque carte représente un nœud du domaine AMF. Par exemple, la création d'un nouveau VLAN sur l'ensemble de

l'infrastructure se fait en quelques secondes comme si un seul commutateur était à configurer. De même, lors de contrôles ou d'investigation les informations, les statistiques ou l'état de différents nœuds peuvent être consolidés dans une seule sortie obtenue à l'aide d'une seule commande.



Sauvegarde automatique

Le système d'exploitation, la configuration et les éventuels scripts de tous les nœuds du domaine sont automatiquement sauvegardés sur le ou les commutateurs maîtres. Ces sauvegardes peuvent également être stockées automatiquement sur un serveur.

Restauration automatique des nœuds

En cas de remplacement d'un commutateur du domaine AMF, reconnecter une nouvelle unité qui sort de son emballage suffit à rétablir le service. Elle récupère automatiquement son système d'exploitation, son fichier de configuration ainsi que ses éventuels scripts et licences sur le maître.

Création de groupe

Automatiquement, les nœuds du domaine AMF sont placés dans des groupes (commutateurs d'accès, commutateurs PoE, commutateur x510 ...). Un nœud peut appartenir à plusieurs groupes et il est possible de créer des groupes personnalisés. Cette fonction est pratique pour adresser seulement certains nœuds du domaine.

Mise à jour automatique des nœuds

La mise à jour des nœuds du domaine ou d'un groupe de nœuds peut se faire à l'aide d'une seule commande. Les commutateurs sont alors mis à jour automatiquement et séquentiellement pour limiter au maximum l'indisponibilité du système d'information.

Planification de tâches

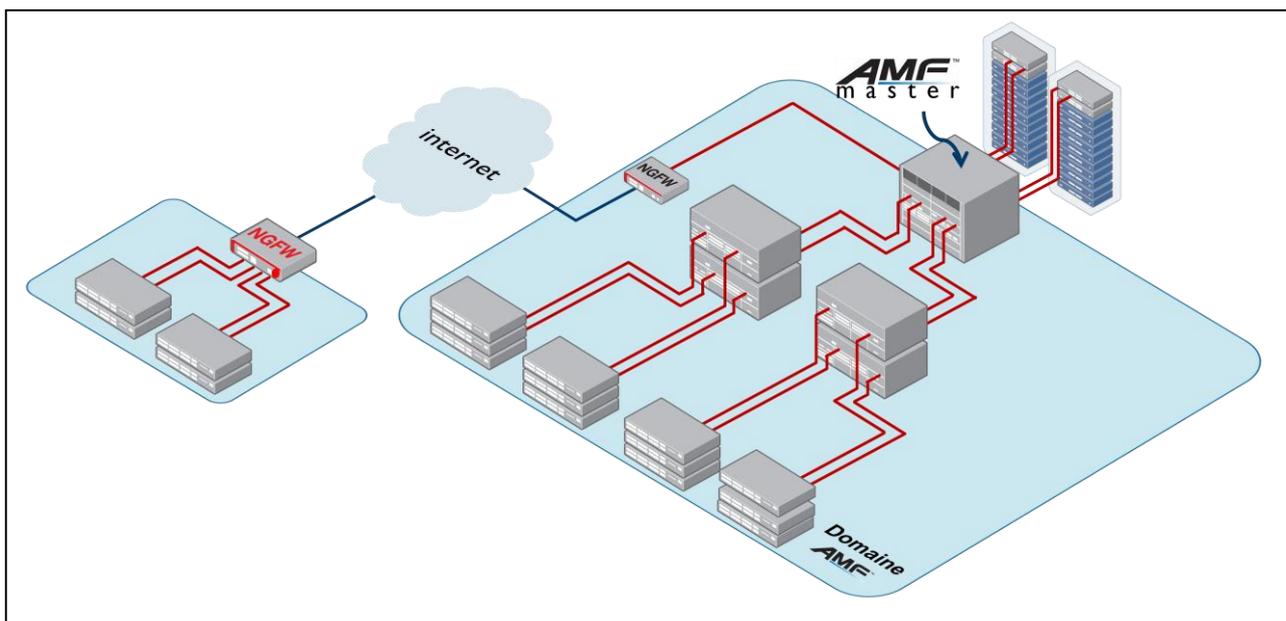
Toutes les tâches peuvent être planifier. Ainsi, une opération de sauvegarde ou de mise à jour peut être planifiée pour une exécution unique ou récurrente.

Provisioning d'équipement

Avec AMF, un nœud qui n'est pas encore présent dans le domaine peut être configuré; il sera automatiquement configuré lorsqu'il sera connecté à l'infrastructure. Il est également possible de cloner la configuration d'un nœud existant pour en provisionner un nouveau; les paramètres pouvant entrer en conflit, tels que les adresses IP, sont alors désactivés et clairement présentés.

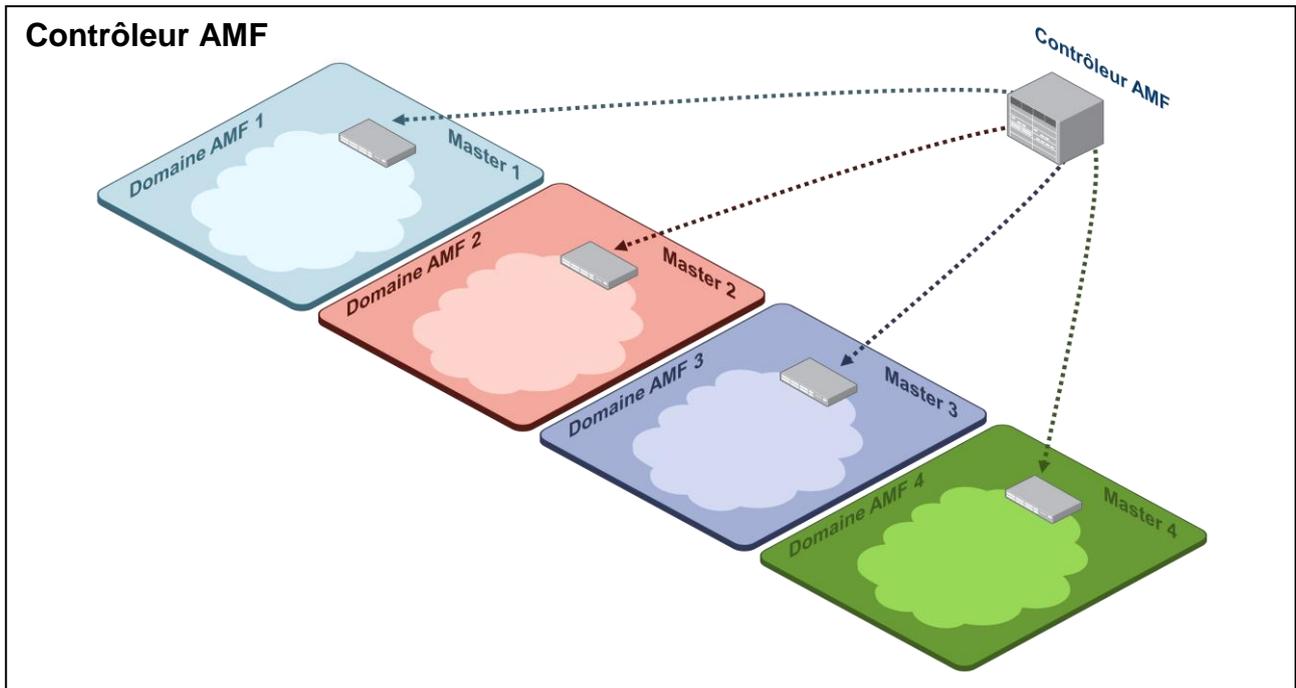
Gestion de domaine non continu

Les différents nœuds d'un domaine AMF n'ont pas obligatoirement besoin d'être attachés directement les uns avec les autres. Des équipements tiers non AMF peuvent s'intercaler entre des nœud AMF de même qu'il est possible d'avoir un nuage de niveau 3 (ex. Internet) entre deux parties d'un même domaine AMF.



Consolidation de plusieurs domaines AMF avec un Contrôleur AMF

Un domaine AMF peut contenir au maximum 120 nœuds, un nœuds étant un équipement ou une pile. C'est donc un maximum de 952 commutateurs qui peuvent être inclus dans le même domaine AMF. Toutefois, il peut être souhaitable de structurer son réseau en créant plusieurs de moindres importances. La fonction Contrôleur AMF permet alors de consolider ces différents domaines AMF en fournissant un point d'entrée unique. Cette fonction est supportée par les châssis SBx8100.



5.2. Empilage : VCStack et VCStack LD

La technologie VCStack™ (Virtual Chassis Stacking) permet d'empiler à très haut débit plusieurs commutateurs. Le châssis virtuel forme alors un commutateur unique constitué de plusieurs unités. La fonction d'empilage permet d'évoluer graduellement tout en mettant en place une architecture haute disponibilité à forte densité de ports.

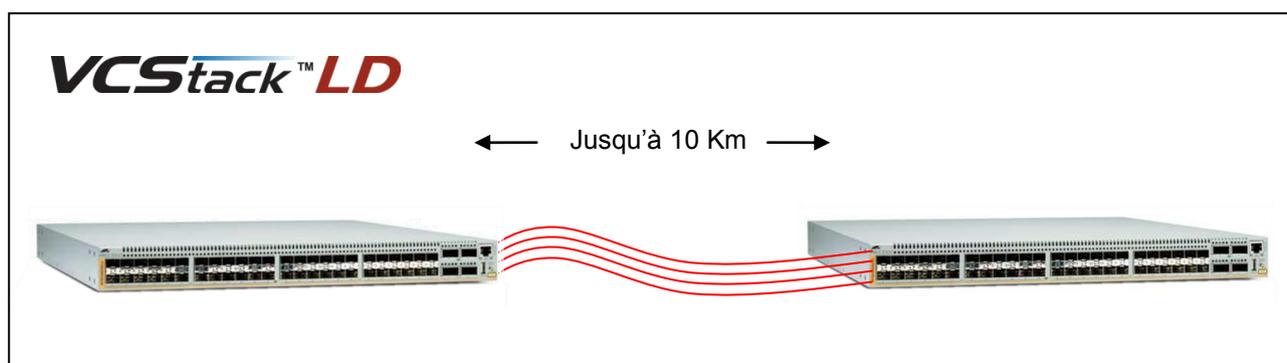
VCStack™ permet d'empiler les AT-DC2552XS/L3 lorsqu'ils sont dans un même local technique en utilisant des câbles Direct Attach 40 Gbs ou des jarretières MTP associées à des modules QSFP+.

Jusqu'à 2 unités AT-DC2552XS/L3 peuvent être empilées avec une capacité totale d'interconnexion allant jusqu'à 320 Gbps.



- AT-QSFP1CU câble cuivre Direct Attach QSFP+, 1 m
- AT-QSFP3CU câble cuivre Direct Attach QSFP+, 3 m
- AT-MTP12-1 : jarretière optique MTP pour AT-QSFPSR, 1 m
- AT-MTP12-5 : jarretière optique MTP pour AT-QSFPSR, 5 m

Il est également possible de les empiler en utilisant des modules QSFP+ et des liaisons optiques standards, il peut ainsi y avoir jusqu'à 10 Km entre les unités (VCStack Long Distance – VCStack LD).



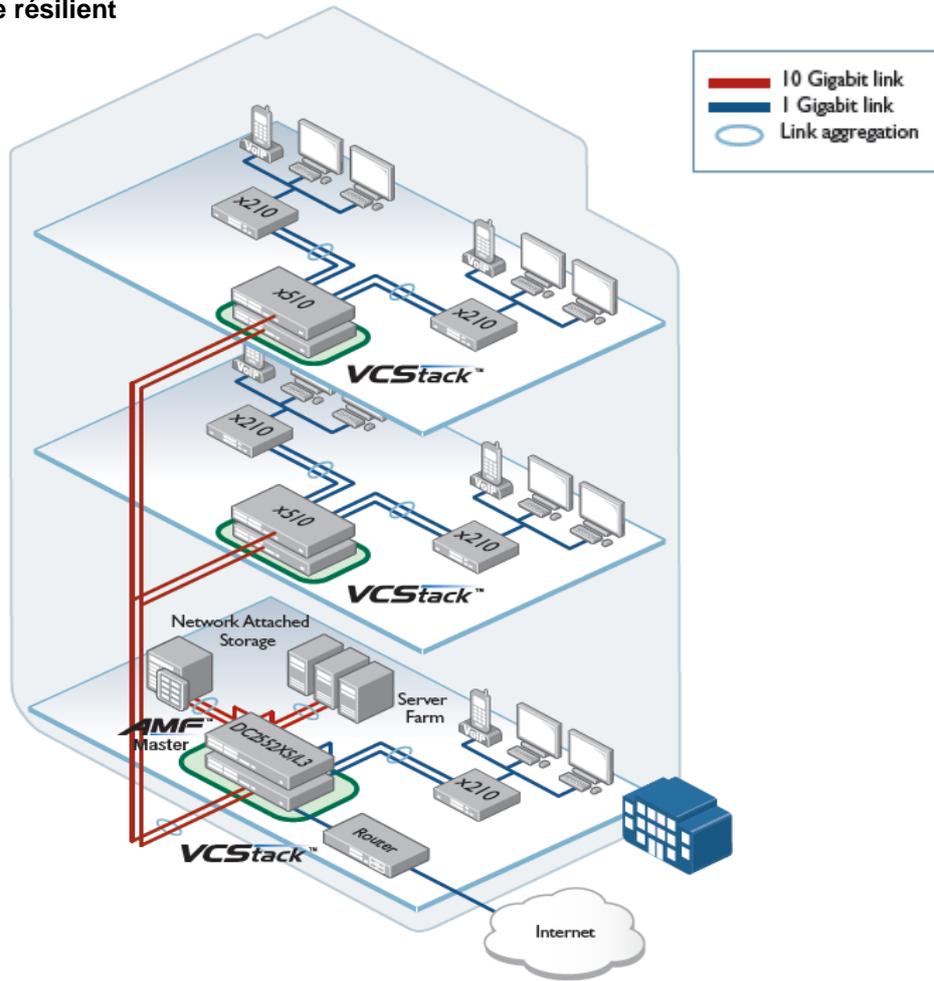
Interactions entre VCStack / VCStack LD et AMF

VCStack et VCStack LD peuvent être utilisés simultanément à AMF. Dans ce cas, si une unité d'une pile doit être restaurée, c'est VCStack qui s'en chargera sans qu'il y ait de conflit avec AMF. De même lors d'une opération de mise à jour, AMF se chargera de la mise à jour du maître et ce dernier, à l'aide de VCStack, fera la mise à jour des autres unités de la pile. Les autres opérations se déroulent sans particularités, AMF considérant la pile comme un seul commutateur.

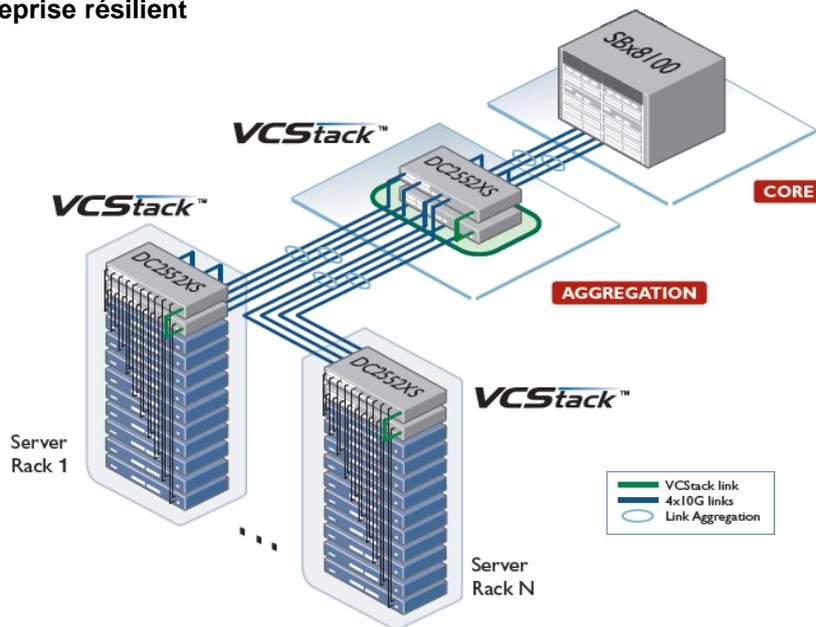
Architecture résiliente avec VCStack

Les possibilités d'empilage des commutateurs permettent de mettre en place de manière simple des architectures hautement disponibles, sans avoir à configurer de processus tels que Spanning Tree et VRRP pouvant rendre les tâches de maintenances plus complexes. Seuls des agrégats 802.3ax LACP sont alors à configurer pour obtenir la haute disponibilité.

Réseau d'entreprise résilient



Datacenter d'entreprise résilient



Fast Failover : reprise sur incident automatique en 50 ms

Dans une pile, l'une des unités a le rôle de maître. Le commutateur maître s'occupe de la gestion de la pile en prenant le contrôle des autres unités mutualisant ainsi le plan de management, de contrôle et de données. Le fichier de configuration de la pile est toutefois distribué dans toutes les unités de la pile et les tables de toutes les unités sont maintenues à jour à l'identique. Ainsi dans une pile tous les commutateurs peuvent potentiellement avoir la fonction de maître et la reprise sur incident automatique est de l'ordre de 50 ms dans le cas de la perte de maître actif et transparente dans le cas de la perte d'une unité esclave.

Architecture distribuée et ingénierie de trafic optimisée

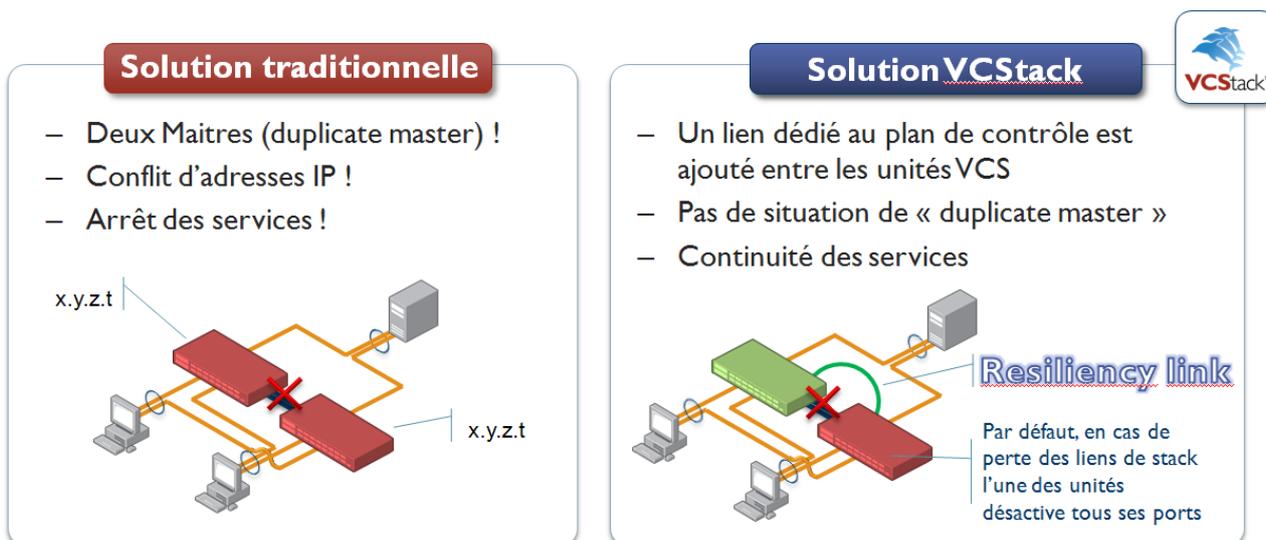
Au sein d'une pile, le trafic des utilisateurs est géré de manière optimum. En effet, quelles que soient les fonctionnalités utilisées, les données utilisateurs prennent toujours le plus court chemin entre le port d'entrée et le port de sortie. Si le port d'entrée et le port de sortie sont situés sur la même unité, le trafic reste en local de celle-ci, autrement dit, le trafic ne transitera par le maître que s'il se trouve sur le plus court chemin.

Maintenance de la pile simplifiée

L'extraction d'une unité ou l'insertion d'une nouvelle unité peuvent se faire à chaud sans perturber le fonctionnement des autres unités. De même, le remplacement d'une unité se fera facilement, la nouvelle récupérant automatiquement le fichier de configuration sur le maître.

Resiliency link

Pour se prémunir des effets d'une séparation accidentelle de la pile pouvant conduire à une interruption du réseau, il est possible de mettre en place un lien supplémentaire entre les unités d'une pile (Resiliency Link). Ainsi, si la pile est accidentellement scindée en deux, l'apparition de maîtres multiples pouvant entrer en conflit est évitée.



Provisioning d'unité

Il est possible de configurer une unité qui n'est pas présente dans une pile. Ainsi lorsque l'unité sera ajoutée, elle sera automatiquement configurée.

Adresse MAC virtuelle

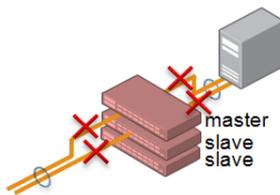
Une adresse MAC Virtuelle peut être configurée pour la pile. Ainsi, l'adresse MAC de la pile ne dépend pas de l'unité qui est maître ce qui contribue notamment à rétablir les communications routées rapidement lors d'un incident.

Rolling Reboot

Une pile de peut être redémarrée automatiquement unité par unité. Il est ainsi possible de faire des opérations de maintenance, telle qu'une mise à jour, sans coupure du réseau.

Solution traditionnelle

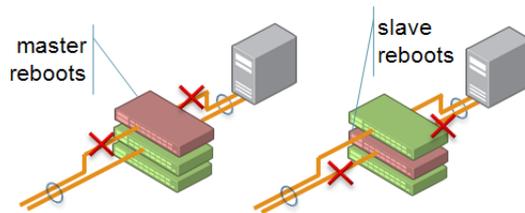
- Toutes les unités redémarrent en même temps
- Interruption des services !



Solution VCStack



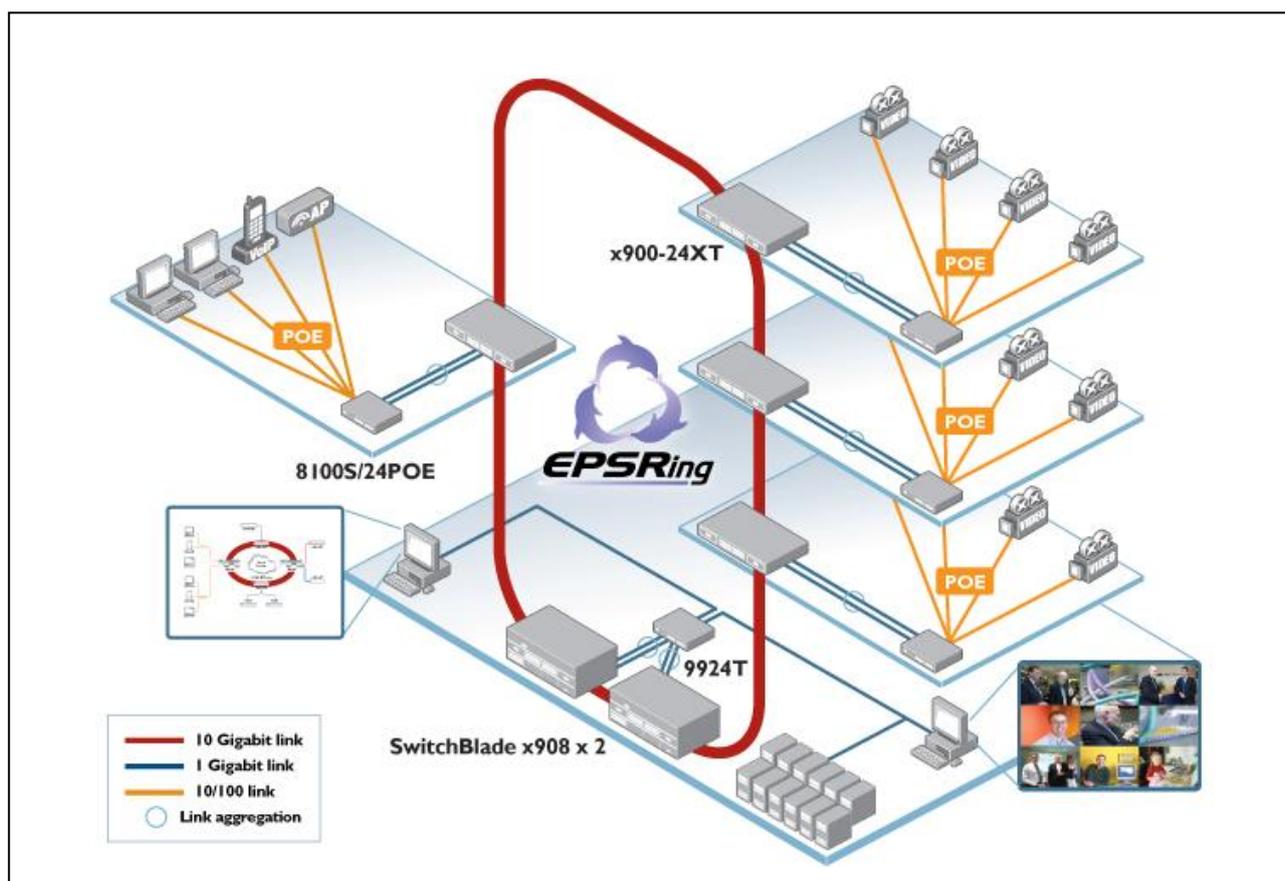
- Fonction **Rolling Reboot**
- Les unités d'un châssis virtuel redémarrent une par une
- Pas d'interruption des services



5.3. EPSR (Ethernet Protection Switching Ring)

Ethernet Protection Switching Ring

EPSR (Ethernet Protection Switching Ring) permet de mettre en place une topologie en anneau avec un temps de reprise sur incident en moins de 50 ms. La reprise sur incident est donc transparente pour l'utilisateur quelle que soit la nature de l'application utilisée (téléphonie, vidéo, télévision...).



EPSR est particulièrement bien adapté aux solutions nécessitant une disponibilité de service sans faille. On peut par exemple citer les systèmes de vidéo surveillance ou certains sites industriels.

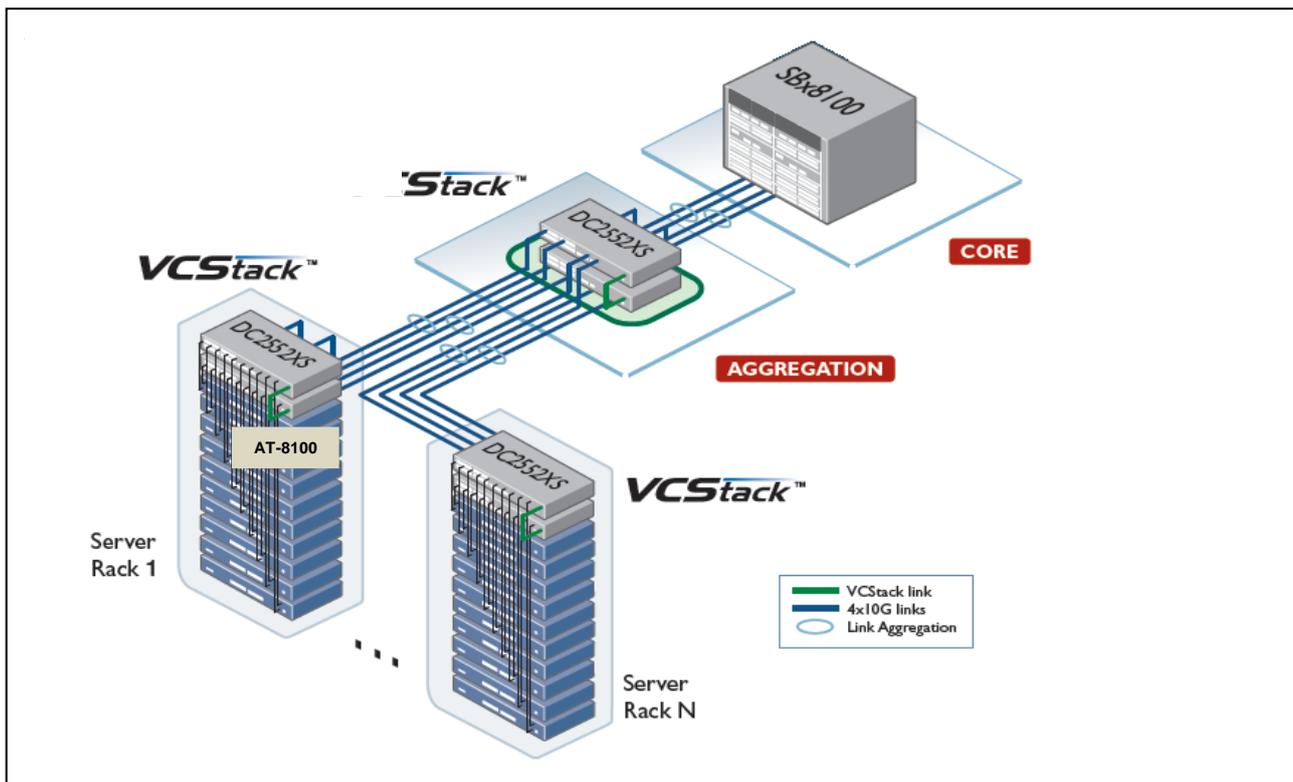
EPSR Superloop Prevention (EPSR SLP)

EPSR supporte la fonction Super Loop Prevention. Cette fonction permet d'associer une interface à plusieurs domaines EPSR. Il est ainsi possible de mettre en place des topologies sophistiquées sans avoir à utiliser une variante de Spanning Tree.

5.4. Agrégation de liens 802.3ad (LACP)

- Conforme au standard IEEE 802.3ax Link aggregation (static and LACP)
- Conforme au standard IEEE 802.3ad Static and dynamic link aggregation
- Jusqu'à 128 agrégats de 8 ports peuvent être créés
- Agrégation distribuée : les ports peuvent appartenir à différentes unités d'une pile
- Reprise sur incident et répartition de charge automatiques

L'agrégation de liens peut être de type statique ou s'appuyer sur le protocole LACP (Link Aggregation Control Protocol). Les ports d'un agrégat peuvent se situer sur différentes unités d'une pile. La répartition de charge est automatique sur les différents liens physiques d'un agrégat. En association avec la fonction VCStack™, l'agrégation de liens permet de mettre facilement en place une architecture haute disponibilité qui sera simple à maintenir.



5.5. Virtual Local Area Network (VLAN)

Il est possible de créer jusqu'à 4094 VLANs selon les critères suivants :

- VLAN par port
- VLAN par protocole
- VLAN par Subnet IP
- Support du 802.1q

Les VLANs peuvent être définis de manière statique et de manière dynamique par le biais du protocole GVRP. L'identifiant des VLANs peut être transporté selon le standard 802.1q.

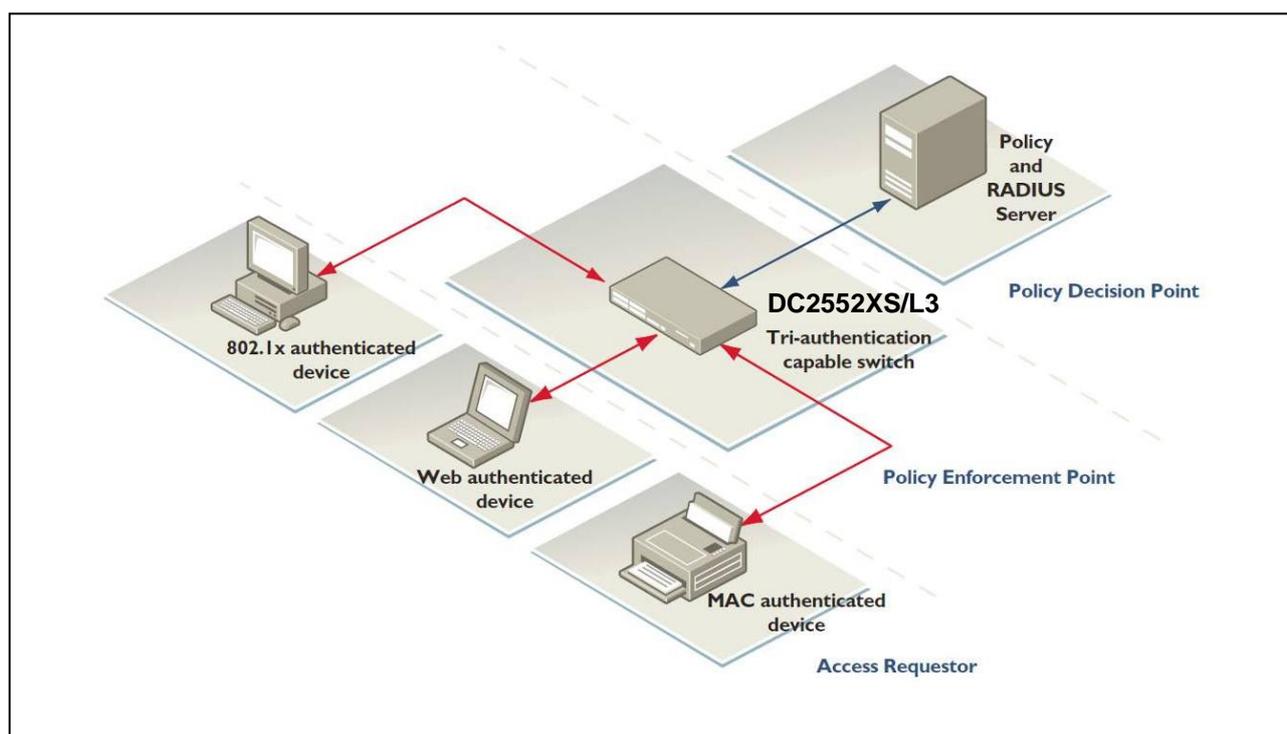
La fonction Private VLAN permet de créer des VLAN dans lesquels les ports clients ne peuvent communiquer qu'avec un ou plusieurs ports uplink. Ceci permet d'interdire de manière simple toutes les communications entre les clients locaux et de ne les autoriser à communiquer qu'avec des ressources accessibles via un lien uplink. Ainsi, la configuration et l'administration s'en trouvent grandement facilitées puisqu'il est possible de mettre en place un seul VLAN par groupe et de n'utiliser ainsi qu'un seul réseau IP. Cette fonction est particulièrement bien adaptée aux environnements de type hôtel ou pépinière d'entreprise.

5.6. Authentification par port 802.1x et Network Access Control (NAC)

- 802.1x (EAP-MD5, -OTP, -PEAP, -TTLS, -TLS)
- Support des modes mono-suppliquant ou multi-suppliquant
- Authentification sur adresse MAC
- Authentification par portail Web captif
- Serveur Radius intégré
- Support de plusieurs serveurs Radius externes
- Assignment dynamique de VLAN
- Multiple assignment dynamique de VLAN
- VLAN Invité
- Network Access Control (NAC)

L'accès au réseau peut être contrôlé par le biais de l'authentification 802.1x. Dans ce cadre, les utilisateurs authentifiés peuvent être placés automatiquement dans leur VLAN (affectation dynamique de VLAN), tandis que les utilisateurs non authentifiés peuvent être placés dans un VLAN isolé (VLAN invité), afin de restreindre leurs possibilités de

communication. Ces fonctionnalités sont également disponibles pour les équipements de disposant pas de client 802.1x (comme des imprimantes), l'authentification se basant alors sur l'adresse MAC de l'équipement (authentification par adresse MAC). Une troisième méthode d'authentification (portail web captif) augmente encore les possibilités de sécurisation de l'infrastructure. Les commutateurs AT-x510 supportent par ailleurs l'utilisation conjointe de chacune de ces 3 méthodes sur le même port, et peuvent authentifier plusieurs équipements sur un même port, y compris conjointement avec l'affectation dynamique de VLANs (multi-suppliquant, affectation dynamique de VLANs multiples).



En s'appuyant sur les différents mécanismes décrits ci-dessus, il est possible de mettre en place un contrôle de l'intégrité des équipements terminaux en plus de leur authentification ou de celle des utilisateurs. En cas de non-conformité à la politique de sécurité de l'entreprise, une correction automatique peut avoir lieu par le biais d'un VLAN spécifique. Cette solution, appelée Network Access Control (NAC), nécessite l'utilisation d'équipement ou de logiciel tiers. Les équipements Allied Telesis sont compatibles avec un grand nombre de solutions disponibles sur le marché et sont certifiés avec les acteurs majeurs (Microsoft NAP, Symantec SNAC).

5.7. Spanning Tree, Rapid Spanning Tree et Multiple Spanning Tree

- Spanning Tree (802.1d)
- Rapid Spanning Tree (802.1w)
- Multiple Spanning Tree (802.1s)

Les commutateurs AT-x510 sont en mesure de gérer la redondance de liens entre plusieurs commutateurs. Afin d'éviter le bouclage Ethernet de ce type d'architecture, il est nécessaire de mettre en place un algorithme (Spanning Tree) qui permet la fermeture des liens redondants. En cas de perte d'un des liens opérationnels, l'algorithme détermine quel lien ouvrir pour qu'il y ait continuité de service. Le temps nécessaire à la reconfiguration du réseau est appelé temps de convergence.

Il est possible de faire fonctionner le Spanning Tree en mode Normal (Spanning Tree 802.1d) ou en mode Rapid (Rapid Spanning Tree 802.1w). Le temps de convergence n'est que de quelques secondes lorsque le RSTP est utilisé.

Le Multiple Spanning Tree (MSTP 802.1s), tout en conservant les avantages du Rapid Spanning Tree, permet en outre la répartition de charge par VLAN ou par groupe de VLANs sur les différents chemins de l'architecture.

5.8. Auto détection des équipements terminaux

Les fonctionnalités LLDP (Link Layer Discovery Protocol, IEEE 802.1AB), LLDP-MED (Link Layer Discovery Protocol / Media Endpoint Discovery) et Voice VLAN permettent une gestion banalisée du parc d'équipements terminaux, quel que soit leur type (ordinateurs, téléphones IP, etc...). L'activation de ces fonctionnalités permet aux commutateurs AT-x510 de découvrir automatiquement le type d'équipement raccordé sur un port RJ45, et d'appliquer dynamiquement au port une configuration adaptée à l'équipement raccordé (identifiant de VLAN data et/ou voix, configuration CoS, puissance PoE délivrée, etc...).

5.9. IGMP Snooping et IGMP

Les commutateurs AT-x510 implémentent IGMP Snooping v1/2/3. Les flux multicast IPv4 sont donc correctement gérés au niveau 2 en étant transmis uniquement sur les ports du commutateur derrière lesquels sont connectés des clients en ayant fait la demande. Dans le cas où cette fonctionnalité n'est pas activée, les flux multicast seraient envoyés sur la totalité des ports du domaine de broadcast (VLAN). Toutefois, pour que l'IGMP Snooping remplisse son rôle, une fonction d'IGMP Querier est nécessaire dans le domaine de broadcast. Cette fonction d'IGMP Querier peut également être assurée par les commutateurs AT-x510.

5.10. IPv4 et IPv6

Jusqu'à 1000 interfaces de niveau 3 peuvent être configurées et jusqu'à 8 adresses IP peuvent être associées à une interface de niveau 2 (Multihoming). Outre le routage statique, les protocoles de routage supportés sont RIP v1/v2 et ng, OSPFv2/v3, BGP4/4+ et MBGP. Le support matériel d'ECMP (Equal Cost Multi Path) permet de répartir la charge sur plusieurs routes présentant le même coût. Pour une même destination, jusqu'à huit routes différentes peuvent être utilisées.

Les protocoles de routage multicast PIM-DM, PIM-SM, PIM-SSM pour IPv4 et IPv6 sont également supportés

5.11. Jumbo Frames

Cette fonction permet l'émission et la réception de trames de grandes tailles. Ceci est particulièrement intéressant pour la connexion de serveurs car il y a amélioration du débit utile du fait de la bande passante moins importante consommée par les entêtes. De plus, le nombre de trames moins important à traiter peut entraîner une baisse de charge au niveau de la CPU des serveurs.

La taille maximum de trame jumbo est de 12Kb

5.12. Sécurisation des ports

Cette fonctionnalité permet de contrôler les stations connectées sur chacun des ports via leur adresse MAC. Si ce mode est activé, le commutateur est en mesure d'apprendre les adresses MAC connectées sur un port jusqu'à une limite définie par l'utilisateur comprise entre 1 et 256. Ensuite, toute nouvelle adresse MAC source est rejetée sur ce port. Dans le cas où une adresse MAC source non autorisée se présente sur le port, 3 types d'actions peuvent être activées:

- Rejet des paquets, sans aucune autre action
- Rejet des paquets et envoi d'un Trap SNMP
- Rejet des paquets, envoi d'un Trap SNMP et désactivation du port.

5.13. Filtrage matériel (ACLs)

Les ACLs (Access List) permettent, entre autres, de désigner les trafics qui sont autorisés et ceux qui sont interdits. La mise en place de règles de filtrage s'appuie sur des fonctions matérielles, l'utilisation d'ACLs n'impacte donc pas les performances du commutateur. Les flux peuvent être identifiés selon des combinaisons de critères de niveau 3 et 4.

Les ACL sont également utilisées avec les fonctions suivantes :

- **Mirroring :**
il est possible de recopier spécifiquement un type de flux quelque soit son port d'entrée.
- **Policy Based Routing (PBR) :**
il est possible d'identifier des flux au moyen d'ACLs afin de leur faire emprunter une route spécifique. Cette fonctionnalité est prise en charge de manière matérielle et n'a donc pas d'impact sur les performances.
- **Gestion de qualité de service QoS)**

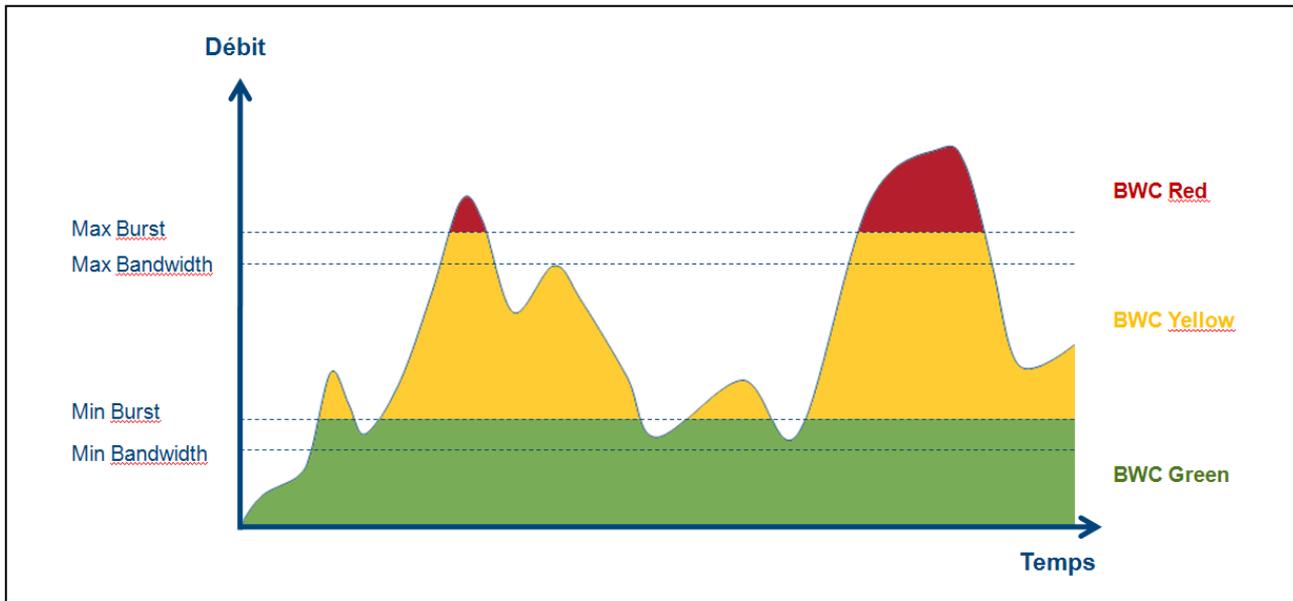
5.14. Gestion de qualité de service (QoS)

Ces commutateurs peuvent gérer la QoS en lisant le champs 802.1p ou DSCP. Ils peuvent également marquer ou remarquer ces champs selon une combinaison de critères de multi niveaux tels que adresses IP source, adresse IP destination, ports applicatif source et destination.

En plus de la gestion de priorité, le niveau de bande passante minimum accordé à un flux en cas de congestion peut être garanti. Il est également possible de fixer une limite maximum d'utilisation de bande passante par flux, l'excédant de trafic pouvant alors être remarqué et traité à un niveau de priorité moindre ou simplement rejeté selon le souhait de l'administrateur.

La classification de trafic est effectuée à vitesse filaire sur des critères multi champs pouvant inclure les champs 802.1p et le DSCP. Ces commutateurs possèdent 8 files d'attente par port et gère 8 niveaux de priorité. Les autres caractéristiques pouvant être mentionnées sont les suivantes :

- **Limitation de bande passante en sortie sur chaque port**
- **Contrôle du rejet de paquets par marquage 3 couleurs (vert, jaune, rouge)**



- Faible latence pour les applications voix et multimédia
- Contrôle de la QoS par MIB SNMP
- Vidage des files d'attente en Strict Priority (SPQ), Round Robin pondéré (WRR), Mix scheduling (SPQ + jusqu'à 2 groupes WRR)
- Limitation de bande passante en sortie sur chaque port

5.15. Gestion des événements (Trigger)

Cette fonction permet d'appeler des scripts lorsque survient certains événements (Date et heure fixe, changement d'état d'une interface, charge CPU dépassant un certain seuil, modification de topologie ...). Le ou les script lus par un Trigger peuvent contenir n'importe quelle commande AlliedWare Plus. De nombreux événements peuvent être surveillés par le biais de ce module, il est ainsi possible de configurer le commutateur de telle manière à ce qu'il s'adapte automatiquement si le contexte change.

5.16. Administration et supervision

AlliedWare Plus les versions 1, 2c et 3 de SNMP. L'administration et la supervision peuvent donc se faire en étant authentifié et avec des échanges chiffrés. L'interface en ligne de commande est accessible au travers du réseau par Telnet ou par SSH v2 pour que les échanges soient sécurisés.

6. Spécifications techniques

Interfaces

48 slots SFP+ (1G/10G)
4 slots QSFP+ (4x10G/40G)
Un port console port RS-232 (connecteur USB)
Une Interface de management out of band (eth0) 10/100/1000T (RJ-45 connector)
Auto négociation, MDI-MDI-X
Forwarding rate 952.32Mpps
Switching capacity 1280Gbps
Packet buffer 9 Mo

Performances

IPv4 routes 16K
IPv6 routes 8K
128 K MAC addresses
Taille maximum des jumbo frames : 12Kb
Temps de latence en mode Cut-through entre ports 10GB : 800ns (trame de 64 octets)
CPU 1.2 Ghz, RAM 2GB, Mémoire flash 128Mo
Wirespeed switching (unicast et multicast) sur tous les ports Ethernet

Outils de diagnostic

Built-In Self Test (BIST)
Find-me device locator
Automatic link flap detection et port shutdown
Optical Digital Diagnostic Monitoring (DDM)
UniDirectional Link Detection (UDLD)
Ping polling pour IPv4 and IPv6
Port mirroring
TraceRoute pour IPv4 and IPv6

IPv4

Black hole routing
Directed broadcast forwarding
DNS relay
Equal Cost Multi Path (ECMP) routing
Policy-based routing
Route maps
Route redistribution (OSPF, BGP, RIP)
Static unicast and multicast routes pour IPv4
UDP broadcast helper (IP helper)
Jusqu'à 64 Virtual Routing and Forwarding (VRF lite) domains (with license)

IPv6

Client et relais DHCPv6
Client et relais DNSv6
IPv4 and IPv6 dual stack
IPv6 aware storm protection et QoS
Management sur IPv6 networks with SNMPv6, Telnetv6 and SSHv6
NTPv6 client et serveur
Routage statique unicast et multicast pour IPv6
Log to IPv6 hosts with Syslog v6

Management

Allied Telesis Management Framework (AMF) enables powerful centralized management and zero-touch device installation and recovery

Try AMF for free with the built-in AMF Starter license

Console management port on the front panel for ease of access

Eco-friendly mode allows ports and LEDs to be disabled to save power

Industry-standard CLI with context-sensitive help

Powerful CLI scripting engine

Comprehensive SNMP MIB support for standards based device management

Built-in text editor

Event-based triggers allow user-defined scripts to be executed upon selected system events

Qualité de Service (QoS)

8 priority queues with a hierarchy of high priority queues for real time traffic, and mixed scheduling, for each switch port

Limit bandwidth per port or per traffic class down to 64kbps

Wirespeed traffic classification with low latency essential for VoIP and real-time streaming media applications

Policy-based QoS based on VLAN, port, MAC and

General packet classifiers

Policy-based storm protection

Extensive remarking capabilities

Taildrop for queue congestion control

Strict priority, weighted round robin or mixed scheduling

IP precedence and DiffServ marking based on layer 2, 3 and 4 headers

Resilience

Control Plane Prioritization (CPP) ensures the CPU always has sufficient bandwidth to process network control traffic

Dynamic link failover (host attach)

EPSRing (Ethernet Protection Switched Rings) with SuperLoop Protection (SLP) and enhanced recovery for extra resiliency

Loop protection : loop detection and thrash limiting

PVST+ compatibility mode

STP root guard

Long-Distance VCStack with 40G QSFP+ modules

QSFP+ stacking ports can be configured as 40G Ethernet ports

VCStack fast failover minimizes network disruption

Securité

Access Control Lists (ACLs) basée sur des critères de niveaux 3 et 4

Guest VLANs et auth-fail VLAN configurable

Authentication, Authorisation and Accounting (AAA)

Protection du bootloader par mot de passé possible pour sécuriser l'équipement

BPDU protection

DHCP snooping, IP source guard et Dynamic ARP Inspection (DAI)

DoS attack blocking et virus throttling

Dynamic VLAN assignment

Filtrage d'adresse MAC and MAC address lock-down

Network Access and Control (NAC)

Port-based learn limits (intrusion detection)

Private VLANs pour contrôler les communication d'utilisateurs dans un même VLAN

Secure Copy (SCP)

Strong password security and encryption

Tri-authentication: MAC-based, web-based et IEEE 802.1x

Spécifications environnementales

Température de fonctionnement 0°C to 40°C

Température de stockage -20°C to 60°C

Taux d'humidité en fonctionnement 10% to 80% (sans condensation)

Taux d'humidité los du stockage 5% to 90% (sans condensation)

Certifications sécurité et électromagnétique

EMI: FCC class A, CISPR class A, EN55022 class A

C-TICK, VCCI Class A, CE

Immunity: EN50024, EN601000-3-3, EN601000-3-2

Safety : UL 60950-1 (cULus), EN60950-1 (TUV)

Restrictions on Hazardous Substances (RoHS) Compliance

Conforme avec le standard RoHS Européen

Spécifications physiques

19 inch rack mount

Dimensions 44.1 cm x 46 cm x 4.4 cm (W x D x H) 17.4 in x 18.1 in x 1.7 in

Poids 8.3 kg /18.3 lb (châssis seul) 11.3 kg/24.9 lb (châssis avec 2 ventilations et 2 alimentations)

Alimentation

100-240V AC (10% auto-ranging), 50/60 Hz

Maximum current: 14A @ 100V

Dissipation thermique : 900 BTU/hr

Consommation électrique

250 W typique (max 280W)

Contenu de l'emballage

Commutateur AT-DC2552XS/L3

Câble de management (RS-232 - USB)

Pieds caoutchoucs autocollants

Kit de montage en baie 19'

Pays d'origine

Chine

7. Standards et protocoles

AlliedWare Plus Operating System

Version 5.4.5-2

Authentication

RFC 1321 MD5 Message-Digest algorithm

RFC 1828 IP authentication using keyed MD5

Border Gateway Protocol (BGP)

BGP dynamic capability

BGP outbound route filtering

RFC 1772 Application of the Border Gateway Protocol (BGP) in the Internet

RFC 1997 BGP communities attribute

RFC 2385 Protection of BGP sessions via the TCP MD5 signature option

RFC 2439 BGP route flap damping

RFC 2545 Use of BGP-4 multiprotocol extensions for IPv6 inter-domain routing

RFC 2858 Multiprotocol extensions for BGP-4

RFC 2918 Route refresh capability for BGP-4

RFC 3392 Capabilities advertisement with BGP-4

RFC 3882 Configuring BGP to block Denial-of-Service (DoS) attacks

RFC 4271 Border Gateway Protocol 4 (BGP-4)

RFC 4360 BGP extended communities

RFC 4456 BGP route reflection - an alternative to full mesh iBGP

RFC 4724 BGP graceful restart

RFC 4893 BGP support for four-octet AS number space

RFC 5065 Autonomous system confederations for BGP

Chiffrement

FIPS 180-1 Secure Hash standard (SHA-1)

FIPS 186 Digital signature standard (RSA)

FIPS 46-3 Data Encryption Standard (DES and 3DES)

Ethernet

IEEE 802.1AX Link aggregation (static and LACP)

IEEE 802.2 Logical Link Control (LLC)

IEEE 802.3 Ethernet

IEEE 802.3ab 1000BASE-T

IEEE 802.3ad Static and dynamic link aggregation

IEEE 802.3ae 10 Gigabit Ethernet

IEEE 802.3ba 40 Gigabit Ethernet

IEEE 802.3x Flow control - full-duplex operation

IEEE 802.3z 1000BASE-X

IPv4

RFC 768 User Datagram Protocol (UDP)

RFC 791 Internet Protocol (IP)

RFC 792 Internet Control Message Protocol (ICMP)

RFC 793 Transmission Control Protocol (TCP)

RFC 826 Address Resolution Protocol (ARP)

RFC 894 Standard for the transmission of IP datagrams over Ethernet networks

RFC 919 Broadcasting Internet datagrams

RFC 922 Broadcasting Internet datagrams in the presence of subnets

RFC 932 Subnetwork addressing scheme

RFC 950 Internet standard subnetting procedure
RFC 951 Bootstrap Protocol (BootP)
RFC 1027 Proxy ARP
RFC 1035 DNS client
RFC 1042 Standard for the transmission of IP datagrams over IEEE 802 networks
RFC 1071 Computing the Internet checksum
RFC 1122 Internet host requirements
RFC 1191 Path MTU discovery
RFC 1256 ICMP router discovery messages
RFC 1518 An architecture for IP address allocation with CIDR
RFC 1519 Classless Inter-Domain Routing (CIDR)
RFC 1542 Clarifications and extensions for BootP
RFC 1591 Domain Name System (DNS)
RFC 1812 Requirements for IPv4 routers
RFC 1918 IP addressing
RFC 2581 TCP congestion control

IPv6

RFC 1981 Path MTU discovery for IPv6
RFC 2460 IPv6 specification
RFC 2464 Transmission of IPv6 packets over Ethernet networks
RFC 3056 Connection of IPv6 domains via IPv4 clouds
RFC 3484 Default address selection for IPv6
RFC 3596 DNS extensions to support IPv6
RFC 4007 IPv6 scoped address architecture
RFC 4193 Unique local IPv6 unicast addresses
RFC 4291 IPv6 addressing architecture
RFC 4443 Internet Control Message Protocol (ICMPv6)
RFC 4861 Neighbor discovery for IPv6
RFC 4862 IPv6 Stateless Address Auto-Configuration (SLAAC)
RFC 5014 IPv6 socket API for source address selection
RFC 5095 Deprecation of type 0 routing headers in IPv6
RFC 5175 IPv6 Router Advertisement (RA) flags option
RFC 6105 IPv6 Router Advertisement (RA) guard

Management

AMF MIB and SNMP traps
AT Enterprise MIB
SNMPv1, v2c and v3
IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
RFC 1155 Structure and identification of management information for TCP/IP-based Internets
RFC 1157 Simple Network Management Protocol (SNMP)
RFC 1212 Concise MIB definitions
RFC 1213 MIB for network management of TCP/IP-based Internets: MIB-II
RFC 1215 Convention for defining traps for use with the SNMP
RFC 1227 SNMP MUX protocol and MIB
RFC 1239 Standard MIB
RFC 1724 RIPv2 MIB extension
RFC 2011 SNMPv2 MIB for IP using SMIv2
RFC 2012 SNMPv2 MIB for TCP using SMIv2
RFC 2013 SNMPv2 MIB for UDP using SMIv2
RFC 2096 IP forwarding table MIB
RFC 2578 Structure of Management Information v2 (SMIv2)
RFC 2579 Textual conventions for SMIv2
RFC 2580 Conformance statements for SMIv2

RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions
RFC 2741 Agent extensibility (AgentX) protocol
RFC 2787 Definitions of managed objects for VRRP
RFC 2819 RMON MIB (groups 1,2,3 and 9)
RFC 2863 Interfaces group MIB
RFC 3164 Syslog protocol
RFC 3176 sFlow: a method for monitoring traffic in switched and routed networks
RFC 3411 An architecture for describing SNMP management frameworks
RFC 3412 Message processing and dispatching for the SNMP
RFC 3413 SNMP applications
RFC 3414 User-based Security Model (USM) for SNMPv3
RFC 3415 View-based Access Control Model (VACM) for SNMP
RFC 3416 Version 2 of the protocol operations for the SNMP
RFC 3417 Transport mappings for the SNMP
RFC 3418 MIB for SNMP
RFC 3635 Definitions of managed objects for the Ethernet-like interface types
RFC 3636 IEEE 802.3 MAU MIB
RFC 4188 Definitions of managed objects for bridges
RFC 4318 Definitions of managed objects for bridges with RSTP
RFC 4560 Definitions of managed objects for remote ping, traceroute and lookup operations
RFC 6527 Definitions of managed objects for VRRPv3

Multicast

Bootstrap Router (BSR) mechanism for PIM-SM
IGMP query solicitation
IGMP snooping (IGMPv1, v2 and v3)
IGMP snooping fast-leave
IGMP/MLD multicast forwarding (IGMP/MLD proxy)
MLD snooping (MLDv1 and v2)
PIM-SM and SSM for IPv6
RFC 1112 Host extensions for IP multicasting (IGMPv1)
RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2715 Interoperability rules for multicast routing protocols
RFC 3376 IGMPv3
RFC 3810 Multicast Listener Discovery v2 (MLDv2) for IPv6
RFC 3973 PIM Dense Mode (DM)
RFC 4541 IGMP and MLD snooping switches
RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): protocol specification (revised)
RFC 4604 Using IGMPv3 and MLDv2 for source-specific multicast
RFC 4607 Protocol Independent Multicast - Source- Specific Multicast (PIM-SSM)

Open Shortest Path First (OSPF)

OSPF link-local signaling
OSPF MD5 authentication
OSPF restart signaling
Out-of-band LSDB resync
RFC 1245 OSPF protocol analysis
RFC 1246 Experience with the OSPF protocol
RFC 1370 Applicability statement for OSPF
RFC 1765 OSPF database overflow
RFC 2328 OSPFv2
RFC 2370 OSPF opaque LSA option
RFC 2740 OSPFv3 for IPv6

RFC 3101 OSPF Not-So-Stubby Area (NSSA) option
RFC 3509 Alternative implementations of OSPF area border routers
RFC 3623 Graceful OSPF restart
RFC 3630 Traffic engineering extensions to OSPF
RFC 4552 Authentication/confidentiality for OSPFv3
RFC 5329 Traffic engineering extensions to OSPFv3

Qualité de Service (QoS)

IEEE 802.1p Priority tagging
RFC 2211 Specification of the controlled-load network element service
RFC 2474 DiffServ precedence for eight queues/port
RFC 2475 DiffServ architecture
RFC 2597 DiffServ Assured Forwarding (AF)
RFC 2697 A single-rate three-color marker
RFC 2698 A two-rate three-color marker
RFC 3246 DiffServ Expedited Forwarding (EF)

Résilience

IEEE 802.1D MAC bridges (STP)
IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
RFC 5798 Virtual Router Redundancy Protocol version 3 (VRRPv3) for IPv4 and IPv6

Routing Information Protocol (RIP)

RFC 1058 Routing Information Protocol (RIP)
RFC 2080 RIPng for IPv6
RFC 2081 RIPng protocol applicability statement
RFC 2082 RIP-2 MD5 authentication
RFC 2453 RIPv2

Securité

SSH remote login
SSLv2 and SSLv3
TACACS+ accounting and authentication
IEEE 802.1X authentication protocols (TLS, TTLS, PEAP and MD5)
IEEE 802.1X multi-suppllicant authentication
IEEE 802.1X port-based network access control
RFC 2818 HTTP over TLS ("HTTPS")
RFC 2865 RADIUS
RFC 2866 RADIUS accounting
RFC 2868 RADIUS attributes for tunnel protocol support
RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) profile
RFC 3546 Transport Layer Security (TLS) extensions
RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP)
RFC 3580 IEEE 802.1x RADIUS usage guidelines
RFC 3748 PPP Extensible Authentication Protocol (EAP)
RFC 4251 Secure Shell (SSHv2) protocol architecture
RFC 4252 Secure Shell (SSHv2) authentication protocol
RFC 4253 Secure Shell (SSHv2) transport layer protocol
RFC 4254 Secure Shell (SSHv2) connection protocol
RFC 5246 TLS v1.2

Services

RFC 854 Telnet protocol specification
RFC 855 Telnet option specifications

RFC 857 Telnet echo option
RFC 858 Telnet suppress go ahead option
RFC 1091 Telnet terminal-type option
RFC 1350 Trivial File Transfer Protocol (TFTP)
RFC 1985 SMTP service extension
RFC 2049 MIME
RFC 2131 DHCPv4 (server, relay and client)
RFC 2132 DHCP options and BootP vendor extensions
RFC 2616 Hypertext Transfer Protocol - HTTP/1.1
RFC 2821 Simple Mail Transfer Protocol (SMTP)
RFC 2822 Internet message format
RFC 3046 DHCP relay agent information option (DHCP option 82)
RFC 3315 DHCPv6 (server, relay and client)
RFC 3633 IPv6 prefix options for DHCPv6
RFC 3646 DNS configuration options for DHCPv6
RFC 3993 Subscriber-ID suboption for DHCP relay agent option
RFC 4330 Simple Network Time Protocol (SNTP) version 4
RFC 5905 Network Time Protocol (NTP) version 4

VLAN

Generic VLAN Registration Protocol (GVRP)
IEEE 802.1ad Provider bridges (VLAN stacking, Q-in-Q)
IEEE 802.1Q Virtual LAN (VLAN) bridges
IEEE 802.1v VLAN classification by protocol and port
IEEE 802.3ac VLAN tagging

Voix sur IP (VoIP)

LLDP-MED ANSI/TIA-1057
Voice VLAN

8. Références

Commutateur

AT-DC2552XS/L3 48 x slots SFP/SFP+, 4 slots QSFP+, 1-port console, 1-port de management (Eth 10/100/1000T), 2 slots pour alimentation, 2 slots pour ventilation
Livré sans alimentation et sans ventilation
Equerres de montage en bais 19' incluses

AT-PWR06-50 Alimentation 220VAC Hot-swappable

AT-FAN06 Module de ventilation Hot-swappable back to front (2 modules sont nécessaires pour un fonctionnement normal).

Equerres coulissante

AT-RKMT-SL01 Kit de montage en baie 19' coulissant

Modules 40G QSFP+

AT-QSFP1CU QSFP+copper cable 1 m
AT-QSFP3CU QSFP+ copper cable 3 m
AT-QSFPSR 40GSR 850 nm short-haul up to 150 m with MMF
AT-QSFPLR4 40GLR4 1310 nm medium-haul up to 10 km with SMF
AT-MTP12-1 MTP optical cable for AT-QSFPSR, 1 m
AT-MTP12-5 MTP optical cable for AT-QSFPSR, 5 m

Breakout Cables pour disposer de 4 connections 10G

AT-QSFP-4SFP10G-3CU QSFP to 4 x SFP+ breakout direct attach cable (3 m)
AT-QSFP-4SFP10G-5CU QSFP to 4 x SFP+ breakout direct attach cable (5 m)

10G SFP+ Modules

AT-SP10SR 10GSR 850 nm short-haul, 300 m with MMF
AT-SP10LRM 10GLRM 1310 nm short-haul, 220 m with MMF
AT-SP10LR 10GLR 1310 nm medium-haul, 10 km with SMF
AT-SP10ER40/I 10GER 1310nm long-haul, 40 km with SMF industrial temperature
AT-SP10TW1 10GBASE SFP+ direct attach cable (1 m)
AT-SP10TW3 10GBASE SFP+ direct attach cable (3 m)
AT-SP10TW7 10GBASE SFP+ direct attach cable (7 m)

1000Mbps SFP Modules

AT-SPTX 1000T 100 m copper
AT-SPSX 1000SX GbE multi-mode 850 nm fiber up to 550 m
AT-SPEX 1000X GbE multi-mode 1310 nm fiber up to 2 km
AT-SPLX10 1000LX GbE single-mode 1310 nm fiber up to 10 km

Licences optionnelles

Référence	Description	Fonctionnalités	Pile (Stack)
AT-FL-DC25-01	Premium License	OSPF ¹ BGP4 PIMv4-SM, DM and SSM RIPng OSPFv3 BGP4+ MLDv1 and v2 PIMv6-SM and SSM VRF lite (64 domains) RADIUS Full UDLD	Une licence par membre de la pile
AT-FL-DC25-AM20 AMF	Licence AMF	AMF Master pour réseau jusqu'à 20noeuds	Une licence par pile
AT-FL-DC25-AM40 AMF	Licence AMF	AMF Master pour réseau jusqu'à 40noeuds	Une licence par pile

¹ Sans licence Premium, le DC2552XS/L3 supporte 64 route OSPF

