



Présentation des commutateurs

AT-X210 et AT-X230

Commutateurs N3 Gigabit

Accès intelligent

Eco-Friendly

Versions POE + (X230)



Brique Technique AT-x210 et X230

Version 1.1

Février 2016

© 2015 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.	PRÉSENTATION	4
2.	ARCHITECTURE ET PERFORMANCES	4
3.	FONCTIONNALITÉS.....	5
4.	CARACTÉRISTIQUES PHYSIQUES GÉNÉRALES.....	15
5.	SPÉCIFICATIONS TECHNIQUES	17
6.	STANDARDS ET PROTOCOLES	19

1. Présentation

Les commutateurs d'accès AT-x200 sont des commutateurs Gigabit Ethernet de niveau 3 qui offrent un très grand nombre de fonctionnalités dans un design compact.

Grâce à leur puissance POE+, les X230 sont particulièrement adaptés pour alimenter les dispositifs à la périphérie du réseau, points d'accès sans fil, caméras de vidéosurveillance, téléphones IP.

Conçus avec une haute exigence environnementale, ils respectent pleinement la norme RoHS 6/6 Cette exigence s'applique également à la consommation électrique des produits. Le label  garantit ainsi une efficacité énergétique accrue, grâce à une optimisation des composants d'alimentation et une réduction de la consommation globale des équipements de la gamme.

Ils disposent par ailleurs d'une fonction « Eco-Switch » désactivant tout port non utilisé ainsi que l'affichage par LEDs en face avant de l'ensemble des ports.

2. Architecture et performances

Grâce à leur architecture non bloquante, les AT-x200 offrent des performances optimales quelque soit le volume de trafic traité. Les fonctionnalités de commutation de **niveau 3** 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-x230.

Référence	Matrice de commutation	Taux d'acheminement
AT-x210-9GT	24Gbps	13.4Mpps
AT-x210-24GT	48Gbps	35.7Mpps
AT-x230-10GP	20Gbps	14.9Mpps
AT-x230-28GP	56Gbps	41.7Mpps

Caractéristiques communes

- Fonctionnement en « Store and Forward »
- Capacité de la table MAC X210 : 8K
- Capacité de la table MAC X230 : 16K
- Jusqu'à 256 VLAN
- Groupes multicast L2 : 256 groupes supportés
- 256 Mo de mémoire vive SODIMM DDR ECC
- 64 Mo de mémoire flash
- Ports auto MDI/MDIX (port cuivre) et auto négociation
- Jumbo frame jusqu'à 10K
- Emplacement carte SD (modèles X230)

3. Fonctionnalités

Les commutateurs AT-x200 sont livrés avec le système d'exploitation AlliedWare Plus™, offrant ainsi une grande richesse fonctionnelle,

Systeme

AlliedWare Plus™ est un système d'exploitation temps réel avancé accessible via le port console, ou Telnet. L'administration peut également se faire de manière sécurisée en utilisant SSH. Plusieurs images de système d'exploitation peuvent être stockées en mémoire flash. Le fichier de configuration est éditable et plusieurs fichiers peuvent être présents sur le commutateur. Les transferts de fichier peuvent se faire par TFTP ou de manière sécurisée par SCP ou SFTP.

La syntaxe de l'interface en ligne de commandes est conforme au standard de l'industrie.

```
awplus>enable
awplus#configure terminal
awplus(config)#vlan database
awplus(config-vlan)#vlan 2
awplus(config-vlan)#exit

awplus(config)#interface port1.0.1-port1.0.4
awplus(config-if)#switchport mode access
awplus(config-if)#switchport access vlan 2

awplus(config)#interface vlan2
awplus(config-if)#ip address 192.168.1.1/24
awplus(config-if)#exit
```

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.

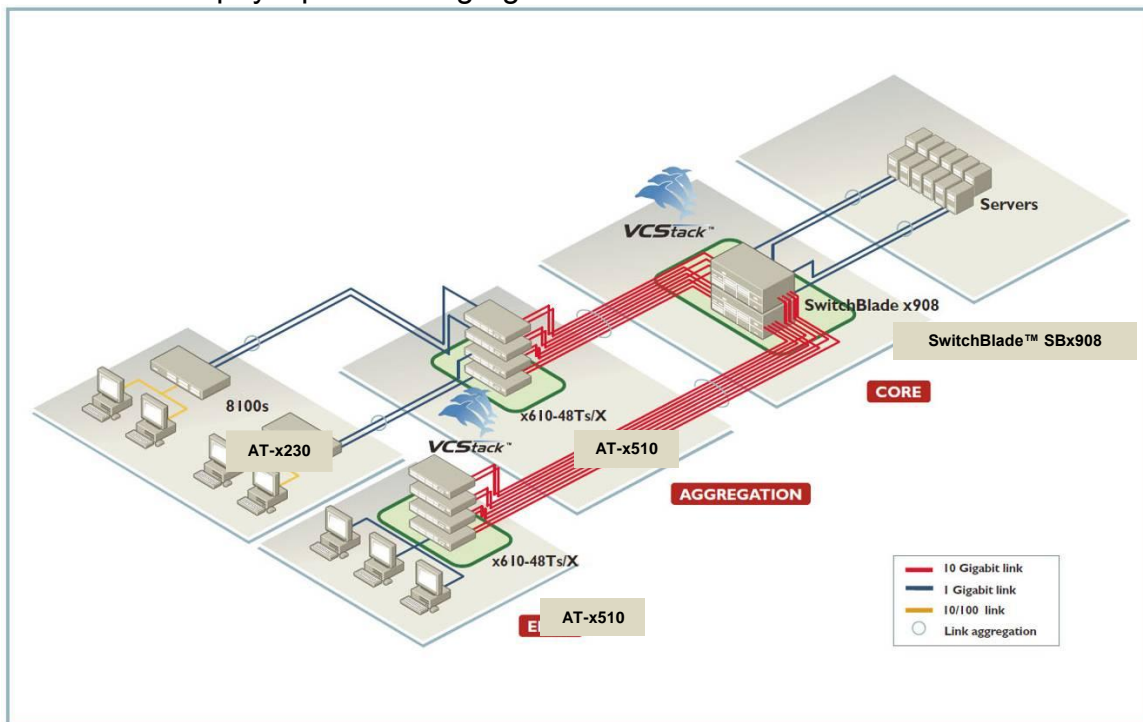
Les tailles maximum de trames admissibles lorsque la fonction Jumbo Frame est activée sont les suivantes :

- 9714 Octets

Agrégation de liens 802.3ad (LACP)

- Jusqu'à 8 agrégats de 8 ports
- Reprise sur incident et répartition de charge automatiques

8 agrégats contenant jusqu'à 8 ports peuvent être configurés sur un commutateur AT-x200. L'agrégation de liens peut être de type statique ou s'appuyer sur le protocole LACP (Link Aggregation Control Protocol). La répartition de charge est automatique sur les différents liens physiques d'un agrégat.



Virtual Local Area Network (VLAN)

Les commutateurs AT-x200 permettent la création de 256 VLANs parmi 4096 selon les critères suivants :

- VLAN par port
- VLAN par protocole
- VLAN par Subnet IP

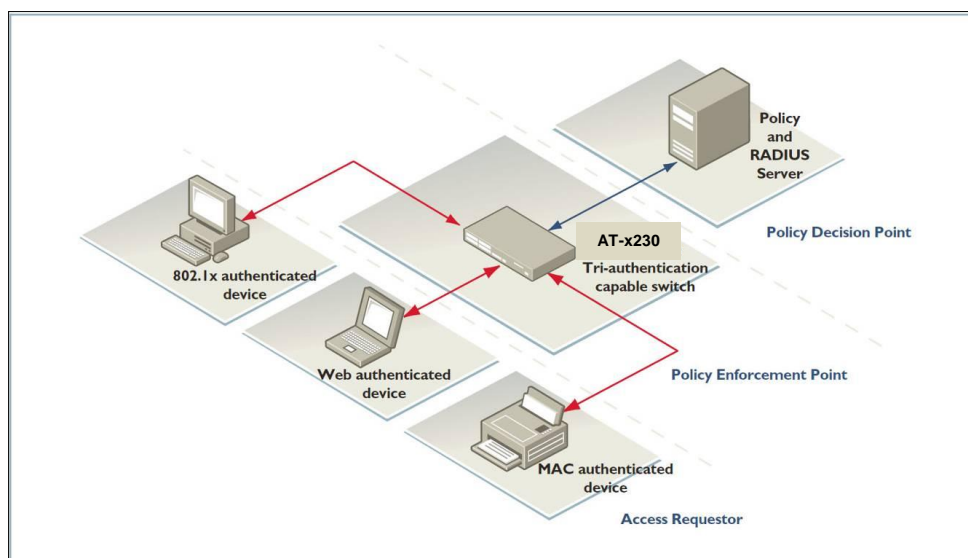
Les VLANs peuvent être définis de manière statique sur les critères mentionnés ci-dessus, et de manière dynamique par le biais du protocole GVRP. L'identifiant des VLANs peut être transporté selon le standard 802.1Q.

La fonction Private VLAN permet de créer des VLANs 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.

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
- Assignation dynamique de VLAN
- Multiple assignation 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 ne 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-x200 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).

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-x200 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.

EPSR (Ethernet Protection Switching Ring)

- Reprise sur incident en 50 ms
- Impact négligeable quel que soit l'application
- (Voix, Données, Images)



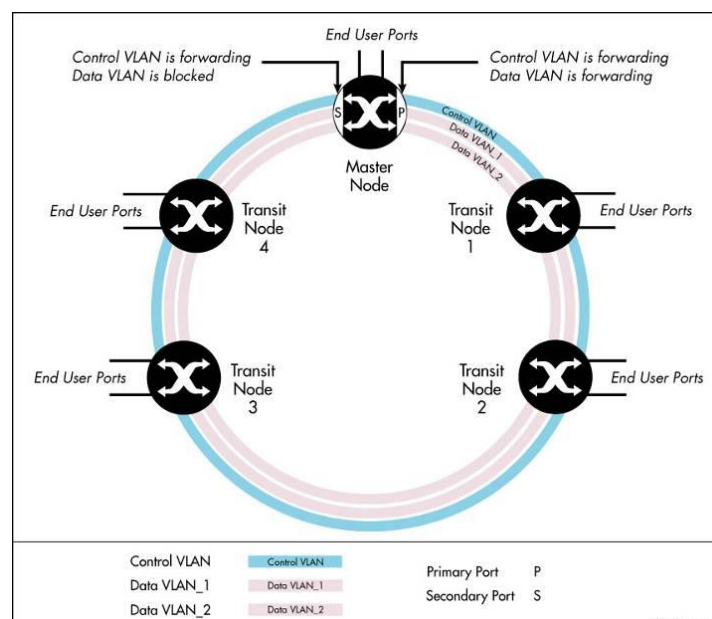
Les commutateurs AT-x200 intègrent la fonctionnalité EPSR Transit en standard qui permet de réaliser des anneaux Gigabit ou 10 Gigabit Ethernet offrant un temps de convergence de l'ordre de 50 ms. Pour pouvoir être utilisés dans un anneau EPSR, un équipement EPSR Master doit être présent dans l'anneau. Il est donc impératif d'avoir dans l'anneau au minimum un équipement des familles suivantes : AT-9900, AT-x600, AT-x610, AT-x900, AT-SBx908, AT-SBx930, AT-SBx8100 ou alors un AT-x510 muni de la licence Premium (AT-x510-FL01).

Cette technologie permet une reprise sur incident transparente pour l'utilisateur quel que soit la nature de l'application (téléphonie, vidéo, télévision...)

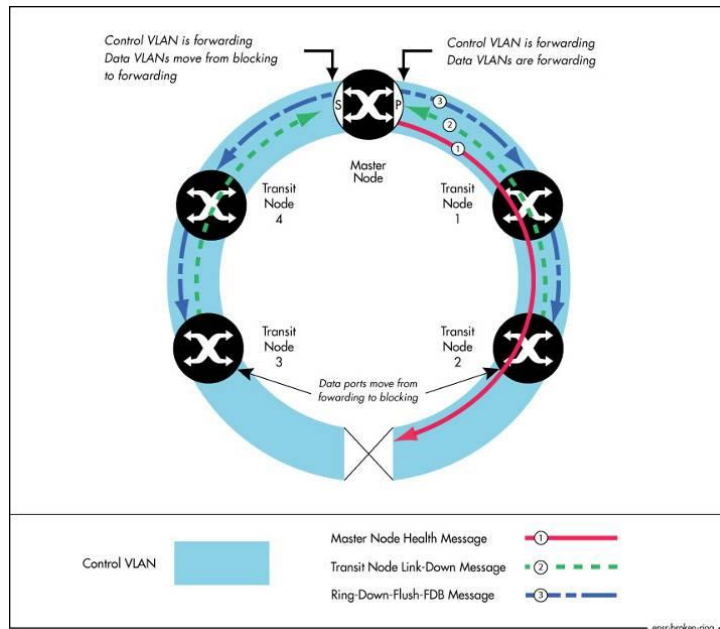
EPSR utilise les éléments suivants :

- Un VLAN de contrôle pour la signalisation
- Un ou plusieurs VLANs de données
- Un Nœud Maître (Master Node)
- Des Nœuds de Transit (Transit Node)

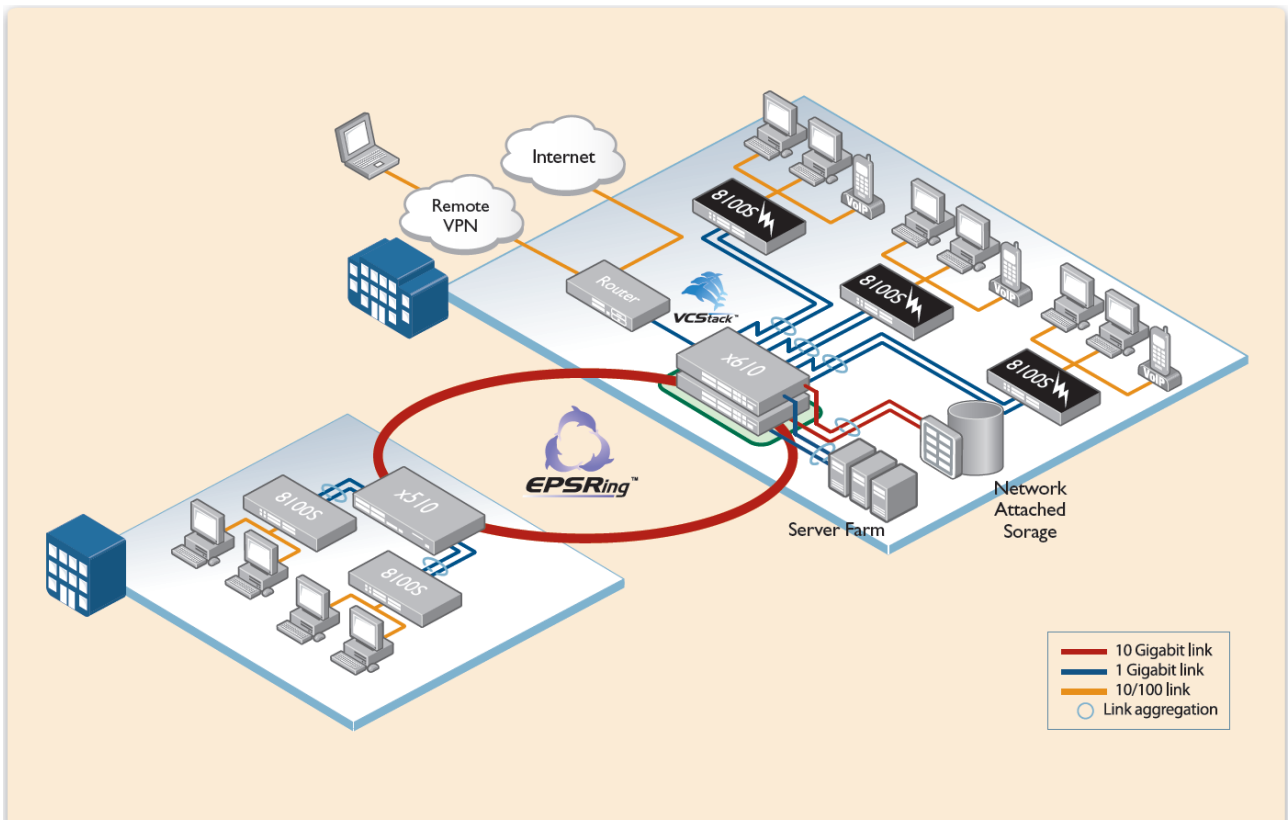
En fonctionnement normal, le Master envoie de manière périodique dans le VLAN de contrôle des « Health Check ». Le port primaire (Primary) envoie et reçoit les flux de tous les VLANs (contrôle & données). Le port secondaire (Secondary) bloque le trafic des VLAN de données et reçoit les informations du VLAN de contrôle.



En cas de rupture d'un des liens, les nœuds de transit les plus proches détectent la coupure et envoient l'information « Link Down » vers le Master. A la réception du « link Down », le Master ouvre le port secondaire (Secondary) pour les VLANs de données et réinitialise la table d'adresses MAC. L'information « ring down » est répercutée aux nœuds de Transit. Ce processus est réalisé dans un délai d'inférieur à 50ms



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.



Autodétection 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-x200 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...).

IPv6

Allied Telesis est Aujourd'hui l'un des constructeurs du marché qui possède le niveau d'implémentation IPv6 le plus avancé.

Le plan de contrôle IPv6 (Gestion du module d'administration en IPv6) est fourni de Base à partir de la Version 5.4.3

IGMP Snooping et IGMP

Les commutateurs AT-x200 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- x200

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.

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 1, 2, 3 et 4.

Les ACL sont également utilisées avec les fonctions suivantes :

- Mirroring : il est possible de recopier spécifiquement un type de flux quel que soit son port d'entrée.

Gestion de qualité de service (QoS)

La classification de trafic peut se faire sur des combinaisons de critères présents au niveau 1, 2, 3 et 4. Les signalisations 802.1p, DSCP (Diffserv) et TOS sont supportés tant en lecture qu'en marquage. Le module de Policing permet de garantir une bande passante minimum par type de flux. Cette garantie peut être fixée avec une grande finesse par pas de 1 Kbps. En utilisant cette fonction, l'utilisation de la bande passante est automatique adaptée selon les conditions de congestion rencontrées en tenant compte des spécifications configurées. Il est également possible de fixer, par flux, une limite maximum d'utilisation de bande passante, l'excédant de trafic pouvant alors être traité et marqué à un niveau de priorité moindre ou rejeté selon le souhait de l'administrateur.

- Classification de trafic à vitesse filaire
- 8 niveaux de priorité
- 8 files d'attente
- Politiques de QoS avancées
- Contrôle de bande passante minimum/maximum par flux, par pas de 1 Kbps
- Limitation de bande passante en sortie sur chaque port
- Contrôle du rejet de paquets par marquage 2 couleurs (vert, 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)

Pour les environnements complexes, il est possible de mixer les modes de vidage des huit files d'attente par port. Par exemple, les trafics très sensibles au temps de latence et à la gigue peuvent être envoyés dans une file d'attente courte qui sera servie de manière prioritaire. Les autres trafics peuvent être dirigés vers des files plus longues sur lesquelles s'opère un cycle, le nombre de trames émises par cycle étant configurable par file d'attente.

Gestion des évènements (Trigger)

Ce module logiciel permet d'appeler des scripts à des moments donnés (Date et heure fixe ...) ou sur analyse de l'état du commutateur. Ce module permet par exemple de modifier dynamiquement la configuration du commutateur lorsqu'une interface change d'état. De nombreux évènements peuvent être surveillés par le biais de ce module. Ainsi, il est possible de configurer le commutateur de telle manière qu'il prenne automatiquement des mesures lorsqu'un évènement indésirable survient.

Administration et supervision

Outre les versions 1 et 2c, la version 3 de SNMP est supportée par AlliedWare Plus. 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. Une interface Web de configuration et de monitoring est également disponible par HTTP/Java.

The screenshot displays the Allied Telesis web management interface. The main window is titled "Allied Telesis" and features a navigation menu with tabs for "System", "Switching", "IP", "Resiliency and High Availability", and "Management". Below the menu, there are sub-tabs for "Status", "Identity", "Environment Monitoring", "File Management", "Stacking", and "License Management". The "Environment Monitoring" tab is active, showing various system metrics:

- Chassis:** Voltage (2.5V, 3.01V, 3.30V), Voltage: 5V, Voltage: 12V, Voltage: 1.25V.
- Temperature:** Temp: CPU (41 C), Temp: PSU Bay (31 C), Temp: PSU (30 C), Temp: Ambient.
- Fan:** Fan: Sys Fan 1 (5819 rpm), Fan: Sys Fan 2 (4692 rpm), Fan: PSU Fan 1 (6818 rpm), Fan: PSU Fan 2.
- PSU:** PSU Power Output.
- Sensors:** No XEM Modules.

On the right side, there is a "Management" panel with tabs for "Management", "Stacking", and "License Management". Below these tabs is a network diagram showing 24 ports (1-24) and a status legend for "SB", "STACK", "MSTR", "L1", "L2", "PRE", "CONSOLE", "STATUS", "FAULT", "OMISTER", "ERR", "ERR", "ERR".

In the foreground, a login dialog box is open, titled "Allied Telesis". It contains fields for "Username" and "Password", along with "OK" and "Clear" buttons. The dialog also features the Allied Telesis logo and the text "AlliedWare Plus™ OPERATING SYSTEM" and "© 2008-2011 Allied Telesis K.K.".

At the bottom right of the main interface, there are two graphs: "CPU Used %" and "Memory Free %", both showing a scale from 0 to 100. Below these graphs is a button labeled "Top Ten Utilised Ports".

Allied Telesis Management Framework

Allied Telesis Management Framework (AMF) est une suite d'outils, apportant une approche simplifiée de la gestion du réseau. La plupart des tâches courantes d'administration peuvent être automatisées, ou effectués simplement via AMF, ce qui permet d'optimiser l'emploi du temps des ressources informatiques.



AMF apporte les fonctionnalités suivantes :

- Gestion centralisée des équipements
- Sauvegarde automatique des configurations
- Mise à jour automatique des équipements
- Configuration automatique des équipements
- Re configuration automatique des équipements en cas de remplacement

Ces fonctionnalités puissantes permettent une administration basée sur les principes « plug and play » et « zero touch »

Les commutateurs de la série x200 nécessitent qu'un nœud « maitre » (au minimum un X510) soit présent dans l'architecture pour bénéficier des fonctionnalités AMF.

4. Caractéristiques physiques générales

Référence	Désignation
AT-x210-9GT	8 ports 10/100/1000T, 1 Emplacement SFP
AT-x210-24GT	24 ports 10/100/1000T, 4 Emplacements SFP Combo
AT-x230-10GP	8 ports 10/100/1000T POE+, 2 Emplacements SFP
AT-x230-28GP	24 ports 10/100/1000T POE+, 4 Emplacements SFP

AT-x210-9GT

Le commutateur AT-x210-9GT offre 8 ports 10/100/1000 RJ45 et un emplacement SFP. L'absence de ventilateur garantit au commutateur AT-x210-9GT un parfait silence de fonctionnement



AT-x210-24GT

Le commutateur AT-x210-24GT offre 24 ports 10/100/1000 RJ45 dont quatre emplacements SFP combo. L'absence de ventilateur garantit au commutateur AT-x210-24GT un parfait silence de fonctionnement



AT-x230-10GP

Le commutateur AT-x230-10GP offre 8 ports 10/100/1000 RJ45 et 2 emplacements SFP. Un emplacement pour carte mémoire de type SD-Card et un port console au format RJ-45 sont également présents. Un budget **POE+** de 120W est disponible



AT-x230-28GP

Le commutateur AT-x230-28GP offre 24 ports 10/100/1000 RJ45 et 4 emplacements SFP. Un emplacement pour carte mémoire de type SD-Card et un port console au format RJ-45 sont également présents. Un budget **POE+** de 370W est disponible



Power over Ethernet (POE) de dernière génération

- Les AT-x230 sont conformes au standard PoE+ IEEE 802.3at, rétro compatible avec tout équipement PoE 802.3af.
- AT-x230-10GP: supporte jusqu'à 8 équipements terminaux POE de classe 3 (15,4 W maximum par port), ou jusqu'à 4 équipements terminaux POE+ de classe 4 (30W maximum par port)
- AT-x230-28GP: supporte jusqu'à 24 équipements terminaux POE de classe 3 (15,4 W maximum par port), ou jusqu'à 12 équipements terminaux POE+ de classe 4 (30W maximum par port)

Modules SFP supportés



Les emplacements SFP permettent de disposer des possibilités suivantes selon le module utilisé :

- 100Base-FX sur fibre optique multimode (AT-SPFX/2)
- 100Base-FX sur fibre optique monomode, 15 km (AT-SPFX/15)
- 1000Base-SX (AT-SPSX)
- 1000Base-EX jusqu'à 2 Km sur fibre multimode (AT-SPEX)
- 10KM 1000Base-LX (AT-SPLX10)
- 40KM 1000Base-LX (AT-SPLX40)
- 80KM 1000Base-ZX (AT-SPZX80)
- 100 Mbs sur 1 brin sur 10 Km mono mode (AT-SPFXBD-LC-13 (AT-SPFXBD-LC-15 à utiliser par paire
- 1000 Mbs sur 1 brin sur 10 Km mono mode (AT-SPBD10-13 et AT-SPBD10-14 à utiliser par paire)
- 1000Base-T sur cuivre RJ-45 (AT-SPTX)

5. Spécifications techniques

Dimensions (H x L x P) :

Modèle AT-x210-9GT

- 3,8 cm x 26.3 cm x 17.9 cm

Modèle AT-x210-24GT

- 4.4 cm x 44 cm x 21 cm

Modèle AT-x230-10GP

- 4.25 cm x 21 cm x 27.5 cm

Modèle AT-x230-28GP

- 4.4 cm x 44 cm x 29 cm

Poids :

- X210-9GT : 1.4Kg
- X210-24GT : 2.7Kg
- X230-10GP : 2.1Kg
- X230-28GP : 4.7Kg

Température de fonctionnement :

- X210-9GT : 0°C à 50°C
- X210-24GT : 0°C à 40°C
- X230-10GP : 0°C à 50°C
- X230-28GP : 0°C à 50°C

Température de stockage :

-25° C à 70° C

Humidité :

5% à 90% sans condensation

Altitude de fonctionnement :

Jusqu'à 3000 m

Tension d'alimentation:

100 - 240 VAC 2A

Fréquence :

47/63 Hz

Consommation électrique (hors PoE) :

- X210-9GT : 12 W
- X210-24GT : 28 W
- X230-10GP : 16 W
- X230-28GP : 37 W

Nuisance sonore x210 : 0 dB
Nuisance sonore x230 : 33-42 dBa

Conformités

Electrical Approvals & Compliances	EMC, EN55022 class A, FCC class A, VCCI class A
Immunité	EN55024, EN61000-3-2/3
Sécurité	UL60950-1, CAN/CSA-C22.2 No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS 60950
Certification	UL, cUL, TUV
Pays d'origine	Chine

6. 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

Encryption

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 802.3af Power over Ethernet (PoE)
IEEE 802.3at Power over Ethernet plus (PoE+)
IEEE 802.3az Energy Efficient Ethernet (EEE)
IEEE 802.3u 100BASE-X
IEEE 802.3x Flow control - full-duplex operation
IEEE 802.3z 1000BASE-X

General Routing

RFC 791 Internet Protocol (IP)
RFC 792 Internet Control Message Protocol (ICMP)
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 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 1812 Requirements for IPv4 routers
RFC 1918 IP addressing

IPv6 Features

RFC 1981 Path MTU discovery for IPv6
RFC 2460 IPv6 specification
RFC 2464 Transmission of IPv6 packets over Ethernet networks
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

Management

AMF MIB and SNMP traps

AT Enterprise MIB

Optical DDM 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 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 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 3621 Power over Ethernet (PoE) MIB

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

Multicast Support

IGMP query solicitation
IGMP snooping
MLD snooping (v1 and v2)
RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
RFC 3376 IGMPv3

Quality of Service

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)

Resiliency Features

IEEE 802.1D MAC bridges
IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)

Security Features

SSH remote login
SSLv2 and SSLv3
TACACS+ accounting and authentication
IEEE 802.1X authentication protocols (TLS, TTLS, PEAP, MD5)
IEEE 802.1X multi-suplicant 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 client
- RFC 2616 Hypertext Transfer Protocol - HTTP/1.1
- RFC 2821 Simple Mail Transfer Protocol (SMTP)
- RFC 2822 Internet message format
- RFC 3315 DHCPv6 client
- RFC 4330 Simple Network Time Protocol (SNTP) version 4
- RFC 5905 Network Time Protocol (NTP) version 4

User Interface Features

- Event-based triggers
- Graphical User Interface (GUI)
- Industry-standard CLI with built-in Help
- Powerful CLI scripting tool

VLAN Support

- Generic VLAN Registration Protocol (GVRP)
- IEEE 802.1Q - 2005 Virtual LAN (VLAN) bridges
- IEEE 802.1v VLAN classification by protocol and port
- IEEE 802.3ac VLAN tagging

VoIP Support

- LLDP-MED ANSI/TIA-1057
- Voice VLAN