

# Support de formation



# Modules

Le support de formation IntraVUE est scindé en plusieurs modules permettant de traiter tout ou partie des sujets selon le profil des utilisateurs.

## Table des Matières

Module 1 : Les Fondamentaux Ethernet.....	5
Modèle OSI	5
Le protocole SNMP	6
Hubs / Commutateurs Niv 2 / Commutateurs Niv 3	7
Routage Niveau 2 / Niveau 3	8
Module 2 : Descriptif Produit .....	9
Composants Logiciel	9
Pré requis Technique (SNMP)	11
Module 3 : Installation / Configuration Initiale .....	12
Configuration Minimale	12
Options d'installations	12
Configuration Initiale	13
Les 6 vues d'IntraVUE	17
Comptes utilisateurs	18
Ecran principal	19
Module : Mode Opérateur.....	21
Menu « Equipement »	22
Icônes	23
Images miniatures	24
Utilisation des couleurs	25
Equipements mobiles	27
Fonctions de survol	28
Propriétés des équipements	29
Seuils sur les liens	30
Graphique Multi-équipements	33
Fenêtre d'événements	38
Recherche	42
Données SNMP	44



Module : Mode Administrateur .....	45
Connexion normale	46
Changement du mot de passe administrateur	46
Ajoutez un utilisateur et un mot de passe à IntraVUE	47
Configuration des équipements	48
Configuration Système	49
Configuration Système - Onglet General	49
Configuration Système - Onglet Database	50
Configuration Système - Onglet Threshold	52
Configuration Système - Onglet Scanner	53
Les VLAN - Virtual Local Area Networks	57
Sélectionner le Top Parent	58
Qu'est-ce qu'un Top Parent?	58
Configuration Système - Onglet Email	60
Import / Export	64
Configuration des équipements	67
Configuration des équipements - Onglet General	67
Vérification Administrateur	70
Configuration des équipements - Onglet View Names	71
Configuration des équipements - Onglet Images	72
Configuration des équipements - Onglet Web Links	74
Déplacement Manuel	76
Module : Mode Avancé .....	82
Description répertoire IntraVUE	82
Sauvegarder des fichiers ne se trouvant pas dans la base de données MySQL.	83
Fichiers de configuration avancés	84
Module : Intégration SCADA.....	93
Intégration de la partie Graphique d'Intravue.	93
Établissement une communication entre Intravue et le SCADA	97
Module : Outils Complémentaires .....	102
Aide en Ligne	102
Forum	102
Vidéos	102

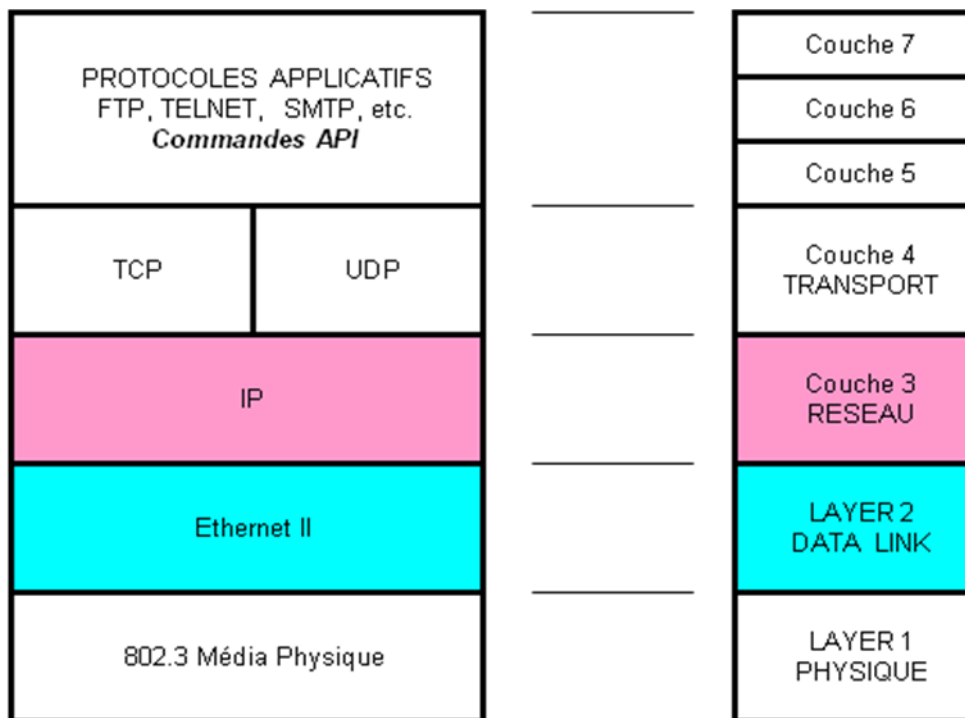


# Module 1 : Les Fondamentaux Ethernet

## Modèle OSI

Couche 2  
Couche 3

Utilise les adresses MAC pour le routage  
Utilise les adresses IP pour le routage



Une adresse MAC est censée être un identifiant unique comme peu l'être une empreinte digital.  
Une adresse IP est un identifiant modifiable comme peut l'être un numéro de téléphone.

## Le protocole SNMP

Il existe deux types de switches :

- Manageable
- Non-Manageable

Les deux types de Switch peuvent fournir les mêmes fonctionnalités, cependant les Switch manageables proposent un protocole commun de communication qui peut être accessible à travers le réseau.

Ce protocole se nomme SNMP (Simple Network Management Protocol).

Les données sont collectées dans des espaces mémoires appelées MIB (Management Information Base)

On peut différencier 3 types de MIB :

- Zone de données standardisée – MIB publique
- Données constructeurs additionnelles – MIB privée
- Données sur le routage des paquets – Bridge MIB

Ces MIB permettent d'accéder à différentes informations mises à disposition par l'équipement en fournissant l'OID (Objet Identification) de ces informations. L'OID peut être vu comme étant l'adresse de l'information dans l'équipement.

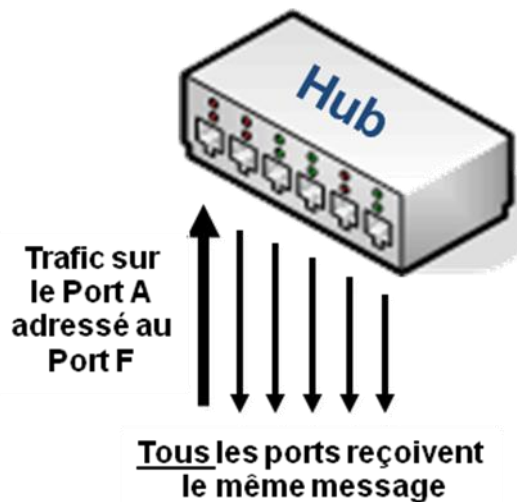
L'OID se présente sous la forme suivante : 1.2.3.12.1.3.8.1.2

Les équipements manageable peuvent également diffuser des TRAP MESSAGE (messages d'alarme) à destination du serveur de TRAP. L'adresse du serveur de TRAP est généralement paramétrable dans l'équipement. Ces TRAP MESSAGE contiennent habituellement l'OID qui est à l'origine du message.

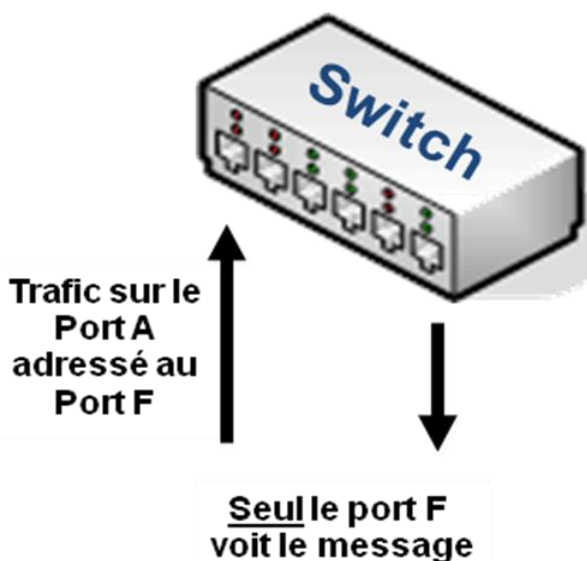
## Hubs / Commutateurs Niv 2 / Commutateurs Niv 3

La plupart des switches utilisés dans les LAN (Local Area Network) utilisent uniquement les adresses MAC afin de router les messages. Lorsque vous avez de multiples réseaux, un routeur ou un Switch de couche 3 est utilisé afin de connecté différents réseaux indépendant pour ne former qu'un important WAN.

Les adresses MAC qui sont considérées comme unique sont apparues dupliquées sur des réseaux industriels. Exemple : le constructeur commercialise tous ses équipements avec la même adresse MAC et demande à l'utilisateur de la modifier. Plusieurs systèmes de redondance préconisent une adresse MAC identique (spoofing). Cela fonctionne avec des Hubs mais dès lors que vous remplacez vos équipements par des switches, cela génère de graves dysfonctionnements. Les duplications d'adresses MAC sont difficilement détectables sans IntraVue.

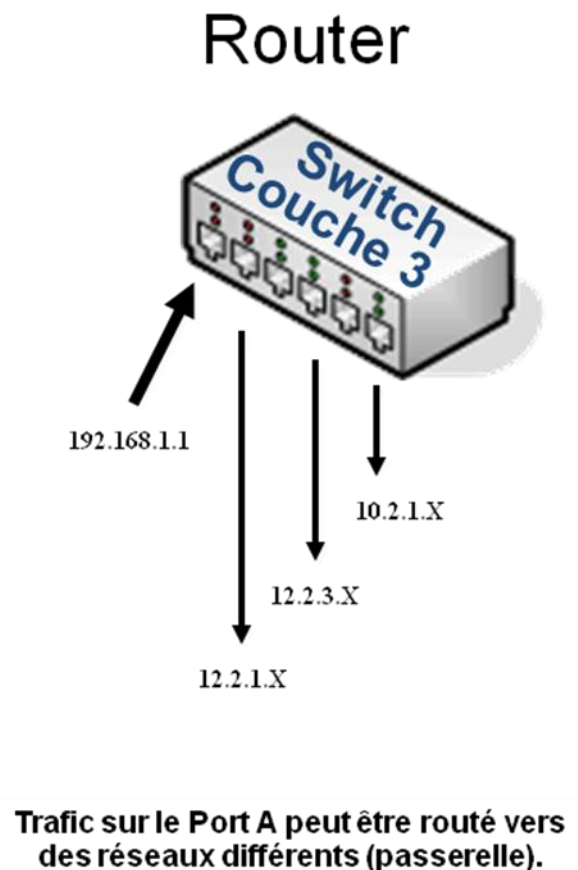
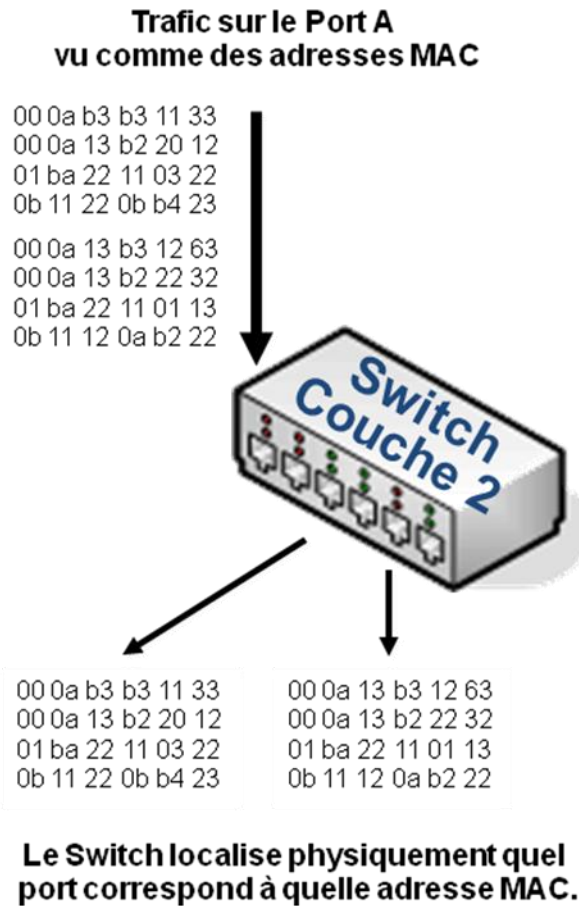


Un Hub effectue uniquement une connexion physique entre les équipements et ceci sans aucune isolement des domaines de collisions.



Un Switch regarde à l'intérieur de la trame et détermine le destinataire. Il interprète le port sur lequel l'adresse MAC est présente. Ceci permet donc de créer plusieurs domaines de collisions et de les isoler

## Routage Niveau 2 / Niveau 3

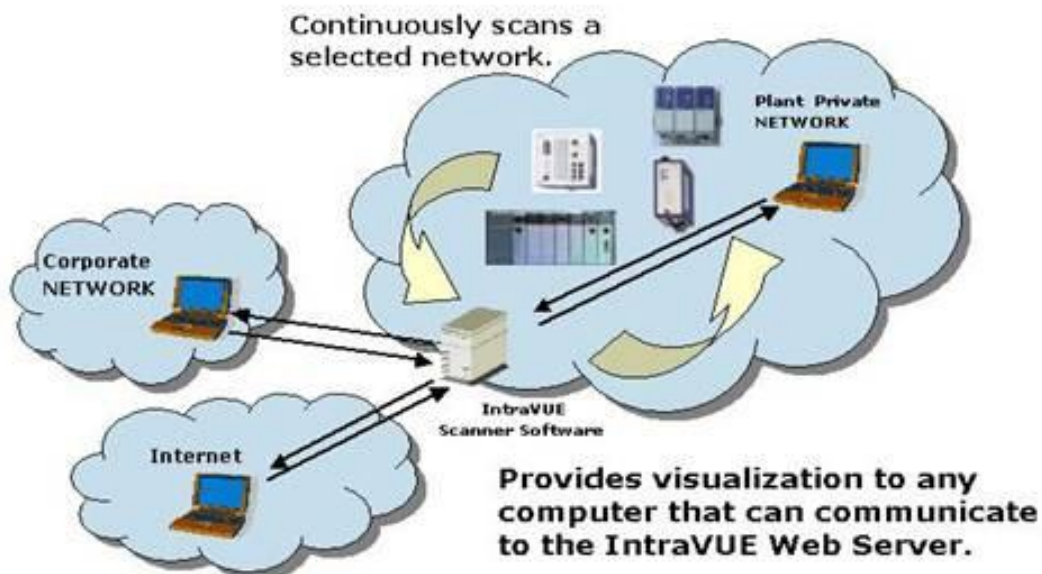


## Module 2 : Descriptif Produit

### Composants Logiciel

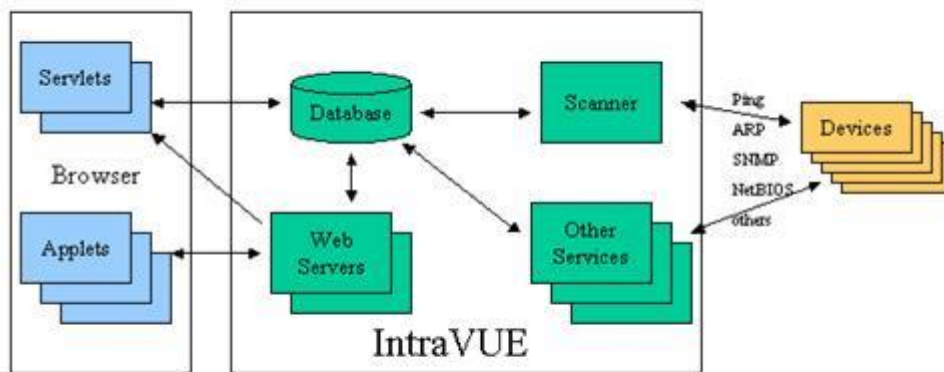
IntraVUE est un outil de visualisation et de contrôle de réseau locaux IP conçu particulièrement pour répondre aux besoins des industriels. Installé comme une application Web, la plupart des ordinateurs sont capables de voir l'état de tout dispositif du réseau.

IntraVUE est une solution de monitoring fournissant à l'utilisateur de précieuses informations sur la performance et les changements qui se produisent sur le réseau.



IntraVUE scanne en permanence le réseau afin de détecter si de nouveaux périphériques se connectent ou si des périphériques actuellement en place sont déconnectés ou déplacés. Cette fonctionnalité dynamique est facilitée par l'utilisation de switches et de routeurs managés dans le réseau concerné.

IntraVUE est constitué de plusieurs composants :



- **Scanner Réseau** : Contrôle en permanence le réseau concerné en surveillant les déconnexions d'équipements, la connexion de nouveaux équipements ainsi que les bandes passantes. Toutes ces informations proviennent des MIB SNMP. Le scanner utilise Ping et ARP pour détecter la présence des équipements et SNMP pour hiérarchiser le réseau. Ces informations sont stockées dans une base de données.
- **Base de données relationnelle** : Base de données MySQL. Cette zone contient à la fois les informations fournies par le scanner, les données configurées par l'administrateur et les événements.
- **Serveur Web** : Serveur Apache Tomcat. Ce serveur sert de support aux servlets et applets d'IntraVUE.
- **Interface Homme-Machine Java** : Le navigateur utilise une méthode de visualisation hyperbolique qui permet à un réseau très complexe d'apparaître sur un seul écran. Cette visualisation est intégrée dans un applet Java mis à disposition aux clients. Cet applet est mis à jour périodiquement afin de fournir l'information la plus récente possible aux navigateurs clients.

IntraVUE est composé également de composants supplémentaires qui peuvent être installés.

- **Auto-IP** est un serveur BootP amélioré qui travaille en parallèle avec IntraVUE. Auto-IP est décrit dans la partie G de ce manuel. Il est installé en mode démo s'il n'est pas enregistré.

## Pré requis Technique (SNMP)

IntraVUE est un outil de contrôle de réseau LAN mais pas un outil de contrôle de réseau WAN.

« *Scanne localement, visualise à distance* » est la règle principale.



**L'hôte IntraVUE doit toujours être connecté à un Switch manageable**

IntraVue doit être placé à proximité des dispositifs à contrôler, ensuite les utilisateurs regardent à distance pour voir les événements qui se passent.

Dans la mise en place de dispositifs locaux, l'hôte IntraVue doit être connecté au switch le plus proche du routeur menant à d'autres sous réseaux.

Un exemple extrême serait une société qui a plusieurs sites distants avec des périphériques Ethernet à surveiller

- Meilleur des cas : Il doit y avoir un hôte IntraVue installé sur chaque site distant. Un poste IntraVue de supervision permettra de voir tous les sites distants comme un seul.
- Cas intermédiaire : Il doit y avoir un hôte IntraVue installé sur chaque site distant. Chaque site distant peut être contrôlé individuellement.
- Pire des cas : Un seul hôte IntraVue contrôle toute l'architecture. Les sites distants sont contrôlés au travers de firewall, routeurs, VPN...

# Module 3 : Installation / Configuration Initiale

## Configuration Minimale

IntraVUE 2 a été conçu pour s'exécuter sur un ordinateur de faible puissance. Au moins 512 Mo de mémoire vive sont nécessaire et 1024 Mo idéalement.

IntraVUE a été testé sur Windows 2000, Windows XP Professional SP2, Windows Server 2000 et 2003. A priori aucun problème avec Windows Vista même si cela n'a pas été testé.

Lors de l'installation d'IntraVUE sur un système d'exploitation Serveur, il est indispensable de passer par la fonction Ajout/Suppression de programmes du panneau de configuration.

Le dossier C:\MySQL doit être exclu des sauvegardes et de l'analyse des virus faire par des programmes de contrôle. Ces programmes de verrouillent l'accès aux fichiers et cause l'arrêt du service MySQL s'il ne peut pas accéder à certains fichiers pendant plus de quelques secondes.

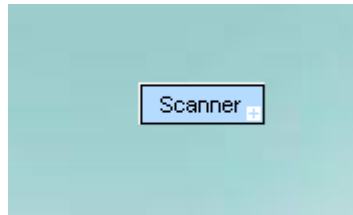


Si cela se produit, le redémarrage du service MySQL fonctionne toujours, mais il n'y aura pas de données recueillies par IntraVUE si MySQL est arrêté.

## Options d'installations

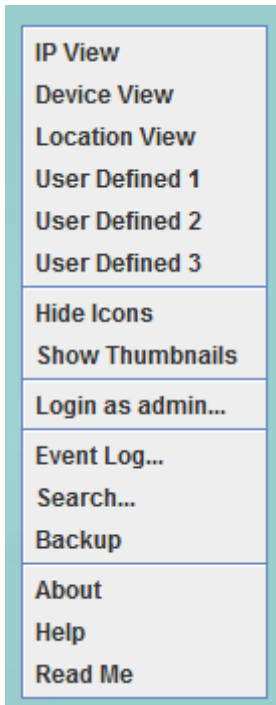
Lorsque vous faite une installation sur Windows Vista choisissez toujours un dossier d'installation HORS de « Program Files » pour ne pas avoir problèmes liés à la sécurité de lecture des fichiers. Nous recommandons un dossier, tels que C:\IntraVUE.

## Configuration Initiale



La première tâche à accomplir après l'installation d'IntraVUE est de préciser les adresses IP que vous voulez contrôler.

Un clic droit sur le fond du navigateur vous permet d'accéder au menu de configuration du système.



Vous avez alors la possibilité de vous connecter en administrateur en sélectionnant « Login as admin... » (Voir chapitre Connexion Administrateur).

Le menu contextuel du clic droit passe alors en « mode admin ». Il est alors possible d'entrer dans la configuration du système. « System configuration... »

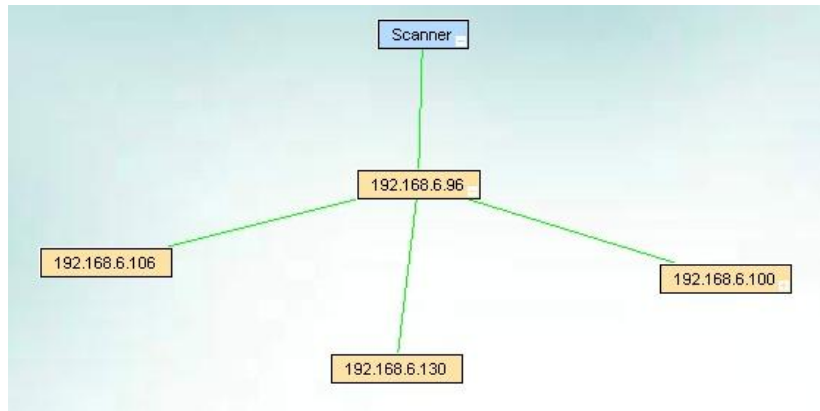
Dans l'onglet « Scanner », le bouton « Add » de la section « Networks » permet d'ajouter un nouveau réseau à contrôler. Sélectionnez ou entrez l'adresse IP de l'ordinateur sur lequel IntraVUE est installé puis la plage d'adresses IP à surveiller.

L'ordinateur « **Top parent** » est le dispositif qui **contient toutes les adresses MAC** des dispositifs que vous désirez contrôler. Regardez le chapitre Onglet Scanner pour plus de détails.

Pour valider la configuration sélectionnez « Apply & Close ».

Lorsque de nouveaux équipements sont découverts par IntraVUE, il peut se passer quelques minutes avant que la topologie du réseau soit mise à jour. Cette durée dépend notamment du nombre d'adresses IP totales couvertes par les plages d'adresse IP.

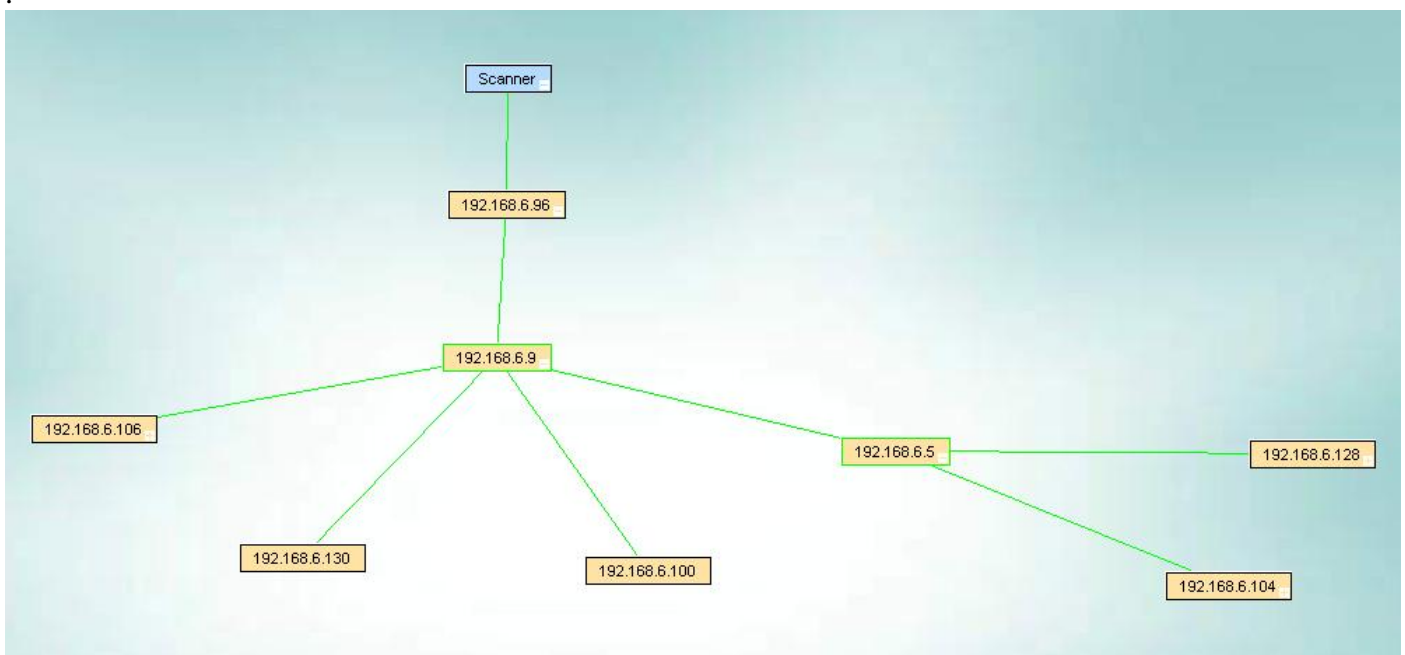
IntraVUE va afficher tous les nouveaux équipements nouvellement découverts sous le nœud du « Top parent»



Dès qu'un équipement répond au Ping, il est placé sous le nœud du « Top Parent ». IntraVUE va chercher les adresses MAC à partir du « Top Parent » et de chaque routeur local.

Une fois l'adresse MAC déterminée, IntraVUE tente de trouver le bon endroit où situer l'équipement dans la hiérarchie du réseau.

Pour tracer la topologie, IntraVue accède aux données SNMP des routeurs et des switches manageables, la topologie se dessine automatiquement en établissant des relations Parents-enfants. Un parent est un équipement qui possède d'autres équipements/nœuds connectés sous lui-même.



**IntraVUE récupère les informations par des requêtes SNMP.**

Si la communauté SNMP configurée dans les équipements (ou par défaut) n'est pas correcte alors IntraVUE sera incapable de déterminer la topologie du réseau.

Il y a cependant des cas où l'utilisation d'équipements non manageable est possible. Par exemple, si le scanner d'IntraVUE découvre deux ou plus équipement connectés au même port d'un équipement manageable, alors IntraVUE va automatiquement insérer un nœud.

Par défaut ce nœud s'appelle « Auto Inserted Node » mais il est possible de personnaliser cet équipement par la suite.

Il est également possible de déplacer manuellement un équipement et même d'en créer un nouveau.



Consultez le chapitre Déplacement Manuels.

- Un bon exemple de cela est d'ajouter un équipement sous un convertisseur Série – Ethernet : un « enfant » pour chaque équipement série derrière le convertisseur.
- Ou un automate série

Cette fonctionnalité vous permet de ne pas voir uniquement les équipements IP mais tous les équipements connectés.

Si la communauté SNMP est inconnue ou incorrecte alors IntraVUE va découvrir l'équipement et le placer sous un nœud "Auto Inserted Node"

Lorsque la communauté est correcte, IntraVUE va déplacer l'équipement et le placer au bon endroit.

Si la communauté n'est pas disponible, l'administrateur pourra déplacer manuellement l'équipement.

## Les 6 vues d'IntraVUE

IntraVUE permet d'afficher six différentes vues de votre réseau.

Dans chaque vue, chaque nœud présente des informations différentes :

- Nom
- Liens Web
- Miniatures
- icônes

La topologie est la même dans chacune des vues.

Le nom de la vue courante est affiché dans le coin supérieur gauche de la fenêtre de navigation.

Trois de ces vues sont définies automatiquement par IntraVUE, il s'agit de « Device View », « IP view » et « Location view ». Sur la « Device View », les noms d'équipements sont renseignés par le scanner, soit par les informations SNMP, soit par le nom NetBIOS. Sur l' « IP View », le nom de l'équipement est toujours l'adresse IP et sur la « Location view » le nom est l'information de localisation du SNMP si celle-ci est disponible.

Trois autres vues sont configurables par l'administrateur. Le nom par défaut peut être modifié dans l'onglet « General tab » du menu « System configuration ». Par défaut, les vues s'appellent « User Defined1 », « User Defined 2 », « User defined 3 »..

Pour chacune des vues, l'administrateur peut configurer les liens Web, les miniatures et les icônes à afficher pour chaque équipement.

Renseigner les paramètres de lien Web ou d'image pour chaque équipement, rendent IntraVUE encore plus puissant et utile.



Veillez regarder *Personnalisation du navigateur* Pour plus d'informations sur la modification des paramètres d'affichage par défaut du navigateur.



Il y a un paramètre dans le fichier *ivserver.properties* qui établit ce qu'IntraVUE utilisera lorsque le navigateur sera lancé et si les icônes et les vignettes doivent être affichés ou pas. Voir la variable nommée "view.settings" vers la fin du fichier

## Comptes utilisateurs

Il y a deux types de comptes dans IntraVUE. USER et ADMIN.

Un USER peut consulter toutes les données disponibles dans chacune des vues d’IntraVUE.


Il peut également ajouter un événement sur un équipement par l’intermédiaire des propriétés de l’équipement ou de la fenêtre d’événements.

Un ADMIN peut configurer IntraVUE grâce au menu « System configuration »

Ce privilège est accessible en saisissant un mot de passe. Le mot de passe par défaut est : intravue.

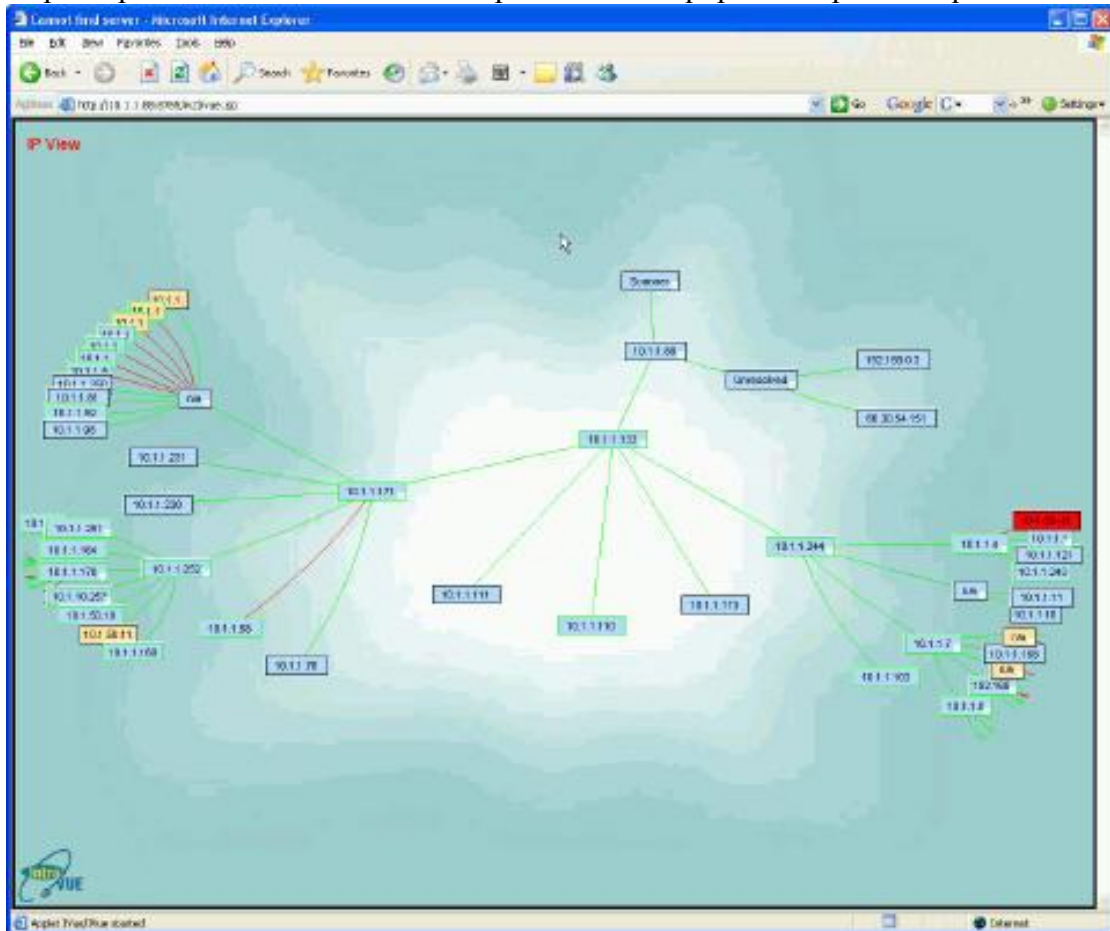
Dans la version actuelle, le mot de passe est identique pour tous les administrateurs.

Dans une future version, la gestion des comptes utilisateurs sera gérée par le serveur Apache et permettra d’accorder des privilèges en fonction du couple nom d’utilisateur / mot de passe.

 Il est cependant possible de configurer un mot de passe pour accéder à l’interface d’IntraVUE voir le chapitre Connexion administrateur.

## Ecran principal

La fenêtre principale d’IntraVUE montre la répartition des équipements pour chaque réseau configuré.



L’interface utilisateur est affichée par le biais d’un navigateur tel qu’Internet Explorer ou Mozilla Firefox. Sur l’ordinateur hôte l’URL est toujours **http://127.0.0.1:8765** .



Le port 8765 est nécessaire après l’adresse IP et, généralement, vous devez également entrer le *http://*.

Le réseau est visualisé sous la forme d’un arbre ou d’une étoile entourant le scanner. Cette méthode brevetée s’appelle un arbre hyperbolique.

Des équipements (ou nœuds) sont représentés par des rectangles de couleur connectés par des lignes de couleur.

Pour visualiser une partie spécifique du réseau, il est possible de glisser la souris (cliquer maintenir et déplacer) pour centrer la vue.

On peut imaginer qu’IntraVUE affiche un plan du réseau autour d’une sphère. Vous ne pouvez donc voir qu’une partie de la sphère.

Cette fonctionnalité permet de représenter des réseaux très grands et très complexes dans une seule fenêtre.

### Commandes

Il est possible d'utiliser quelques raccourcis dans la fenêtre d'affichage d'IntraVUE.

- Clic droit sur un nœud : Affiche le menu correspondant au nœud.
- Clic droit sur une ligne : Affiche le graphique de bande passante et quelques informations supplémentaires.
- Clic droit sur le fond : Affiche le « System menu »
- Glisser : Déplace la vue du réseau.
- ALT+ Clic gauche : allonge la longueur des lignes.



Attention, toutes les lignes sont concernées par cette modification.

### Fonctions disponibles

C'est une autre forme de commandes de la souris.

- «menu Système» accessible par un clic droit sur le fond.
- «menu Equipement» accessible par un clic droit sur un nœud.
- Graphique de bande passante accessible par un clic droit sur une ligne.
- Informations du port accessible par survol du lien avec la souris.

### Développer et réduire les nœuds

Pour simplifier l'affichage de réseaux très complexes, les nœuds avec beaucoup de sous nœuds peuvent être cachés ou affichés en cliquant sur le – ou le + du nœud (Dans le coin en bas à droite).

Cacher un groupe d'équipements ne cache pas pour autant les alarmes et les seuils associés. Si un événement se produit alors que l'équipement est caché, un triangle de couleur indique la nature de l'événement sur le nœud à étendre.

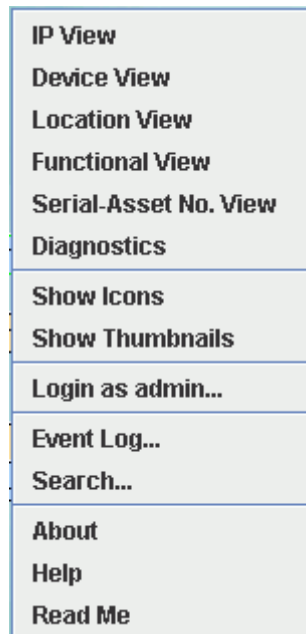


Voir également le chapitre Utilisation des couleurs

## Module : Mode Opérateur

Ce menu, affiché par un clic droit sur le fond. Se compose de plusieurs sections.

La première section permet la sélection de la vue à afficher.



La seconde partie permet d'activer ou non l'affichage des icônes et des images miniatures.

Le « Login as admin » permet à l'utilisateur d'acquérir les privilèges administrateur. Cette fonction est protégée par un mot de passe.

Le « event log » affiche la fenêtre d'événement pour tous les équipements présents sur le réseau. Cependant il est possible de filtrer l'affichage notamment grâce à l'adresse IP, MAC ou au nom.

**Search** permet de rechercher un équipement.

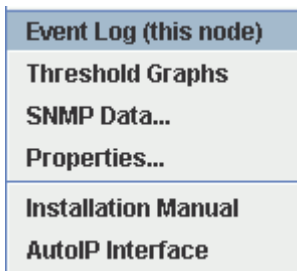
« About » donne la version d'IntraVUE installée.

« Help » affiche l'aide en ligne.

« Read me » affiche des informations propres à la version installée.

## Menu « Equipement »

Ce menu s'affiche lors d'un clic droit sur un nœud.



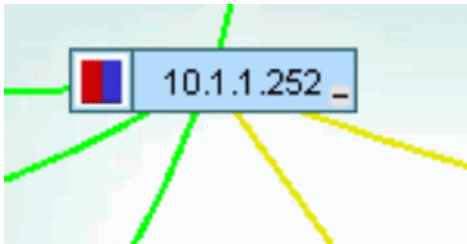
Quatre fonctions majeures sont possibles :

- « **Event log** » affiche les événements associés uniquement au nœud sélectionné.
- « **Threshold Graphs** » affiche le diagramme de seuil pour cet équipement et tous les équipements connectés dessus.
- « **SNMP data** » affiche les informations SNMP de l'équipement sélectionné.
- « **Properties** » Affiche les propriétés de l'équipement sélectionné.

Si un lien Web est configuré dans les propriétés de l'équipement, il est alors possible d'y accéder directement à partir de ce menu par le bouton « Active Web link ».

## Icônes

Les icônes permettent d'identifier rapidement un attribut spécifique de l'équipement.



Par exemple:

- Une couleur pour chaque LAN,
- Une couleur pour les connexions sécurisées ou non,
- Une couleur pour chaque localisation.
- 

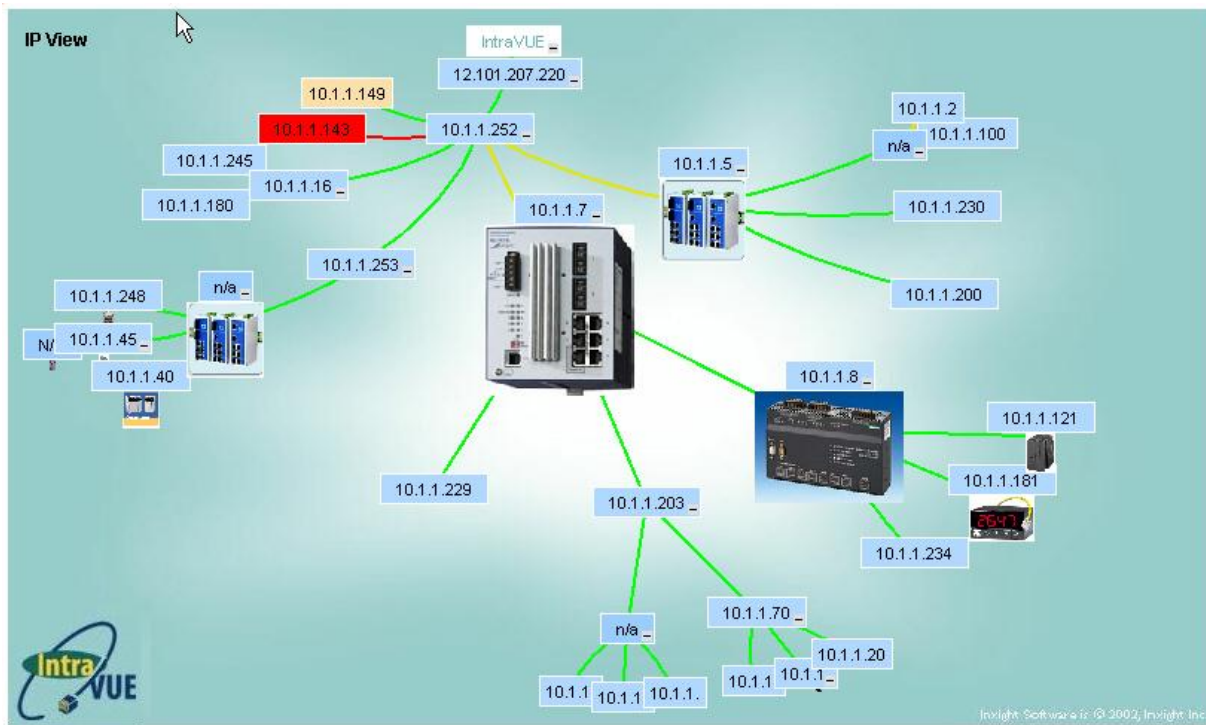
Les icônes sont des images de petites tailles (inférieures à 32\*32 pixels) de préférence. Car l'utilisation d'icônes plus grandes peut entraîner des pertes de performances importantes.

Ces icônes sont uniquement configurées par l'administrateur.

---

## Images miniatures

Les miniatures sont des images de plus grandes tailles (Par rapport aux icônes). Elles peuvent être utilisées pour identifier plus facilement les types d'équipements du réseau.



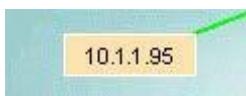
Chaque vue possède ses propres images miniatures pour chaque équipement.

Par exemple, dans la « Location View » il est possible de mettre une photo de l'armoire électrique avec une flèche pointant vers l'équipement concerné. Cette utilisation est très pratique lorsque plusieurs équipements se trouvent dans la même armoire électrique.

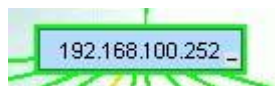
## Utilisation des couleurs

Un nœud (représentant un équipement) est un rectangle. Un nœud peut avoir 3 couleurs de fond et 4 couleurs de pourtour

### Couleur de fond des nœuds

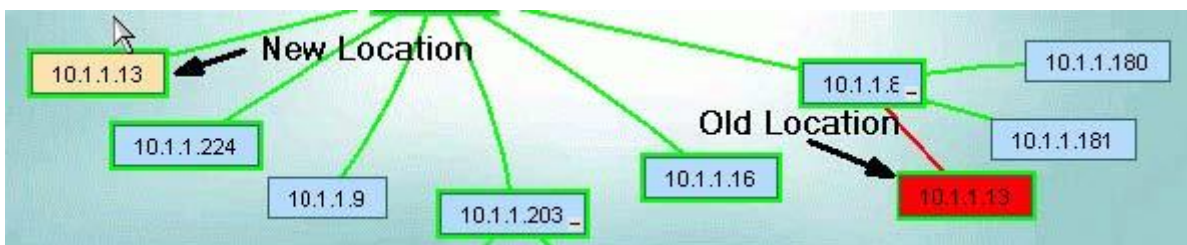


Les équipements nouvellement découverts et/ou qui n'ont pas été vérifiés par l'administrateur apparaissent sur fond orangé.



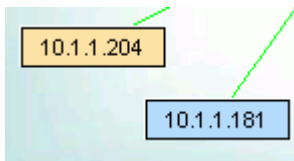
Les équipements vérifiés par l'administrateur apparaissent sur fond bleu.

**Idéalement, un réseau normal doit contenir uniquement des nœuds sur fond bleu.** Ainsi un nouvel équipement sera facilement identifiable.

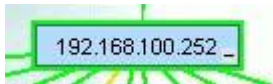


Si un équipement préalablement vérifié par l'administrateur change de place, l'ancienne localisation est représentée par un nœud sur fond rouge et la nouvelle localisation par un nœud sur fond orange. (En attente de validation par l'administrateur)

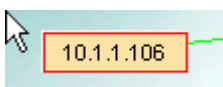
### Couleur du pourtour des nœuds



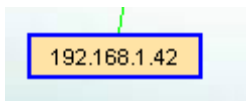
Les équipements entourés de noir ne supportent pas le SNMP.



Les équipements entourés de vert supportent le SNMP et communiquent avec IntraVUE.

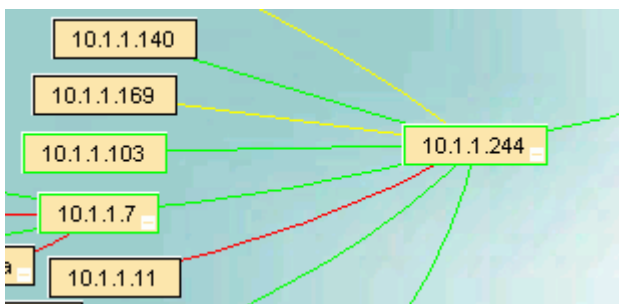


Les équipements entourés de rouge supportent le SNMP mais les informations ne sont pas accessibles.



Les équipements sélectionnés ont une bordure Bleue épaisse.

### Couleur des liens



Les liens peuvent être de cinq couleurs différentes :

- Vert : Indique que l'équipement est connecté et la communication est établie.
- Jaune : Indique qu'un seuil a été dépassé.
- Rouge : Indique que le lien est coupé et que l'équipement ne répond pas au ping.
- Noir : Indique un lien manuellement ajouté.
- Bleu : Indique que le lien est sélectionné par un clic gauche.

Les liens en pointillés représentent les connexions Sans-fil.

## Equipements mobiles

Certains équipements peuvent être configurés par l'administrateur pour se déplacer d'un endroit à un autre endroit sans afficher la moindre alarme lorsqu'ils sont déconnectés. Ces mouvements seront enregistrés dans la fenêtre d'événements.

Dans un premier temps, l'équipement apparaît déconnecté. Puis lorsque la communication est rétablie, l'ancienne position de l'équipement est effacée.

Si l'équipement a été vérifié par l'administrateur, la boîte sur fond rouge ne sera jamais affichée. Seule une boîte sur fond bleu changera de position.

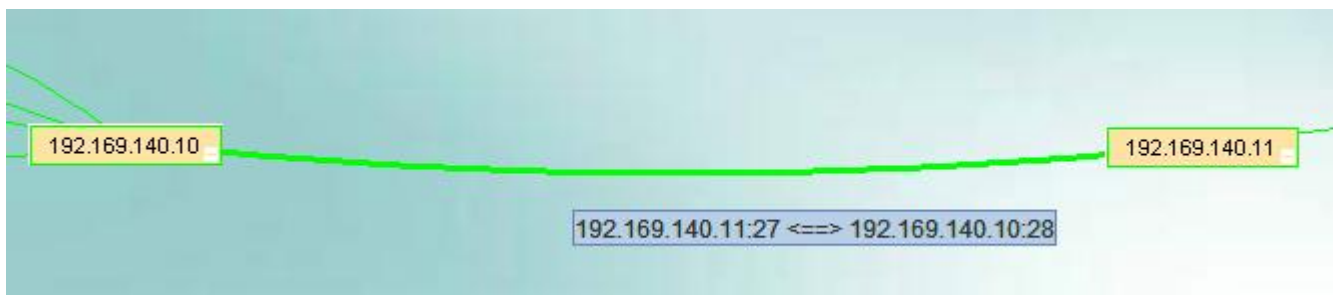
Les équipements sans-fil doivent avoir cette options de validé pour leur permettre de se déplacer sans émettre des alarmes.

Cette option se trouve dans la fiche de configuration de l'équipement -> case à cocher « Auto connect ».

## Fonctions de survol

Lorsque le pointeur de souris est placé sur un équipement ou sur un lien sans cliquer, une info bulle sur fond bleu apparaît.

### Au dessus d'un lien

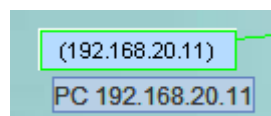


L'info bulle affichée sur l'image ci-dessus montre la connexion entre deux switches. Dans cet exemple, le switch 192.168.140.11 utilise le port 27 pour communiquer avec le switch 192.168.140.10 sur le port 28.



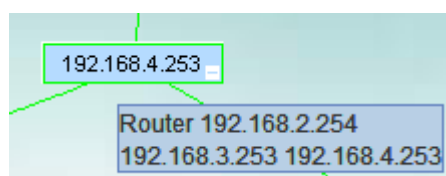
Note: Si les numéros de port sont faux et que vous voulez avoir d'autres numéros, regardez le chapitre Utilisation du Trunking dans les Switchs

### Au dessus d'un équipement



L'info bulle affiche l'adresse IP et le nom de l'équipement (champs « IP address » et « Device Name »)

Notez que l'info bulle d'un routeur contient d'autres adresses IP qui correspondent à ses différentes interfaces.



## Propriétés des équipements



En plus des noms des 6 vues d'IntraVUE, l'adresse MAC et la catégorie de l'équipement sont affichées.

Pour chaque vue, chaque lien Web configuré est accessible par son bouton approprié. Si aucun lien n'est configuré, « none » apparaît et le bouton est grisé. Si un nom de lien est configuré mais sans adresse « no url » apparaît dans le bouton.

A partir de cette fenêtre de propriété, il est possible d'afficher directement la fenêtre d'événement associée à l'équipement.

## Seuils sur les liens

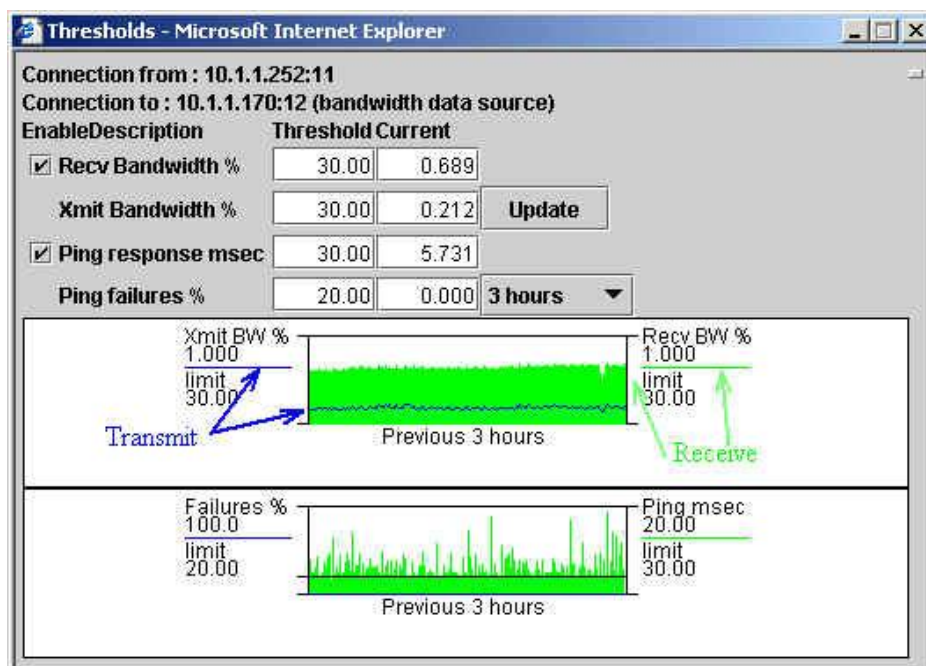
Quatre données sont surveillées et tracées sur des graphes. Ces graphes sont accessibles par un clic droit sur le lien entre les deux équipements.

- Transmitted Bandwith (Xmit) – Pourcentage de bande passante utilisé en émission.
- Recived Bandwith (Recv) – Pourcentage de bande passante utilisé en réception.
- Ping response – Temps de réponse au ping.
- Ping failure – Pourcentage d'échec de réponse au ping.



Le graphe est mis à jour chaque minute. L'affichage est dynamique et rafraîchi automatiquement.

**Ping data** est recueilli plusieurs fois par minute, en général 5 à 10 fois. Ces succès de Ping dans une période d'une minute ont leurs temps de réponse moyennés et cette moyenne sur une minute est utilisée comme un point de données pour Thresholding. Si la requête ping échoue et le Ping suivante est réussie, il est compté comme un échec de Ping. Au cours de la période d'une minute, le nombre de pannes divisé par le nombre de Ping pour la période une minute devient le taux de défaut de Ping pour cette période d'une minute. (Si deux Ping successifs échouent, il est enregistré comme une déconnexion du dispositif.)



## Activer ou désactiver les alarmes

Il y a deux cases à cocher pour activer ou non les alarmes sur bande passantes ou sur réponse au Ping. Ces options sont accessibles uniquement par l'administrateur.

L'alarme sur le Ping et la bande passante est activée dans l'exemple ci-dessus. La bande passante transmise ou reçue peut déclencher une alarme de bande passante. De même le taux d'échec au Ping sur la dernière minute ou un dépassement du seuil de réponse Ping sur la dernière minute va générer une alarme.

### Ping

Les informations sur le Ping sont récupérées 5 à 7 fois par minute et la moyenne de cette minute est utilisée pour tracer un unique point. Tout défaut de Ping est enregistré et apparaît dans le pourcentage de défaut.

### Bande passante

Si un équipement ne supporte pas le SNMP, IntraVUE va essayer d'obtenir l'information à partir du switch sur lequel est connecté l'équipement. L'équipement source de cette information est identifié par l'item « data source » sur le lien entre les équipements.

### Data Résolution

Les données sont stockées en interne de manière à créer progressivement les données d'historiques des données les plus récentes.

Sous le bouton « update », une liste déroulante vous permet de choisir l'intervalle de temps à afficher sur les graphes. (Entre 3h et 1 an)

- 3 h
- 6 h
- 30 h
- 60 h
- 15 jours
- 30 jours
- 6 mois
- 12 mois

### Echelle

Au sommet de chaque graphe, la valeur de la pleine échelle est affichée. Cette valeur change dynamiquement en fonction des valeurs relevées afin d'adapter l'échelle en conséquence.

La représentation graphique des valeurs max va changer pour vous offrir la meilleure interprétation de données

### Graphes de bande passante

La bande passante de transmission est affichée par une ligne bleue et la bande passante de réception est affichée par une ligne verte.

Dans l'exemple page précédente, l'échelle du graphe de bande passante est de 100% et tous les seuils sont configurés à 30 %. S'il y a un pic à 22 % dans les 3 heures indiquées, l'échelle aurait été fixé à environ 25 % ainsi il est possible de voir toutes les données sans dépasser le maximum.

### Graphes de réponse au Ping

Les défauts de réponse au Ping et les temps de réponse au Ping sont affichés sur le même graphe. Le maximum du graphe de défaut de Ping est toujours 100 %. Le maximum du graphe de temps de réponse au Ping est dynamique, l'échelle est adaptée aux valeurs relevées.

Dans l'exemple ci-dessus la réponse Ping max est de 20 millisecondes montrant des pointes d'environ 19 millisecondes et la Ping seuil de réponse est de 30 millisecondes.

### Réglage des seuils

Le bouton « update » est disponible pour l'administrateur pour changer les valeurs des seuils et pour mettre à jour la base de données avec les nouveaux réglages. Attention les graphes ne sont pas mis à jour immédiatement après le clic.

## Graphique Multi-équipements

Le Multi Threshold Graph (ou Graphique Multi-équipements) permet de voir un type de seuil pour plusieurs équipements en même temps.

### Sélection

La méthode principale de sélection vient du menu d'un équipement. Dans ce cas tous les équipements connectés vers et depuis cet équipement sont affichés ensemble.

- Si vous cliquez sur le scanner, vous aurez tous les équipements - même s'ils sont dans différents réseaux IntraVUE.
- Si vous cliquez sur un top parent, vous aurez uniquement les équipements d'un même réseau IntraVUE.
- Si vous cliquez sur un switch, vous aurez uniquement le switch et les équipements en dessous du switch.
- Si vous cliquez sur un équipement terminal, vous aurez uniquement les données de cet équipement.

La deuxième méthode est disponible à partir du journal des événements. En faisant un clic droit sur un événement, le graphique est disponible depuis le menu contextuel.

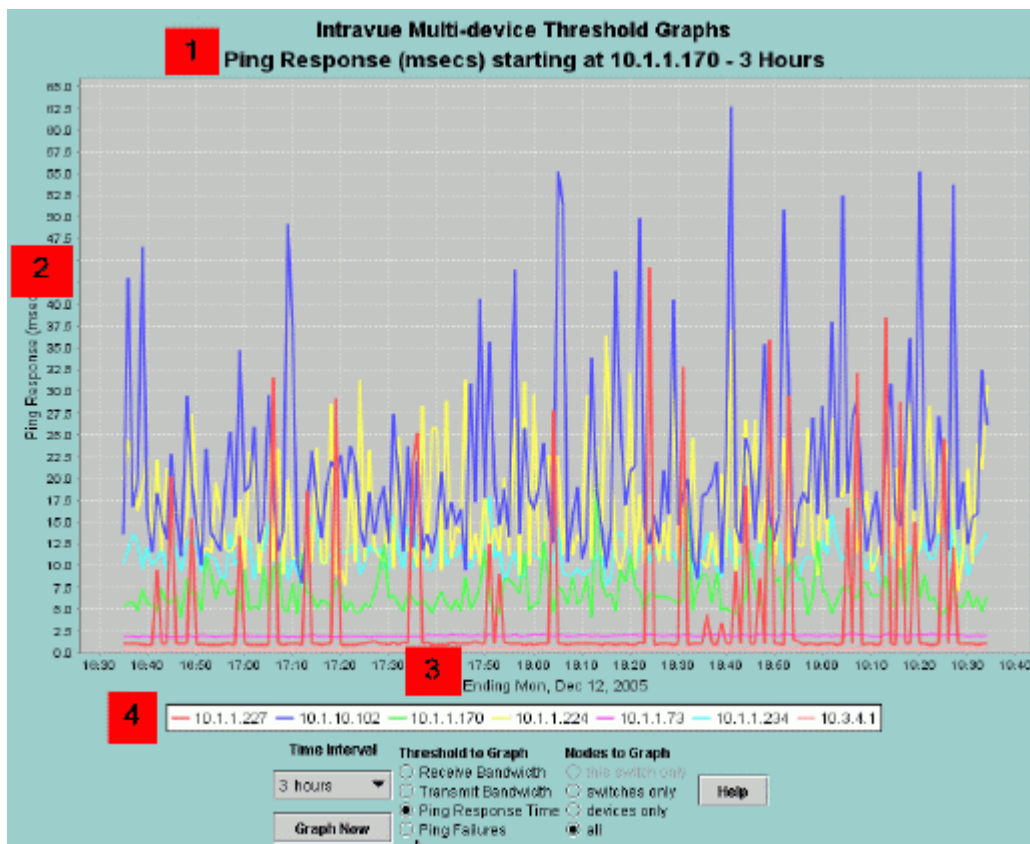
### Données

Les données disponibles pour le Mutli-Threshold Graphs sont exactement les mêmes que pour les graphiques de lignes disponibles par un clic droit sur n'importe quelle ligne de connexion.

Les données comprennent:

- La bande passante en Réception
- La bande passante en Transmission
- Le temps de réponse au Ping
- Les échecs de Ping

## Eléments Graphique



L'image ci-dessus contient des marqueurs numérotés pour chacun des éléments graphiques majeurs.

La boîte rouge 1 est à côté du *Titre du diagramme*, qui inclut le seuil spécifique actuellement affichée et la période des données.

L'échelle de *valeur des données* est près du 2 rouge. L'échelle change à chaque fois qu'une nouvelle donnée est affichée et est redessinée sur le graphique. La valeur maximale est proche du sommet du graphe.

Le 3 rouge est près de la *valeur de temps* du graphique. Lors de l'affichage sur 3 heures les valeurs des données seront affichées avec l'horloge en temps normal. Lors de l'affichage des données sur des périodes plus longues il peut y avoir jusqu'à trois lignes d'informations de temps à savoir l'année, le mois et le jour.

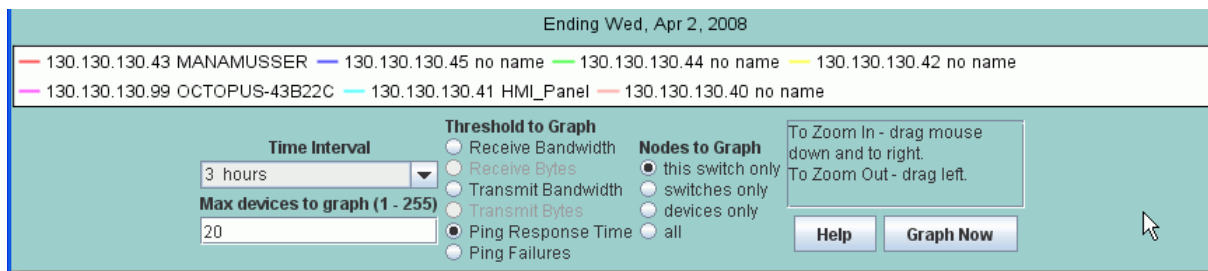


Notez que les données disponibles combleront le graphe de gauche à droite. S'il y a seulement quelques semaines de données dans la base et que vous sélectionnez la vue de 12 mois, les données disponibles combleront l'axe des x.

Il y aura normalement une indication de dates/heures de début et de fin dans ce cas.

Le 4 rouge indique l'endroit où la *légende du graphique* se trouve. Chaque appareil aura une couleur assignée. Si vous avez des problèmes pour dire à quelle ligne appartient quel périphérique, un texte peut s'afficher près des points du graphique et une fonction de zoom est disponible (voir ci-dessous).

## Sélection des options utilisateur



La liste déroulante du **Time Interval** vous permet de choisir entre 3 heures de données et 12 mois de données. Si les données ne sont pas disponibles pour toute la période sélectionnée alors le temps sera limité aux données misent à disposition Si vous deviez choisir l'option 12 mois et qu'IntraVUE a uniquement une heure d'analyse alors aucune donnée ne sera disponible.

Le champ **Max Devices To Graph** vous permet de limiter le nombre d'appareils qui apparaîtront dans le graphique. La limite est fondée sur les pires cas des données. Si 20 périphériques (ou moins) sont représentées, une légende sera affichée sous le graphique. Si vous définissez "Max Devices" pour le graphique à 21 ou plus alors aucune légende ne sera affichée.

Les boutons radio **Threshold to Graph** vous permettent de choisir parmi les quatre types de graphiques

Les boutons radio **Nodes to Graph** vous permettent de filtrer les données pour les switches seulement, seuls les périphériques, tous les périphériques, ou si le dispositif actuel est un switch, seuls les ports du switch courant.



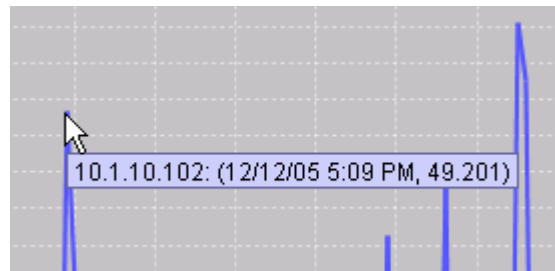
Notez que cette dernière option n'est pas disponible dans la pré-release

Le bouton **Graph Now** permet d'obtenir de nouvelles données de la base de données IntraVUE et affiche les résultats.



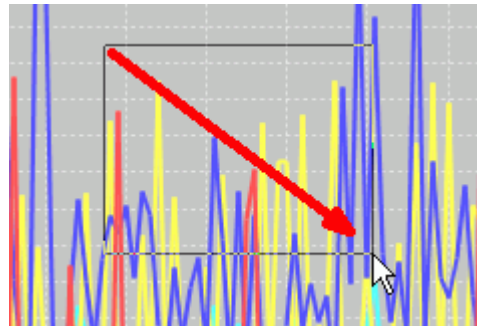
Remarque: Le graphique ne se met pas à jour après avoir modifié les sélections, il se met à jour uniquement lorsque ce bouton est sélectionné.

## Bulle Texte



Quand la souris est positionnée près d'un Point graphique, sur un pic, la bulle Texte indiquera l'adresse IP de l'appareil, la valeur du pic et l'horodatage.

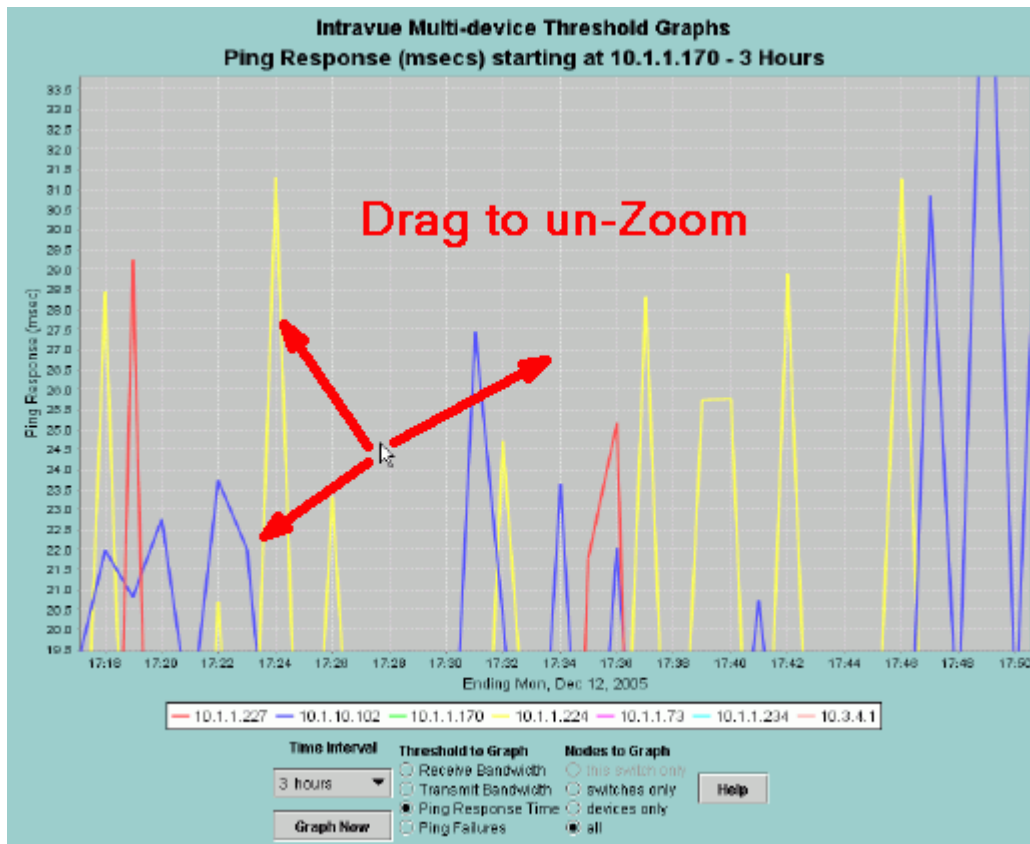
## Zoom Plus



Vous pouvez zoomer sur n'importe quelle portion du graphique en faisant glisser la souris avec le bouton gauche de la souris. Pour zoomer, vous devez faire glisser la souris vers la droite et vers le bas. Lorsque vous faites glisser, vous verrez le contour de la zone de zoom. Lorsque vous relâchez le graphique sera zoomée.

Vous pouvez zoomer autant de fois que vous le souhaitez.

## Zoom Moins

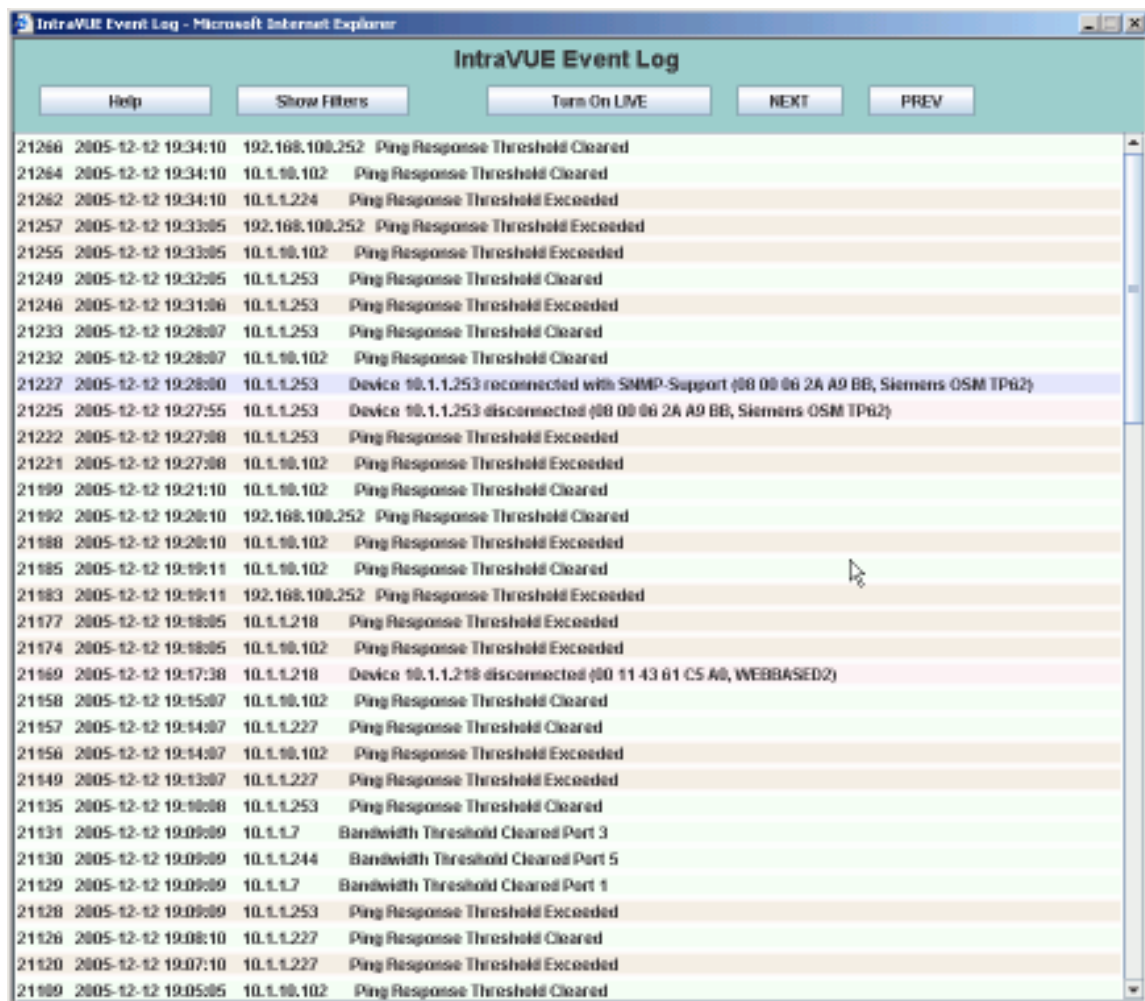


Lorsque vous êtes prêt à effectuer un zoom arrière, faites simplement glisser la souris dans n'importe quelle direction, sauf le droit et le bas.

## Fenêtre d'événements

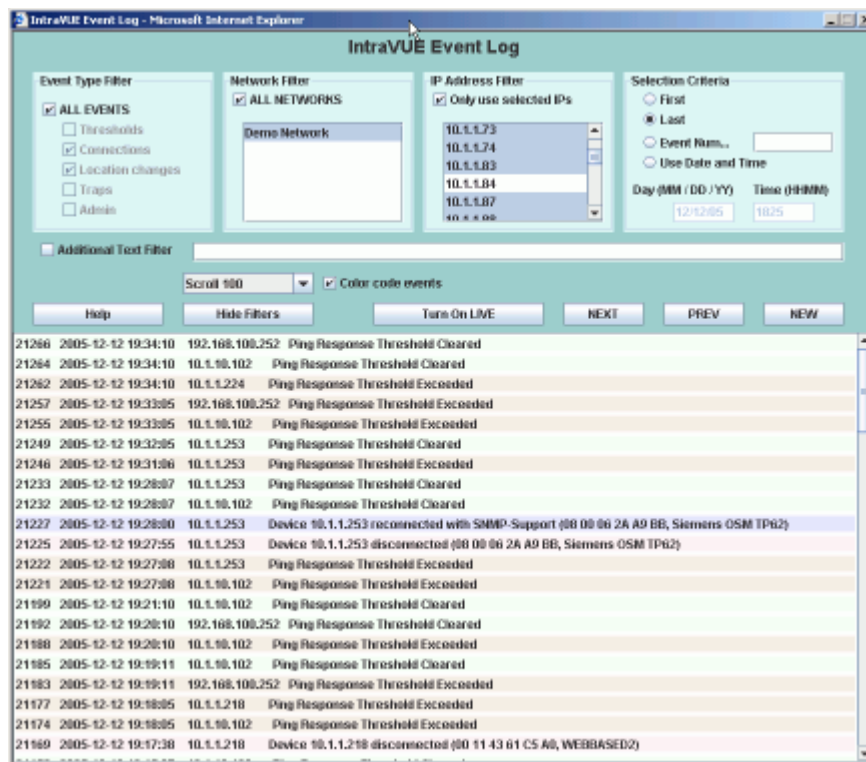
Il y a deux manières d'afficher le journal d'événements

La première maximise le nombre d'événements à afficher.



ID	Timestamp	IP Address	Event Description
21286	2005-12-12 19:34:10	192.168.100.252	Ping Response Threshold Cleared
21284	2005-12-12 19:34:10	10.1.10.102	Ping Response Threshold Cleared
21282	2005-12-12 19:34:10	10.1.1.224	Ping Response Threshold Exceeded
21257	2005-12-12 19:33:05	192.168.100.252	Ping Response Threshold Exceeded
21255	2005-12-12 19:33:05	10.1.10.102	Ping Response Threshold Exceeded
21249	2005-12-12 19:32:05	10.1.1.253	Ping Response Threshold Cleared
21246	2005-12-12 19:31:06	10.1.1.253	Ping Response Threshold Exceeded
21233	2005-12-12 19:28:07	10.1.1.253	Ping Response Threshold Cleared
21232	2005-12-12 19:28:07	10.1.10.102	Ping Response Threshold Cleared
21227	2005-12-12 19:28:00	10.1.1.253	Device 10.1.1.253 reconnected with SMMP-Support (08 00 06 2A A9 BB, Siemens OSM TP62)
21225	2005-12-12 19:27:55	10.1.1.253	Device 10.1.1.253 disconnected (08 00 06 2A A9 BB, Siemens OSM TP62)
21222	2005-12-12 19:27:08	10.1.1.253	Ping Response Threshold Exceeded
21221	2005-12-12 19:27:08	10.1.10.102	Ping Response Threshold Exceeded
21199	2005-12-12 19:21:10	10.1.10.102	Ping Response Threshold Cleared
21192	2005-12-12 19:20:10	192.168.100.252	Ping Response Threshold Cleared
21188	2005-12-12 19:20:10	10.1.10.102	Ping Response Threshold Exceeded
21185	2005-12-12 19:19:11	10.1.10.102	Ping Response Threshold Cleared
21183	2005-12-12 19:19:11	192.168.100.252	Ping Response Threshold Exceeded
21177	2005-12-12 19:18:05	10.1.1.218	Ping Response Threshold Exceeded
21174	2005-12-12 19:18:05	10.1.10.102	Ping Response Threshold Exceeded
21169	2005-12-12 19:17:38	10.1.1.218	Device 10.1.1.218 disconnected (00 11 43 61 C5 A0, WEBBASE02)
21158	2005-12-12 19:15:07	10.1.10.102	Ping Response Threshold Cleared
21157	2005-12-12 19:14:07	10.1.1.227	Ping Response Threshold Cleared
21156	2005-12-12 19:14:07	10.1.10.102	Ping Response Threshold Exceeded
21149	2005-12-12 19:13:07	10.1.1.227	Ping Response Threshold Exceeded
21135	2005-12-12 19:10:08	10.1.1.253	Ping Response Threshold Cleared
21131	2005-12-12 19:09:09	10.1.1.7	Bandwidth Threshold Cleared Part 3
21130	2005-12-12 19:09:09	10.1.1.244	Bandwidth Threshold Cleared Part 5
21129	2005-12-12 19:09:09	10.1.1.7	Bandwidth Threshold Cleared Part 1
21128	2005-12-12 19:09:09	10.1.1.253	Ping Response Threshold Exceeded
21126	2005-12-12 19:08:10	10.1.1.227	Ping Response Threshold Cleared
21120	2005-12-12 19:07:10	10.1.1.227	Ping Response Threshold Exceeded
21109	2005-12-12 19:05:05	10.1.10.102	Ping Response Threshold Cleared

La vue alternative montre des champs de filtre supplémentaires.

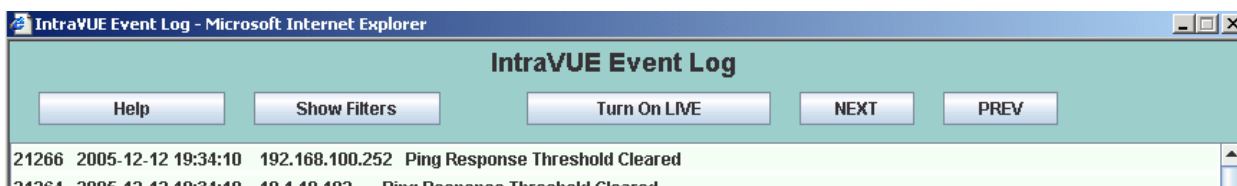


IntraVUE continue en permanence à surveiller toute l'activité du réseau. Pour accéder à la fenêtre d'événement de tout le réseau, il suffit de sélectionner « event log » dans le « menu system ». Pour accéder à l' « event log » d'un équipement en particulier, il faut d'abord sélectionner l'équipement puis cliquer sur « event log » du « menu équipement ».



Note: Il n'y a qu'une fenêtre d'événement. Une fois ouverte vous pouvez passer de tous les équipements à ceux que vous voulez voir en utilisant la case à cocher **Only Use Selected IP's**

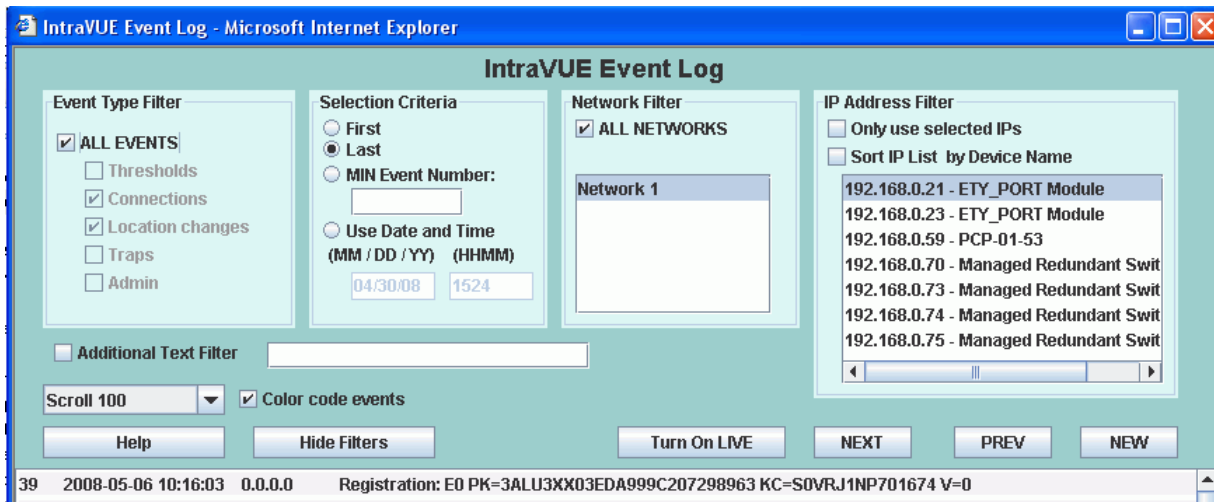
Initialement, au chargement de la fenêtre d'événement, aucun filtre n'est sélectionné :



Dans la vue principale, vous pouvez naviguer vers les éléments suivants en cliquant sur les boutons « Next et Prev ».

Le bouton « Turn on live » permet de passer la fenêtre d'événements en mode « fil de l'eau ». La période de rafraîchissement est de 5 secondes.

Cliquez sur « Show filters » pour afficher le menu de configuration des filtres.



La liste des événements peut être triée selon plusieurs critères :

- Type d'événements,
- Réseau,
- Adresse IP
- Choisissez de d'afficher en tête le premier ou le dernier événement,
- Saisissez un filtre qui peut être un libellé.

Lorsque le filtre par adresse IP est actif, si la case « only use selected IP » est cochée, seules les adresses IP en surbrillance sont affichées.

Astuce: pour exclure une adresse, utiliser Ctrl-A pour sélectionner tous, puis de contrôle + clique gauche pour désélectionner les appareils que vous ne voulez pas voir. Ceci est illustré dans l'exemple ci-dessus où 10.1.1.84 est désélectionnée.

Si vous faites une sélection par date, la date choisie sera placée au milieu de la fenêtre.

Un champ vous permet de sélectionner le nombre d'événements à afficher :

- Pleine page
- 100
- 500
- 1000
- 2000

Si la case “Color code events” est décochée, les événements sont affichés avec plusieurs niveaux de gris et non par des couleurs différentes.

Une fois les paramètres sélectionnés, cliquez sur le bouton “New” pour appliquer le filtre.

Les boutons "next" et "prev" permettent d'afficher les éléments suivants.

Le bouton "Turn on live" utilise les critères sélectionnés et rafraîchit la fenêtre toutes les 5 secondes.

21269	2005-12-12 19:34:37	10.1.1.37	Device 10.1.1.37 reconnected (00 13 20 8F 6C 23, W2003-SVR)
21268	2005-12-12 19:34:10	10.2.49.1	Ping Response Threshold Cleared
21267	2005-12-12 19:34:10	10.2.10.1	Ping Response Threshold Cleared
21266	2005-12-12 19:34:10	192.168.100.252	Ping Response Threshold Cleared
21265	2005-12-12 19:34:10	192.168.100.1	Ping Response Threshold Cleared
21264	2005-12-12 19:34:10	10.1.10.102	Ping Response Threshold Cleared
21263	2005-12-12 19:34:10	10.1.1.1	Ping Response Threshold Cleared
21262	2005-12-12 19:34:10	10.1.1.224	Ping Response Threshold Exceeded
21261	2005-12-12 19:33:42	10.1.1.37	Device 10.1.1.37 disconnected (00 13 20 8F 6C 23, no name)

Center this device in IntraVUE  
Spotlight this device in IntraVUE  
Threshold Graph this device  
Filter for this device only

Si plusieurs équipements différents sont affichés, il est possible d'en sélectionner un ou plusieurs grâce à la touche CTRL.

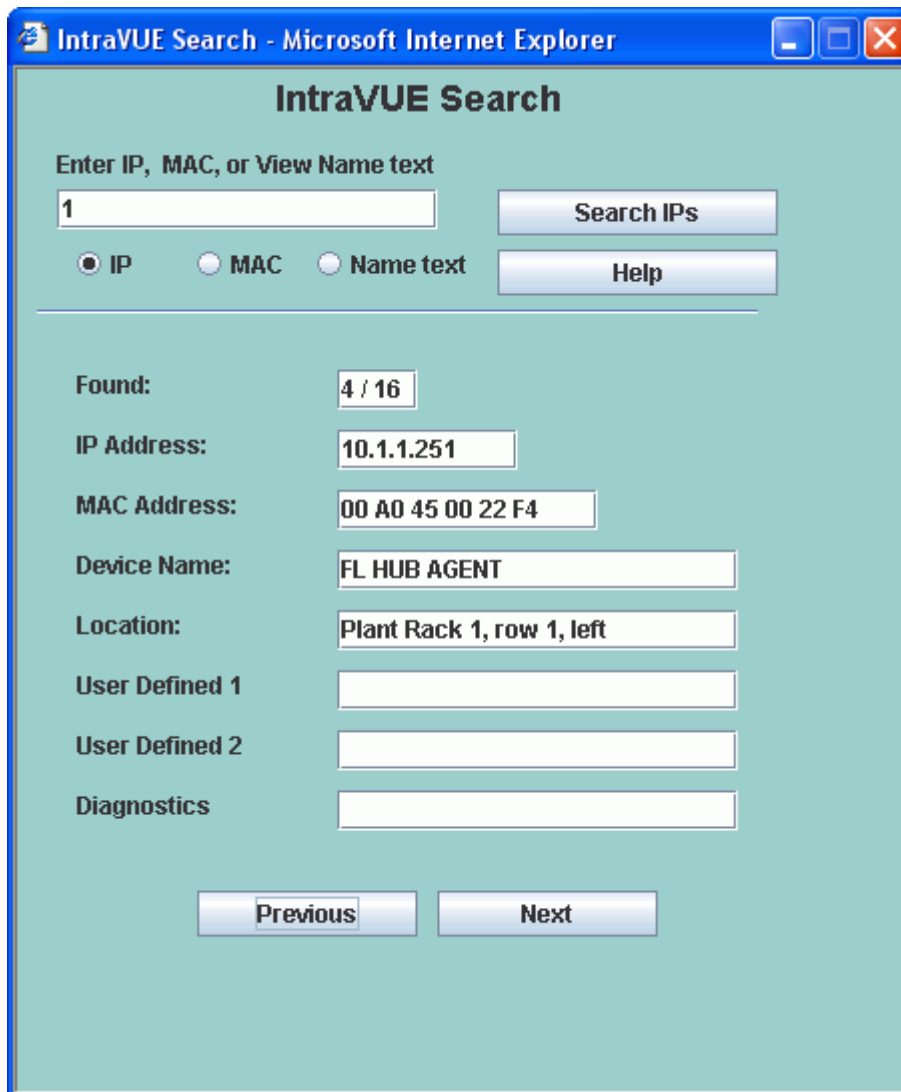
Le clic droit vous permet d'effectuer plusieurs opérations:

- Centrer l'équipement concerné dans la fenêtre principale d'IntraVUE,
- Mettre en surbrillance l'équipement par un triangle violet (Uniquement en 2.1),
- Tracer le graphe correspondant,
- Si plusieurs équipements sont sélectionnés, il est possible d'en sélectionner un seul.

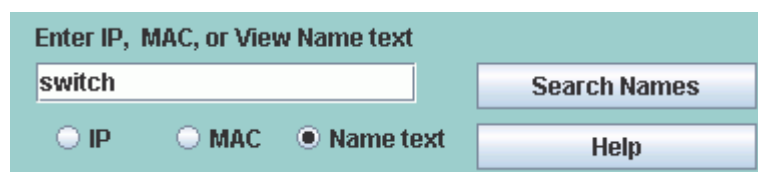
## Recherche

Le menu de recherche est accessible dans le “ menu Système ”

Cela fourni un moyen rapide de recherche d'équipements lorsque beaucoup de nœuds sont affichés.



3 boutons radio permettent de sélectionner le filtre sur adresse IP, MAC ou par nom.



Quel que soit le type de recherche que vous utilisez, la recherche est automatiquement précédés d'un astérisque (\*).

Pour les adresses IP, différents formats sont acceptés :

- Adresse IP complète,
- xxx.xxx.xxx.1.
- 100.xxx.xxx.xxx

Exemple, un ".100." va trouver X.100.X.X, X.X.100.X, mais pas X.X.X.100

Pour le filtrage par adresse MAC il est possible de séparer les caractères par des espaces ou des tirets.

La boîte de dialogue est mise à jour dès qu'un équipement répondant aux critères de recherche correspondants.

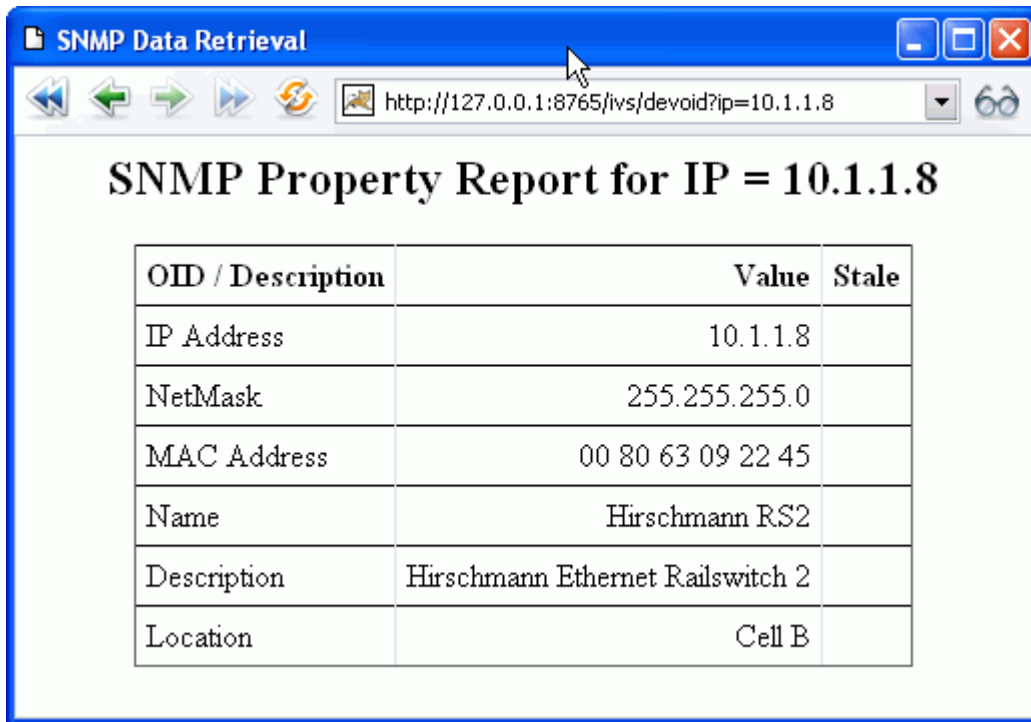
Il y a deux caractères joker : \* et ?.

- Un '\*' va correspondre à n'importe quel nombre ou caractère.
- Un '?' va correspondre à un seul caractère. Dons '.11?' va correspondre à .111, et .114, mais pas à .11

Vous pouvez utiliser les boutons « Prev » et « Next » pour naviguer entre les équipements. Chaque sélection centre automatiquement l'équipement dans la vue principale d'IntraVUE.

## Données SNMP

Les données SNMP fournissent des informations supplémentaires sur un périphérique.



OID / Description	Value	Stale
IP Address	10.1.1.8	
NetMask	255.255.255.0	
MAC Address	00 80 63 09 22 45	
Name	Hirschmann RS2	
Description	Hirschmann Ethernet Railswitch 2	
Location	Cell B	

Les 6 premières lignes sont des entrées standard MIB II et sont disponibles de n'importe quel dispositif de support de SNMP.

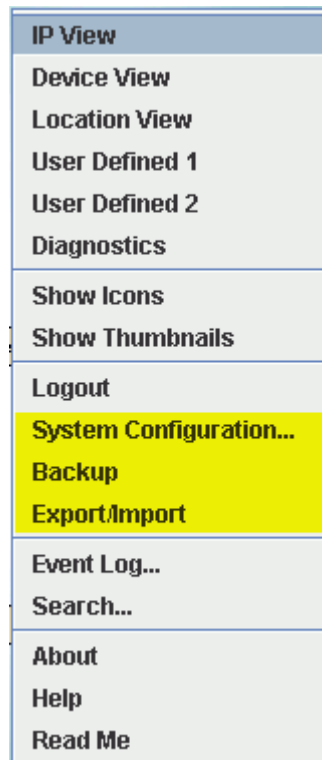
En outre, l'administrateur IntraVUE peut configurer n'importe quelles autres données SNMP de l'appareil et les mettre à disposition dans cette boîte de dialogue ainsi que pour le serveur Modbus/TCP disponible dans IntraVUE.



Pour plus d'information regardez la section Configuration Modbus/TCP et des données SNMP dans le chapitre Le fichier ivserver.xml

## Module : Mode Administrateur

Une fois enregistré en tant qu'administrateur, 3 items supplémentaires apparaissent dans le menu.



«**System Configuration**» donne accès à la configuration de la base de données et du scanner IntraVUE.

«**Backup**» sauvegarde la base de données MySQL dans le dossier d'installation d'IntraVUE (Dossier dbBackup). Le nom de la sauvegarde est généré automatiquement et basé sur la date et l'heure courante.

«**Export/Import**» permet d'exporter et d'importer la base de données IntraVUE en format csv.

## Connexion normale

L'administrateur peut accéder au menu système en cliquant droit sur le fond bleu.

Lorsque vous êtes logué en tant qu'administrateur, des options supplémentaires sont accessibles dans ce menu.

Un contour noir entourant la fenêtre montre que l'utilisateur courant est un administrateur.

Dans IntraVUE 2.0, le mot de passe de l'administrateur est le même que celui du serveur Apache Tomcat.

## Changement du mot de passe administrateur

Le mot de passe est renseigné dans un fichier du répertoire d'installation d'IntraVUE. Dans le fichier User.xml se trouvant par défaut sous C:\Program Files \IntraVUE \AutoIP \tomcat6 \conf.

Recherchez la balise XML commençant par "user" et contenant l'utilisateur "admin".

```
<user username="admin" password="IntraVUE" roles="admin,manager" />
```

**Éditez ce fichier et changez le mot de passe par défaut : "IntraVUE".**

**La sécurité par mot de passe permet de limiter l'accès à l'hôte IntraVUE.** IntraVUE permet une administration à distance sans avoir besoin de droits particulier sur le serveur IntraVUE. Les répertoires de configuration ne sont pas accessibles via l'interface Web.

## Ajoutez un utilisateur et un mot de passe à IntraVUE

Le serveur Web Apache permet de configurer un mot de passe pour accéder à l'interface d'IntraVUE.

La 1ère étape est d'ajouter des données dans le fichier ...\\IntraVUE\\AutoIP\\tomcat6\\webapps\\iv2\\WEB-INF\\web.xml. Copiez les lignes ci-dessous et insérez-les à la fin du fichier, juste avant la ligne de fin </web-app>

```
<!-- Define a Security Constraint on this Application -->
<security-constraint>
  <web-resource-collection>
    <web-resource-name>IntraVUE Application</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <!-- NOTE: This role is not present in the default users file -->
    <role-name>IntraVUE</role-name>
  </auth-constraint>
</security-constraint>
<!-- Define the Login Configuration for this Application -->
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>IntraVUE Application</realm-name>
</login-config>
<!-- Security roles referenced by this web application -->
<security-role>
  <description>The role that is required to log in to the IntraVUE Application </description>
  <role-name>IntraVUE</role-name>
</security-role>
</web-app> NOTE: do not copy this line. Insert just before this line in the file
```

Le code ci-dessus, va demander à l'utilisateur de se connecter avec le 'role-name' "IntraVUE". Ces 'role-name' sont définis dans le fichier tomcat-users.xml, décrit ci-dessus. Le rôle «IntraVUE» est déjà défini dans ce fichier et a un nom d'utilisateur d'IntraVUE et un mot de passe : IntraVUE.

Par conséquent, vous devez modifier le fichier tomcat-users.xml et ajouter un nouveau rôle. Les deux lignes ci-dessous peuvent être ajoutées à ce fichier pour créer un nouveau rôle nommé «remote» avec pour ce rôle a un nom d'utilisateur "remoteUser" et un mot de passe "IntraVUE2"

```
<role rolename="remote"/>
<user username="remoteUser" password="IntraVUE2" roles="remote"/>
```

Pour compléter le processus, redémarrez le service Windows "Apache Tomcat eTomcat".

Toutes les connexions vont nécessiter un nom d'utilisateur et un mot de passe

## Configuration des équipements

Ce menu de configuration est accessible par un clic droit sur un nœud.

Copy
Cut
Paste
Delete
Add Child
Move
Event Log...
Threshold Graphs...
SNMP Data...
Properties...
Configure...
Installation Manual
AutoIP Interface



NOTE : Copier, couper et coller n'est pas fonctionnel en version 2.0

**Copier** sauvegardera les réglages dans le presse-papier.

**Couper** même comportement que Copier mais l'équipement sera également supprimé.

**Coller** copiera les données du presse-papier vers l'équipement sélectionné excepté l'adresse IP, MAC et les réglages vérifiés par l'administrateur.

**Add Child** insère manuellement un nœud sous l'équipement sélectionné. Ces équipements ont "N/A" comme nom par défaut sur toutes les vues. Ce nom est en majuscules afin d'éviter les confusions avec les nœuds insérés automatiquement. Un lien de couleur noir va donc apparaître entre les équipements.

**Move** déplace les nœuds sélectionnés sous le nœud où vous avez appelé ce menu.

**Configure** affiche le menu de configuration équipement qui permet d'éditer les réglages, créer les liens web et ajouter des images.

Toutes les autres options sont les même qu'en mode utilisateur classique.

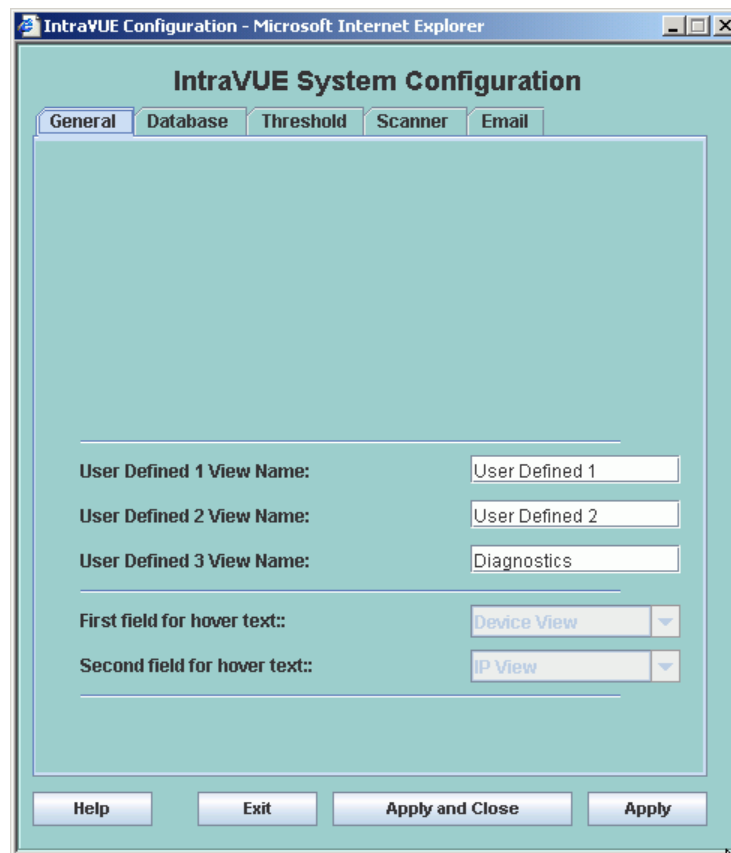
Comme le menu "Equipement" pour les utilisateurs classiques, les liens web sont affichés en bas du menu.

## Configuration Système

L'item "System configuration" autorise à l'administrateur uniquement la configuration d'IntraVUE. Il est donc indispensable d'être identifié en tant qu'administrateur pour accéder à ce menu.

Vous devez absolument être connecté en tant qu'administrateur pour accéder à ce menu

## Configuration Système - Onglet General

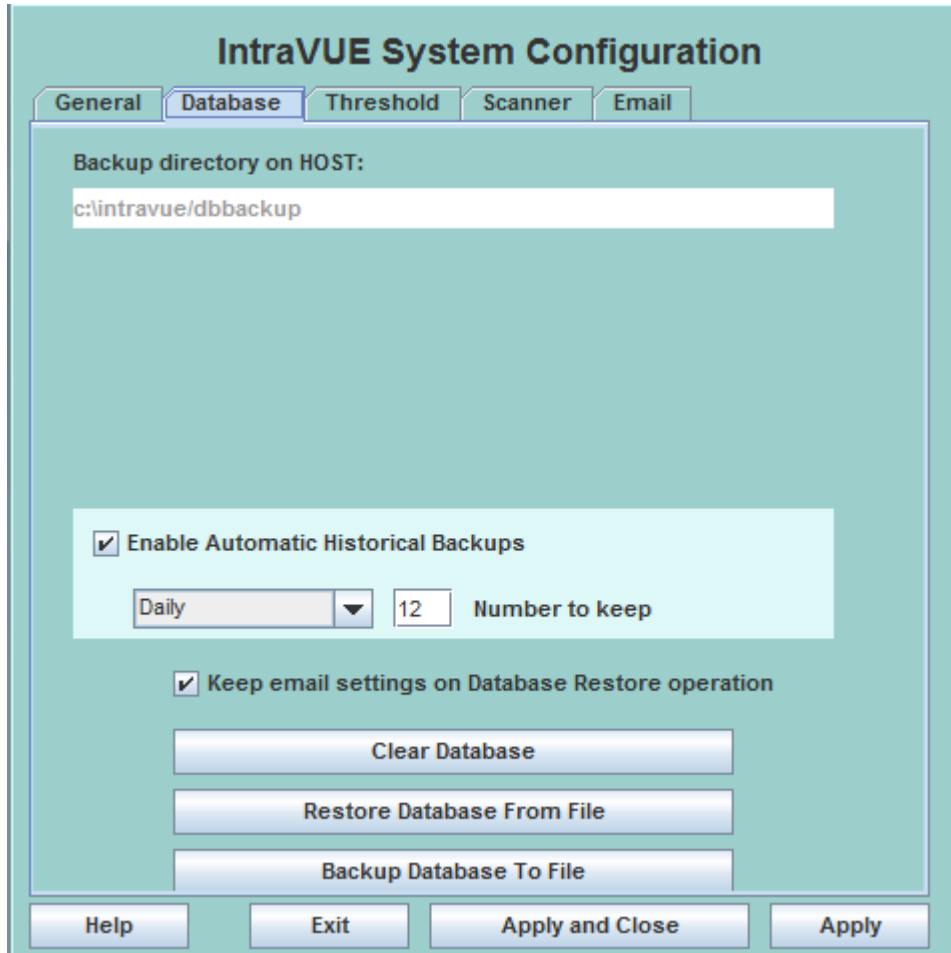


La partie supérieure de cet onglet montre les informations de licence, La version IntraVUE qui est installée, le nombre de nœuds ont été retrouvés et le nombre de nœuds de la licence IntraVUE.

Au milieu de l'onglet se trouve le nom des 3 vues personnalisables. Ces noms apparaissent dans l'interface d'IntraVUE, le « menu système », et le « device configuration ».

En bas de l'onglet, il est possible de choisir le nom de la vue à afficher lors du passage de la souris (en info bulle). Cette fonctionnalité sera active en version 2.1

## Configuration Système - Onglet Database



The screenshot shows the 'IntraVUE System Configuration' dialog box with the 'Database' tab selected. The 'Backup directory on HOST:' field contains the path 'c:\intravue/dbbackup'. Below this, there is a checked checkbox for 'Enable Automatic Historical Backups'. Underneath, a dropdown menu is set to 'Daily' and a text box contains the number '12', with the label 'Number to keep' to its right. There is also a checked checkbox for 'Keep email settings on Database Restore operation'. At the bottom of the dialog, there are three buttons: 'Clear Database', 'Restore Database From File', and 'Backup Database To File'. The bottom-most row of the dialog contains four buttons: 'Help', 'Exit', 'Apply and Close', and 'Apply'.

Dans la partie supérieure de l'onglet, vous avez le chemin du dossier où IntraVUE va stocker les sauvegarde de la base de données MySQL.

Les sauvegardes automatiques de la base de données permettent de garder des sauvegardes régulièrement sans aucune action de l'opérateur. Il est possible de les planifier chaque jour, chaque semaine ou chaque mois. Ainsi que le nombre de sauvegardes gardées.



Note : Une fois le nombre de sauvegarde atteint, la plus ancienne est efface et ainsi de suite.

La partie basse permet d'effectuer 3 opérations majeures sur la base de données :

- Vider la base de données et restaurer les paramètres par défaut d'IntraVUE.
- Restaurer les bases de données sauvegardées précédemment et écraser les paramètres courants.
- Sauvegarder la base de données sous un nom paramétrable.



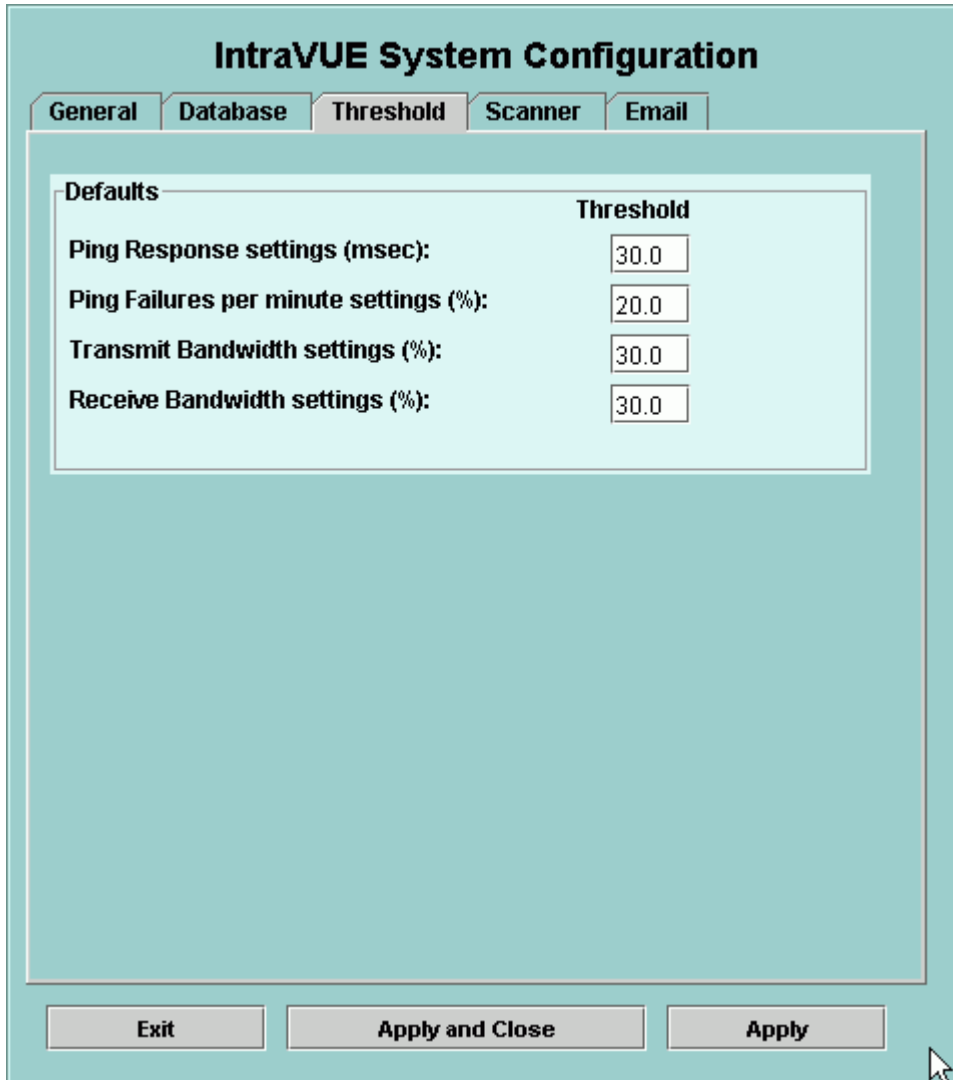
Note : il n'est pas nécessaire d'arrêter IntraVUE pour appliquer ces modifications.

Après la restauration de la base de données, une boîte de dialogue permet de passer mode off-line. Dans le mode off-line, le scanner d'IntraVUE ne modifie pas cette base de données. Si vous restaurez une base de données issue d'une version antérieure d'IntraVUE vous devez absolument passer en mode off-line.

Si vous avez déjà sélectionné le mode off-line et que vous voulez passer en on-line, restaurez la base de données à nouveau et ne sélectionnez pas le mode off-line.

---

## Configuration Système - Onglet Threshold



The screenshot shows the 'IntraVUE System Configuration' window with the 'Threshold' tab selected. The window has a title bar and five tabs: 'General', 'Database', 'Threshold', 'Scanner', and 'Email'. The 'Threshold' tab is active and contains a table with the following data:

Defaults	Threshold
Ping Response settings (msec):	30.0
Ping Failures per minute settings (%):	20.0
Transmit Bandwidth settings (%):	30.0
Receive Bandwidth settings (%):	30.0

At the bottom of the window, there are three buttons: 'Exit', 'Apply and Close', and 'Apply'.



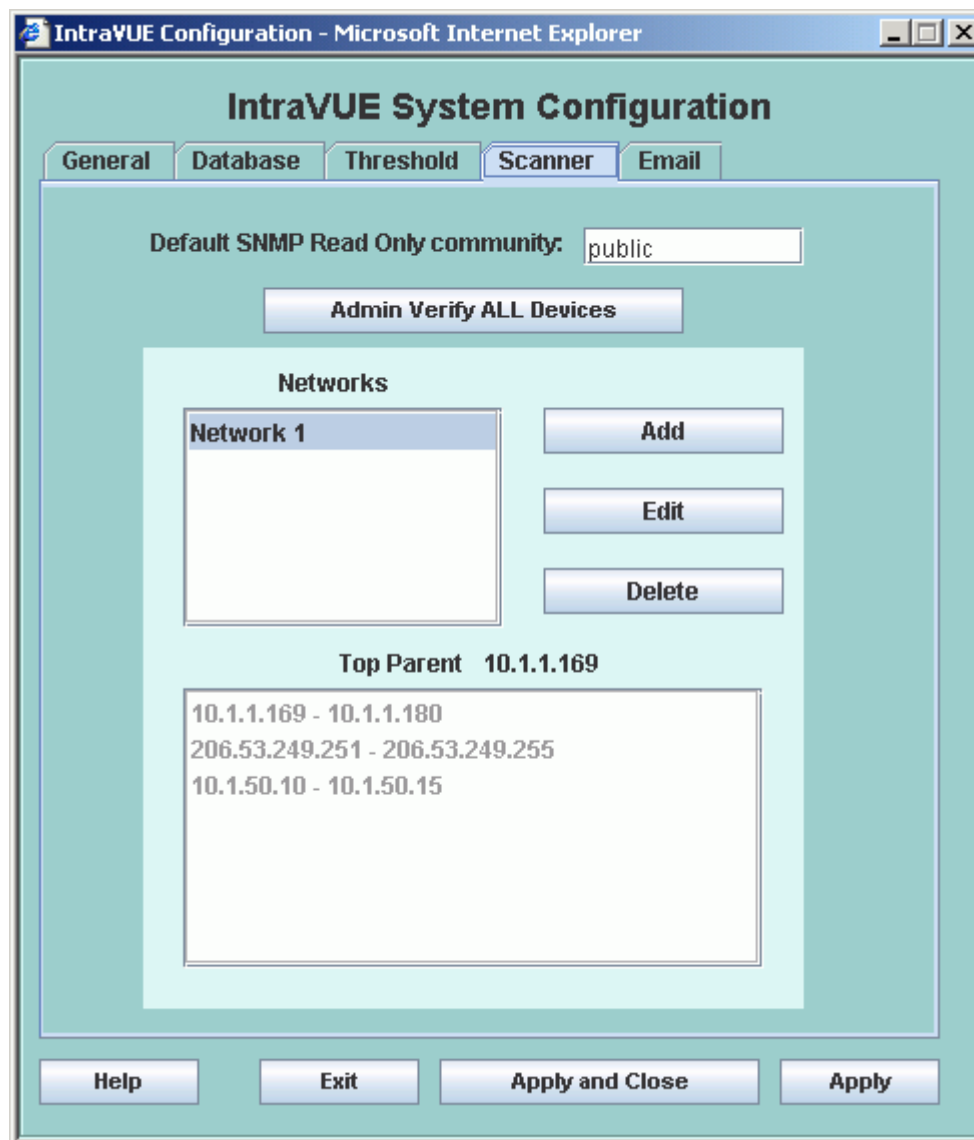
Note : Ces paramètres ne seront accessibles qu'à partir de la version 2.1 d'IntraVUE.

Lorsqu'un équipement est découvert, ces paramètres initiaux de configuration des seuils sont appliqués.

Une fois l'équipement découvert, il est toujours possible de modifier individuellement par un clic droit sur le lien.

## Configuration Système - Onglet Scanner

L'onglet "Scanner" permet de configurer les réseaux et les plages d'adresses IP à surveiller grâce à IntraVUE.



Dans la partie supérieure se trouve le nom de la communauté SNMP par défaut. Si vous n'êtes pas familier avec le protocole SNMP, vous pouvez assimiler cela à un mot de passe.



Note : IntraVUE accède aux informations SNMP uniquement en lecture, il n'écrit jamais de données SNMP.

Dans la partie supérieure se trouve le bouton "Admin verify all devices" permet de vérifier tous les équipements en une seule opération. Toutes les boîtes passent donc en fond bleu.

La vitesse du scanner d'IntraVUE peut être ajustée.

- SLOW - 60 Milliseconde écart entre chaque paquet sortant et une limite de 20 ARP par cycle de balayage .
- MEDIUM - écart de 15 millisecondes et une limite de 64 ARP
- FAST – écart de 4 millisecondes et une limite de 64 ARP
- ULTRA - écart de 1 milliseconde et une limite de 64 ARP.

Trois boutons permettent d'ajouter, d'éditer ou de supprimer des réseaux.

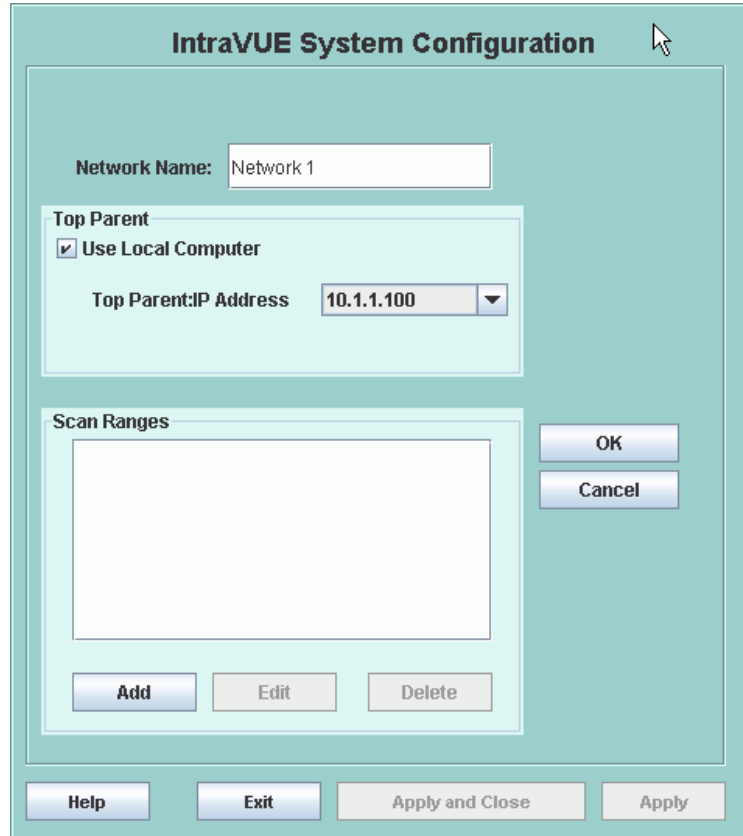
*La suppression d'un réseau ou la modification de la plage d'adresse n'entraîne pas de suppression des équipements dans la base de données d'IntraVUE. L'historique des événements est présent dans la base de données pour les équipements découverts par le scanner et affichés dans la topologie du réseau. Vous devez supprimer manuellement les équipements que vous ne voulez pas voir dans l'architecture. Pour effacer totalement les historiques d'un réseau, utilisez le bouton « Clear Database »*

#### **Note à propos des communautés SNMP**

La communauté SNMP pour un périphérique ne sera pas définie jusqu'à ce que la communication SNMP soit un succès pour ce périphérique. Vous pouvez fixer par défaut la valeur des switches et laisser tous les switches être découverts et ensuite paramétrer une autre communauté. À la fin, nous recommandons de laisser à l'ensemble de la communauté «public», le SNMP par défaut, qui s'appliquera à la plupart des appareils nouvellement découverts.

## Ajouter un réseau dans IntraVUE

Cliquez sur le bouton Add. Si vous avez des VLAN, vous devez lire le chapitre « Les VLAN - Virtual Local Area Network » avant de continuer.

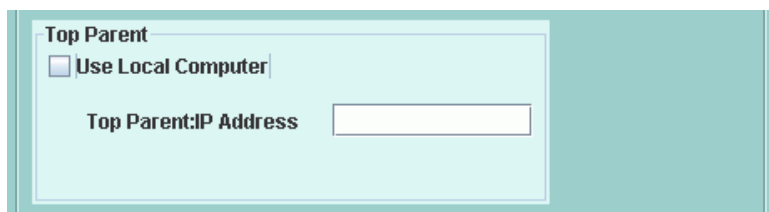


Lors de l'ajout ou de la modification d'un réseau, il est possible de lui spécifier un nom. Ce nom doit être unique.



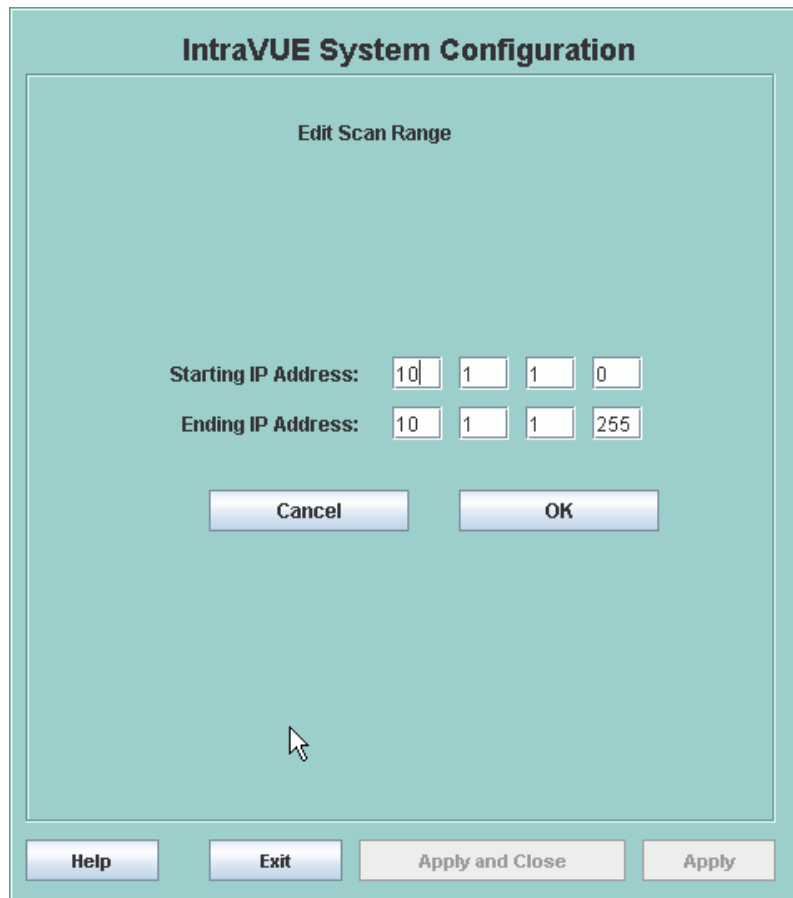
Note : Il est impossible de changer le « Top parent » une fois le réseau configuré.

La case “Use local Computer” est à cocher dans 90% des cas. Si cette case est cochée, une liste déroulante apparaît avec les adresses IP locales de la machine hôte (Une pour chaque carte réseau). Pour plus de détails consultez le chapitre Sélectionner le Top Parent.



Si cette case n'est pas cochée, il est possible d'entrer manuellement l'adresse IP d'un routeur. Un routeur est l'unique autre équipement qui peut être sélectionné comme « Top parent ». Le Top Parent est un équipement qui possède la table ARP ou les adresses MAC des équipements à surveiller.

Une fois le « Top parent » renseigné, cliquez sur « Add » dans le « Scan range » pour ajouter une plage d'adresses IP à surveiller.



Une plage d'adresses IP peut contenir une seule adresse en entrant la même adresse deux fois.

Exemple : Surveiller uniquement le 10.1.1.100

Adresse de début : 10.1.1.100

Adresse de fin : 10.1.1.100

Exemple 2 : Surveiller tout sauf le 10.1.1.100

Adresse de début : 10.1.1.0

Adresse de fin : 10.1.1.99

Adresse de début : 10.1.1.101

Adresse de fin : 10.1.1.255



Note: Si votre ordinateur possède plusieurs cartes NIC, une seule doit être dans la gamme de balayage.

## Les VLAN - Virtual Local Area Networks

Les VLAN fournissent un moyen de grouper des dispositifs comme s'ils étaient les seuls dispositifs dans un sous réseau.

Les VLAN sont configurés avec des switchs de niveau 2

Le trafic de diffusion au sein d'un VLAN n'est pas diffusé à des appareils en dehors du réseau local virtuel même si elles sont attachées au même switch. C'est l'un des principaux avantages d'un VLAN. Il peut empêcher les équipements de voir le trafic de diffusion d'autres appareils, y compris ARP.

Si deux périphériques sont connectés au même switch de niveau 2, mais qu'ils sont dans différents réseaux locaux virtuels, le trafic physique entre les deux appareils doit Voyager du switch de couche 2 vers tout autre switch jusqu'à ce qu'il atteigne un routeur, Ce dernier envoie le trafic vers le bas dans le même câble jusqu'au switch de niveau 2 d'origine. Là, le trafic est envoyé au port de l'appareil sur l'autre VLAN.

Un Power Point de présentation, au format html, explique visuellement les VLAN et IntraVUE (Lorsque vous exécutez le fichier choisissez "ouvrir" avec votre navigateur et vous devez autoriser le contenu actif).

Cette présentation se trouve sous :

IntraVUE\AutoIP\tomcat6\webapps\ROOT\help\fr\images\VLAN2.mhtml

## Sélectionner le Top Parent

### Qu'est-ce qu'un Top Parent?

Chaque 'réseau' IntraVUE est un regroupement logique d'équipements selon les besoins de l'utilisateur. Chaque réseau IntraVUE consiste à paramétrer des adresses à scanner et un Top Parent.

Seul 2 équipements peuvent être des Top Parent: le PC Hôte et un router pour lequel la communauté SNMP est connue.

#### Définitions:

Le **Top Parent** IntraVUE d'un réseau est l'appareil qui peut fournir la MAC adresses pour les appareils de la gamme de balayage.

**Local** : tous les appareils du même sous réseau que l'hôte IntraVUE en terme d'adresse IP. Local est déterminé par l'adresse IP de ordinateur ou se trouve l'application, ainsi que par son masque de sous réseau. Les Pings aux adresses IP vont directement à l'appareil et les adresses MAC seront stockées dans le cache ARP de l'ordinateur hôte. Un calculateur en ligne de sous réseau est utile si vous avez des masques de sous réseau peu courant. [www.subnetonline.com](http://www.subnetonline.com) et [www.subnetmask.info](http://www.subnetmask.info) en sont deux exemples

**Remote**: tous les dispositifs PAS dans le même sous réseau que l'hôte IntraVUE en terme adresse IP. Les pings et d'autres informations de trafic pour les équipements distants quitteront le sous réseau local pour aller à la passerelle par défaut (un routeur) si il est configuré. La passerelle utilisera ses tables de routage pour diriger le trafic d'une de ses interfaces ou de ses gateway si elle ne dispose pas d'une interface appropriée.

#### Les règles générales pour la détermination du 'top parent':

- L'ordinateur hôte de IntraVUE doit être le top parent si **tous** les appareils du réseau IntraVue sont locaux à l'hôte. Ceci parce que les adresses MAC seront dans le cache ARP de l'hôte suite aux pings du scanner.
- Les adresses MAC de tous les périphériques qui ne sont pas «locales» à l'ordinateur hôte IntraVUE seront dans un routeur. Elles seront dans le dernier routeur menant à un dispositif, le «last hop router». Si tous les dispositifs dans un réseau IntraVUE sont distants, le last hop router doit être Top Parent de ce réseau. (Le last hop router peut être déterminée à l'aide de l'outil de ligne de commande DOS "tracert ipaddress").
- Un routeur à seulement besoin d'être dans un réseau IntraVUE pour trouver les adresses MAC de tous les autres réseaux IntraVUE. Mettre le routeur dans son propre réseau IntraVUE sans autres appareils est une méthode pour faire cela.
- L'adresse IP du Top Parent d'un réseau doit être incluse dans l'une des plages d'adresses IP pour ce réseau.

Encore une fois, le **top parent** de chaque réseau IntraVUE est le dispositif qui a accès à l'adresse MAC des dispositifs qui seront à sa gamme de balayage (s).

Le scanner va tenter d'identifier les routeurs qui se trouvent dans une gamme de balayage et le scanner va essayer d'obtenir des adresses MAC à partir de n'importe quel routeur qu'il trouve.

Si un réseau IntraVUE a certains périphériques qui sont locaux et certains périphériques qui sont à distance, l'ordinateur hôte doit être le top et une (et seulement une) des adresses IP des routeurs doit être dans une gamme de balayage.

Si vous avez des VLAN alors chaque VLAN doit être dans un réseau IntraVUE. Cela permet d'indiquer clairement la voie de circulation nécessaire pour passer d'un périphérique à un autre.

Si les switches sont séparés dans un VLAN, la plage d'adresses IP peuvent être ajoutées aux autres gammes de VLAN. Ainsi, chaque réseau IntraVUE aura les switches et montrera comment les périphériques sont connectés. Les switches qui ne sont pas utilisées dans un VLAN peuvent ensuite être supprimés de ce réseau IntraVUE.

## Exemple:

S'il y a un routeur et de nombreux réseaux locaux virtuels et que vous souhaitez scanner ces VLAN, faire de l'adresse IP du routeur le Top Parent de chaque réseau. Chaque réseau aura alors deux gammes de balayage - une seule pour l'IP du routeur et une pour la gamme de dispositifs, SAUF l'IP du routeur dans cette gamme. Par exemple:

L'hôte IntraVUE 10.1.1.35.

Le Router a les adresses IP 10.1.1.1, 10.1.2.1, 10.1.3.1, et 192.168.1.254.

Vous voulez scanner toutes ces classes C

Réseau 1

top parent 10.1.1.35 (local host pour trouver les adresses MAC des équipements locaux)  
range 10.1.1.0 - 10.1.1.255 (comprend le router 10.1.1.1 et le top parent)

Réseau 2

top parent 10.1.1.1  
range 10.1.1.1 - 10.1.1.1 (le top parent doit être dans la gamme du scanner)  
range 10.1.2.2 - 10.1.2.255 (exclure l'adresse du routeur 10.1.2.1 )

Réseau 3

top parent 10.1.1.1  
range 10.1.1.1 - 10.1.1.1 (le top parent doit être dans la gamme du scanner)  
range 10.1.3.2 - 10.1.3.255 (exclure l'adresse du routeur 10.1.3.1 )

Réseau 4

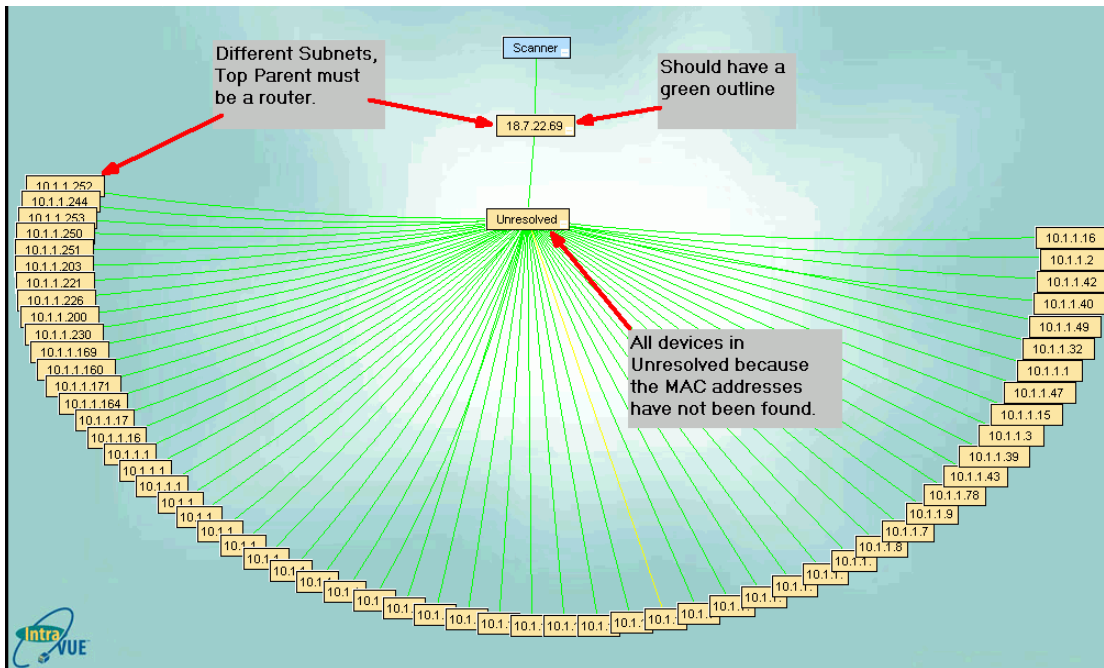
top parent 10.1.1.1  
range 10.1.1.1 - 10.1.1.1 (le top parent doit être dans la gamme du scanner)  
range 192.168.1.1 - 192.168.1.253 (exclure l'adresse du routeur 192.168.1.254)

Le but de ce qui précède est d'éviter les demandes inutiles du scanner sur le même routeur physique lorsque le routeur va répondre exactement la même chose quelle que soit l'ip /interface que vous utilisez.

SI VOUS SCANNEZ DES DISPOSITIFS LOCAUX A L'ORDINATEUR HOTE, l'hôte est le SEUL appareil qui peut être le Top Parent. Ceci parce l'hôte aura les adresses MAC des dispositifs à partir du scanner Ping.

## Problèmes Top Parent

Si vous ne sélectionnez pas le bon Top Parent, ou si le Top Parent n'est pas configuré pour utiliser correctement le SNMP, vous obtiendrez une représentation proche de l'image ci-dessous dans le navigateur.



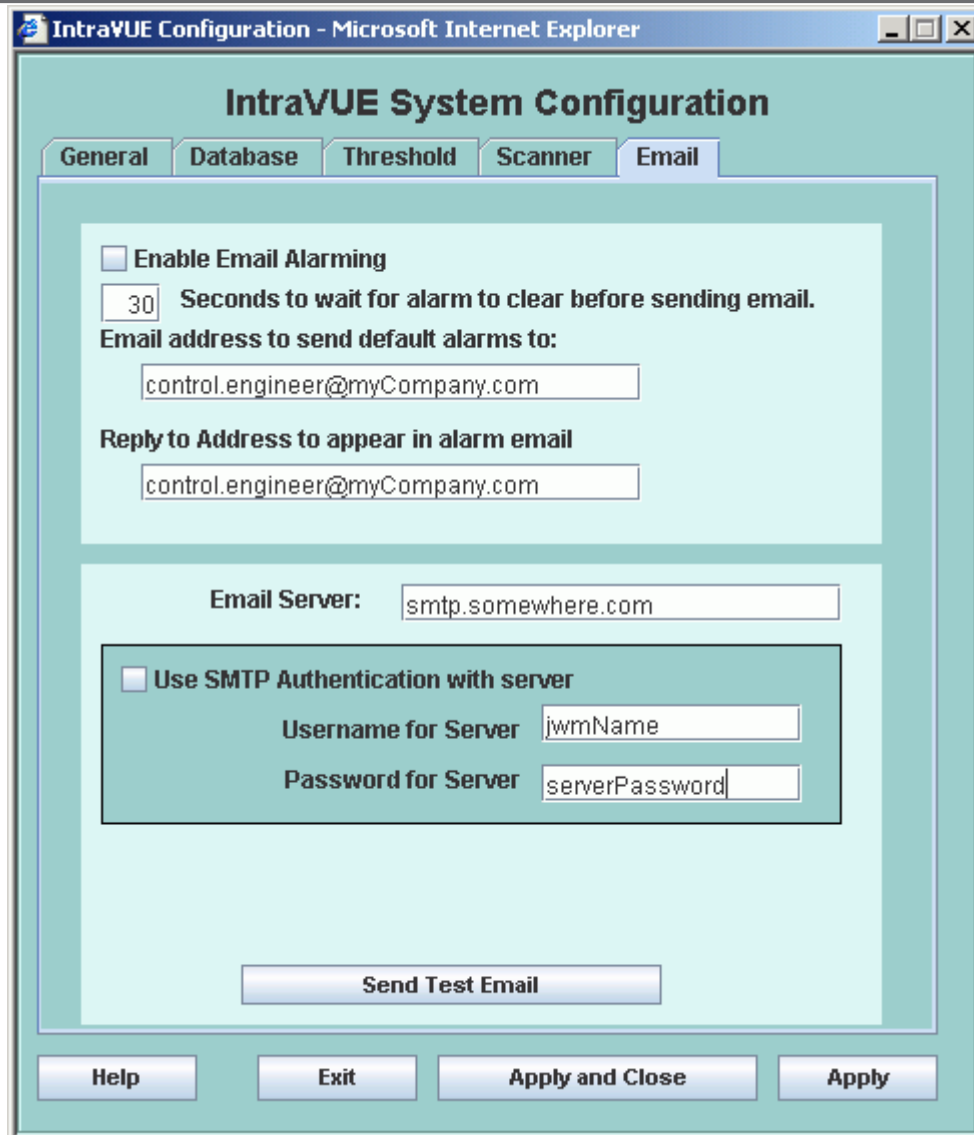
Si le Top Parent n'est pas le PC local, il doit s'agir d'un ROUTEUR car les routeurs sont des équipements qui donnent l'adresse MAC lorsqu'ils fournissent une adresse IP. Dans l'image, le Top Parent est dans une gamme d'adresse IP différente de l'équipement qu'il scanne. C'est un indice permettant de définir que le Top Parent doit être un routeur.

Dans l'image il n'y a pas contour vert autour du nœud du Top Parent. Si l'IP du Top Parent correspond à un routeur, alors la communauté SNMP n'est pas correcte ou le routeur est configuré avec une liste de contrôle d'accès et le l'hôte d'IntraVUE n'est pas dans la liste.

Si le Top Parent n'est pas le PC local, il doit avoir un contour vert qui indique que la communauté SNMP est correcte pour le routeur qui contient les adresses MAC des équipements de la gamme de recherche.

## Configuration Système - Onglet Email

La case à cocher "Enable Email alarming" doit être cochée pour activer l'envoi d'alarmes par email. Actuellement, chaque équipement va générer un email pour chaque équipement configuré de la sorte.



Le champ “seconds to wait” spécifie le temps d’attente entre l’apparition de l’alarme et l’envoi de l’email correspondant. A la fin de ce délai, IntraVUE contrôle si l’alarme est toujours présente et envoie l’email. La valeur par défaut est 30 secondes.

Le champ « email address to send » précise quelle adresse sera utilisée pour l’envoi d’emails.

Le champ « reply to address » peut être utilisé lorsque le serveur SMTP l’exige. Cette adresse peut être valide ou pas selon votre serveur SMTP.

La dernière partie de cette fenêtre contient les données d’identification du serveur SMTP utilisé pour l’envoi d’email. Le serveur IntraVUE doit pouvoir accéder à ce serveur.

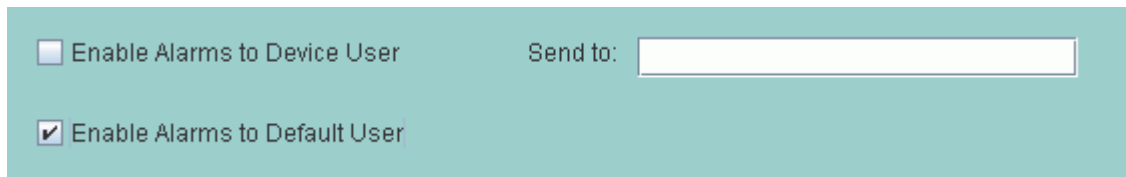
Enfin, un bouton de test permet d’envoyer immédiatement un mail de test avec les paramètres enregistrés dans la base de données. Si ces paramètres ont été modifiés, cliquez sur « Apply » avant de lancer ce test.

Le bouton **Send Test Email** génère immédiatement un message de test en utilisant les paramètres **DANS LA BASE DE DONNÉES**. **Si vous apportez une modification, sélectionnez le bouton Appliquer**

**avant de sélectionner Envoyer un message de test.** Cette fonctionnalité évite d'avoir à débrancher un appareil juste pour tester les paramètres de votre email.

Dans la boîte de dialogue du "Device Configuration", une case à cocher "Enable Alarms to default user" permet d'activer l'envoi d'email à l'adresse configurée précédemment. Par défaut cette case n'est pas cochée.

Une case à cocher supplémentaire « Enable Alarms to device user » permet de spécifier une adresse spécifique à l'équipement sélectionné.



Enable Alarms to Device User      Send to:

Enable Alarms to Default User

Lorsque vous utilisez le bouton test E-mail et que vous ne recevez pas de réponse, il y aura un texte dans un message d'exception indiquant la cause précise de la panne. Par exemple, refusée par hôte SMTP, un nom d'utilisateur ou mot de passe incorrect, etc.

Ce message se trouve dans le fichier journal du scanner situé sous ...\\IntraVUE\\log et sera nommé ivserver\_(date)\_(heure).out au moment où vous avez appuyé Test Email.

Un échantillon de ce qui est produit est présenté ci-dessous. Il a été généré en faisant un essai avec les paramètres par défaut. Le stacktrace ligne "javax.mail.MessagingException: Unknown SMTP host: smtp.somewhere.com;" vous indique que le serveur SMTP, le fournisseur de services de messagerie, est erronée ou que vous ne pouvez vous connecter à lui

```
0120 100016 event: Device 10.1.1.67 reconnected
0120 100054 event: Device 10.1.1.90 moved from 10.1.1.244:9 to 10.1.1.16:2
0120 100054 event: deleted child node at 10.1.1.244:9
0120 100111 event: 10.1.1.32 Ping Response Threshold Exceeded
0120 100122 received mod request send test email 0 0
0120 100122 send test email
0120 100123 EmailTask runs: IntraVUE has been instructed by the admin to send a test email. Please see
http://10.1.1.59:8765/
to [unused]
0120 100123 Unexpected Exception thrown - stacktrace follows:
javax.mail.MessagingException: Unknown SMTP host: smtp.somewhere.com;
nested exception is:
java.net.UnknownHostException: smtp.somewhere.com
at com.sun.mail.smtp.SMTPTransport.openServer(SMTPTransport.java:1211)
at com.sun.mail.smtp.SMTPTransport.protocolConnect(SMTPTransport.java:311)
at javax.mail.Service.connect(Service.java:233)
at javax.mail.Service.connect(Service.java:134)
at javax.mail.Service.connect(Service.java:86)
at com.sun.mail.smtp.SMTPTransport.connect(SMTPTransport.java:144)
at javax.mail.Transport.send0(Transport.java:150)
at javax.mail.Transport.send(Transport.java:80)
```

```
at database.EmailTask.run(EmailTask.java:76)
at java.util.TimerThread.mainLoop(Unknown Source)
at java.util.TimerThread.run(Unknown Source)
0120 100146 device 10.1.1.67 disconnected
0120 100146 event: Device 10.1.1.67 disconnected
0120 100207 device 10.1.1.90 reconnected
```

### Personnalisation du message électronique

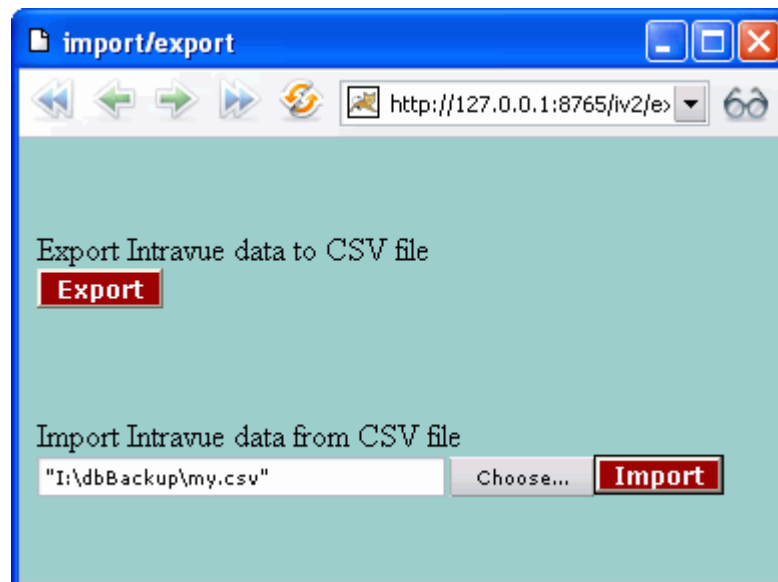
Le message qui est envoyé à l'utilisateur peut être personnalisé en utilisant des options du fichier `ivserver.properties` qui se trouve sous `IntraVUE\AutoIP`.

- Le sujet de l'e-mail peut être personnalisé pour inclure le nom du périphérique
- Au corps du message pour un périphérique déconnecté peut être ajouté le nom du périphérique et un lien.
- L'adresse IP utilisée pour fournir un lien vers l'hôte IntraVUE peut être modifiée pour permettre aux utilisateurs d'utiliser une adresse proxy plutôt que la véritable adresse de l'hôte pour atteindre le navigateur IntraVUE.

## Section 4.5

## Import / Export

L'import Export est accessible par le " menu Système ".



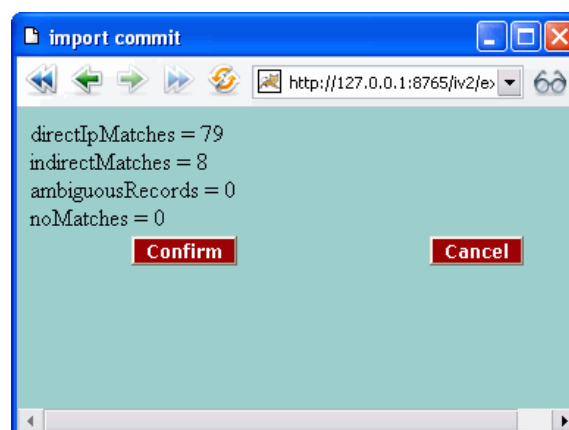
### Export

Le bouton "export" permet d'exporter toute la configuration d'IntraVUE dans un fichier au format csv exploitable par Microsoft Excel ou par tout autre éditeur compatible.

Le champ "Choose" permet de spécifier le chemin d'accès au fichier à importer et le bouton d'importer le fichier dans la base de données d'IntraVUE.

### Import

Le bouton "import", va lancer l'importation des fichiers sélectionnés.



Les données importées sont basées sur l'adresse IP présente dans le fichier csv. Ce qui permet d'importer un fichier en provenance d'un autre IntraVUE.

Si IntraVUE n'arrive pas à identifier l'équipement par son adresse IP, celui-ci va rechercher le switch sur lequel il est connecté et son numéro de port.

Dans la majorité des cas, seul les équipements manuellement insérés ou déplacés peuvent ne pas être identifiés par IntraVUE.

Enfin sélectionnez le bouton « Confirm » pour valider l'import.

## Spreadsheet Notes

Lorsque vous regardez les données exportées vous trouverez plusieurs colonnes. Il y a 3 sections de base:

- Référence data
- Données de configuration pour chaque vue IntraVUE
- Données de configuration pour l'onglet général des équipements



L'export génère beaucoup de colonnes et vous pouvez supprimer celles qui ne vous intéressent pas SAUF les 8 premières (colonnes A à H). Ces colonnes sont utilisées lors de l'import. Vous ne devez pas changer la valeur dans ces colonnes. Elles sont représentées ci-dessous.

- IP - l'adresse IP ou n/a si la ligne représente un nœud inséré automatiquement.
- Active - 1 Si l'équipement est actuellement connecté.
- MAC - Adresse MAC.
- Ref - numéro interne de référence.
- ParentRef - numéro interne de référence de l'équipement parent.
- ParentIP - Adresse IP de l'équipement parent. Il s'agit d'un switch, router ou du Top Parent du réseau IntraVUE.
- ParentPort - Le numéro de port de l'équipement parent.
- UlinkPort - Si le parent est un switch, le UlinkPort est le port relié au Top Parent. Sinon 0.

C'est particulièrement pratique pour trier les données exportées par adresse IP du parent et ensuite par port du parent. Ceci vous donnera la liste de tous vos équipements classés par switch sur lequel ils sont connectés et par ordre de port. Particulièrement utile lorsque vous souhaitez comparer ce que dit IntraVUE avec ce que dit votre documentation.

La section suivante contient les colonnes pour les noms, liens web et images. Il n'y a pas de sous-section pour chacune des 6 vues d'IntraVUE; Notez qu'il n'y a pas de colonne pour la vue d'adresse IP car vous ne pouvez pas la changer.

- \_\_\_ViewName - Le nom qui apparaît dans la vue.
- \_\_\_ViewWeblink1Title - Le nom qui apparaît dans le sélecteur.
- \_\_\_ViewWeblink1URL - url qui va être appelée lorsque l'utilisateur clic sur le lien.
- \_\_\_ViewWeblink2Title
- \_\_\_ViewWeblink2URL
- \_\_\_ViewIconImage - icone à afficher dans la vue.
- \_\_\_ViewThumbnailImage - image à afficher dans la vue.

La dernière section contient des informations de l'onglet général de configuration équipement.

- Category
  - Auto Connect
  - AutoBootp
  - IsWireless - Correspond à la case à cocher WAP.
  - Send Alarms - Pour cet équipement spécifique.
  - AlarmEmailAddress - email pour cet équipement spécifique.
  - SendToDefaultUser- email par défaut configuré dans la boîte de dialogue System Configure sous l'onglet Email.
  - Verified - Vérifié par l'administrateur.
  - Properties - Une encapsulation de plusieurs éléments de l'onglet général des équipements. Cette colonne ne doit pas être éditée mais peut être copiée d'un équipement configuré vers un autre équipement non configuré. Elle inclue des informations comme 'disable all snmp', 'ignore bridge mib', 'use snmp for mac', et la communauté snmp.
-

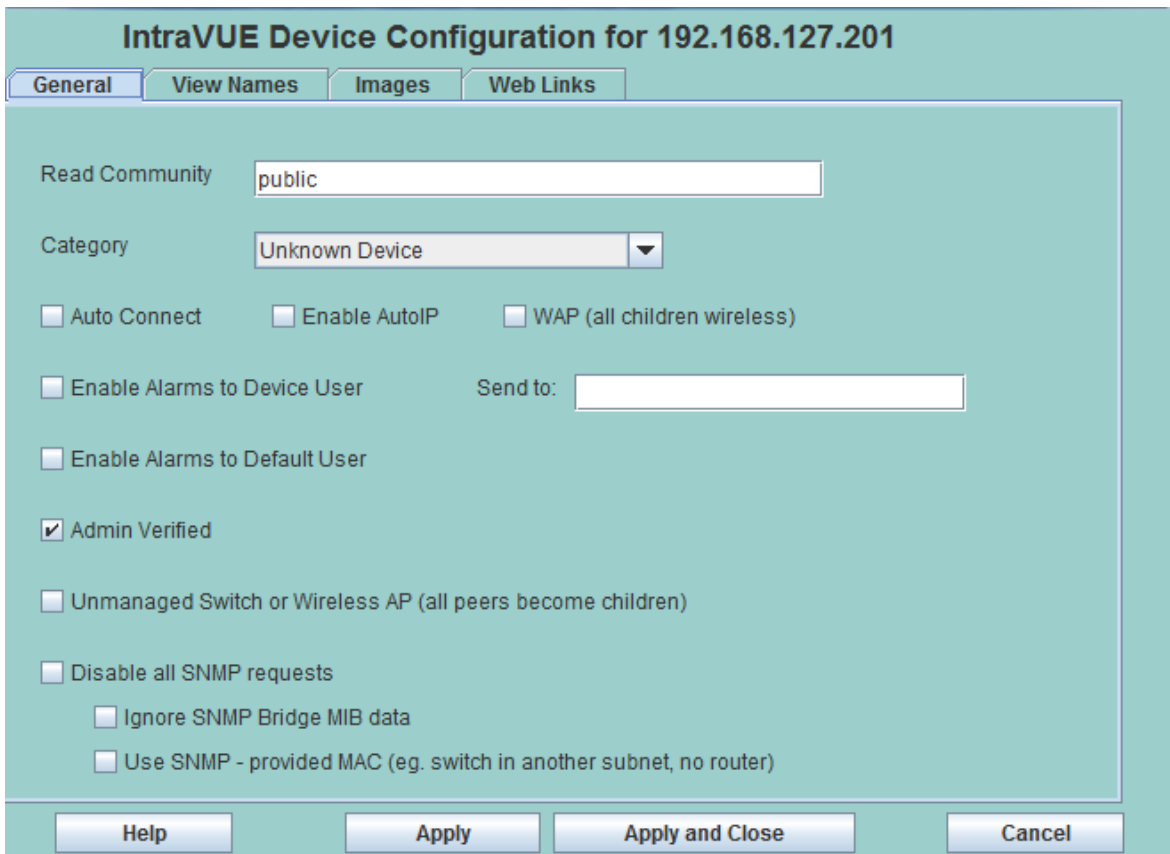
## Configuration des équipements

La configuration des équipements possède 4 onglets qui permettent de configurer les propriétés de l'équipement.

- L'onglet General contenant la vérification administrateur, sans-fil, SNMP et email.
- L'onglet View Names permet de configurer le nom des équipements sur chaque vue.
- L'onglet Images permet d'assigner une miniature et une icône pour chaque vue.
- L'onglet Web Links permet de configurer 2 liens web par équipement.

## Configuration des équipements - Onglet General

Cet onglet fixe les propriétés générales de chaque équipement.



The screenshot shows the 'IntraVUE Device Configuration for 192.168.127.201' window with the 'General' tab selected. The configuration options are as follows:

- Read Community:
- Category:  (dropdown menu)
- Auto Connect
- Enable AutoIP
- WAP (all children wireless)
- Enable Alarms to Device User
- Send to:
- Enable Alarms to Default User
- Admin Verified
- Unmanaged Switch or Wireless AP (all peers become children)
- Disable all SNMP requests
  - Ignore SNMP Bridge MIB data
  - Use SNMP - provided MAC (eg. switch in another subnet, no router)

Buttons at the bottom: Help, Apply, Apply and Close, Cancel.

En commençant par :

### Read Community

“Read community” renseigne la communauté SNMP à lire spécifiquement pour l'équipement sélectionné.

Cette valeur est fixée automatiquement une fois la connexion SNMP réussie en se basant sur la valeur disponible dans l'onglet SCANNER de la boîte de dialogue System Configuration.

### **Catégorie**

Permet de sélectionner la catégorie de l'équipement (Routeur, Switch...)

En version 2.1, IntraVUE sera capable de renseigner automatiquement ce paramètre.

### **Auto Connect**

Cette fonctionnalité fonctionne en corrélation avec la vérification de l'administrateur. Si c'est case est cochée, l'équipement pourra se déconnecter et se reconnecter dans créer de nœud avec un fond rouge.

Par exemple ce paramètre peut être utilisé avec les équipements wifi qui bougent sans cesse d'endroit. Lorsqu'un équipement de ce type se reconnecte au réseau, il devient vérifié automatiquement sans action de l'administrateur.

### **Enable AutoIP**

Cette case à cocher permet d'autoriser l'équipement à communiquer avec AUTO IP (Produit de l'offre IntraVUE, Contactez l'équipe commerciale pour plus de renseignements)

### **WAP (all children wireless)**

Ce paramètre change le type de ligne utilisé pour la connexion de l'équipement. Cette ligne devient en pointillé et utilise la couleur appropriée en fonction de son état. Cette option est cochée automatiquement si l'équipement est découvert comme un point d'accès sans fils (Wireless Access Point)

### **Enable Alarms to Device User**

En cochant cette case, les alarmes déclenchées par cet équipement seront envoyées à l'adresse spécifiée.

### **Send To**

Si cette case est cochée, les alarmes seront envoyées à l'adresse spécifiée dans le "Send to".

### **Admin Verified**

Lorsque cette case est cochée, la position de l'équipement est bloquée à sa position actuelle. Si l'équipement se déplace, IntraVUE va montrer un nœud sur fond rouge et une boîte orange à la position actuelle.

### **Unmanaged Switch or Wireless AP**



Lorsque différents équipements sont trouvés et positionnés sous une boîte N/A, cocher cette option sur un des équipements permet de positionner l'équipement en lieu et place de la boîte N/A. Les autres équipements deviennent alors les fils de cet équipement. Les machines virtuelles peuvent utiliser cette option pour être affichées sous le PC hôte.

### **Disable SNMP requests for this device**

Cette fonctionnalité sera présente en 2.1. Si cette case est cochée, IntraVUE n'interroge plus l'équipement sélectionné et vous pouvez renseigner manuellement les informations sur l'équipement.

### **Ignore SNMP Bridge Mib data**

Utilisez cette option pour manager les switchs avec une implémentation SNMP pauvre. Cette option est typiquement utilisée en conjonction avec l'option Unmanaged Switch or Wireless AP

### **Use SNMP provided MAC**

Cette option permet au Scanner de IntraVUE de récupérer l'adresse MAC d'un switch dans un sous-réseau différent sans avoir d'accès SNMP par le router de ce sous-réseau. De nombreuses installations ont seulement accès à leurs appareils locaux, mais pas aux autres switchs/routers dans des sous-réseaux différents. Ne fonctionne qu'avec les switchs

---

## Vérification Administrateur

La vérification Administrateur est un processus de création d'un "Etat contrôlé" de votre réseau, ou les dispositifs que vous contrôlez avec IntraVUE.

Chaque nœud vérifié par l'administrateur a des caractéristiques différentes d'un nœud non vérifié.

- le nœud a normalement un fond bleu
- Si la position d'un périphérique change, le nœud vérifié est alors affiché sur un fond rouge.
- la position réelle de l'appareil devient un nœud dont la couleur est jaune pale

Lorsque tous les périphériques d'un réseau sont vérifiés, les nœuds IntraVUE seront tous bleues. Certains peuvent avoir des lignes de raccordement jaunes ou rouges, voire des contours rouges, mais vous vous pencherez essentiellement sur toutes les boîtes bleues.

Pour effectuer une vérification d'administration simple, il y a un bouton unique qui permet automatiquement de vérifier chaque appareil avec une adresse IP qui n'a pas encore été vérifiée. Il se trouve dans l'onglet scanner de la boîte de dialogue System Configuration.

Quand une case est jaune pale elle se démarquera. Elle appellera votre attention. Découvrez de quel équipement il s'agit et ensuite vérifier le ou prenez des mesures pour supprimer l'appareil.

Un nœud rempli en rouge est le «fantôme» de la position réelle d'un appareil. Dans la vue IP, le dispositif réel aura une vraie adresse IP comme 10.1.100.56 et dans la boîte rouge l'adresse IP sera 10-1-100-56.

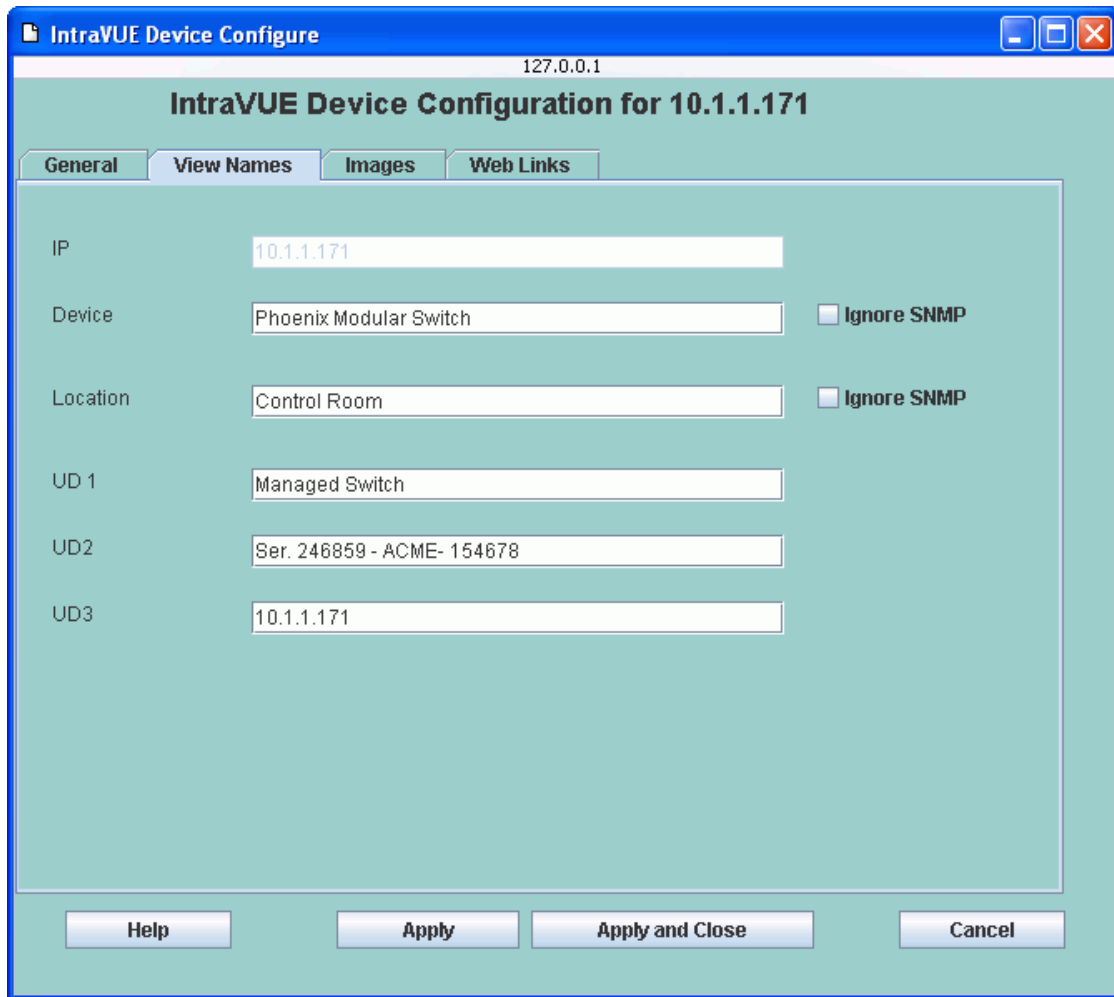
Si vous voyez une boîte rouge, trouver la boîte jaune pale correspondante.

Si la nouvelle position est acceptable, supprimez la boîte rouge et vérifiez la nouvelle position.

Si la position est temporaire vous pouvez laisser la case rouge. Lorsque l'appareil retourne à son ancienne place alors la boîte rouge sera remplacée par une boîte bleue.

## Configuration des équipements - Onglet View Names

Chaque champ permet de spécifier le nom porté par l'équipement pour chaque vue.



Field	Value	Ignore SNMP
IP	10.1.1.171	
Device	Phoenix Modular Switch	<input type="checkbox"/>
Location	Control Room	<input type="checkbox"/>
UD 1	Managed Switch	
UD 2	Ser. 246859 - ACME- 154678	
UD 3	10.1.1.171	

Seul le nom de l'équipement sur la vue IP ne peut être changé.  
Si aucun nom n'est configuré, l'adresse IP apparaît entre parenthèses.



### NOTE

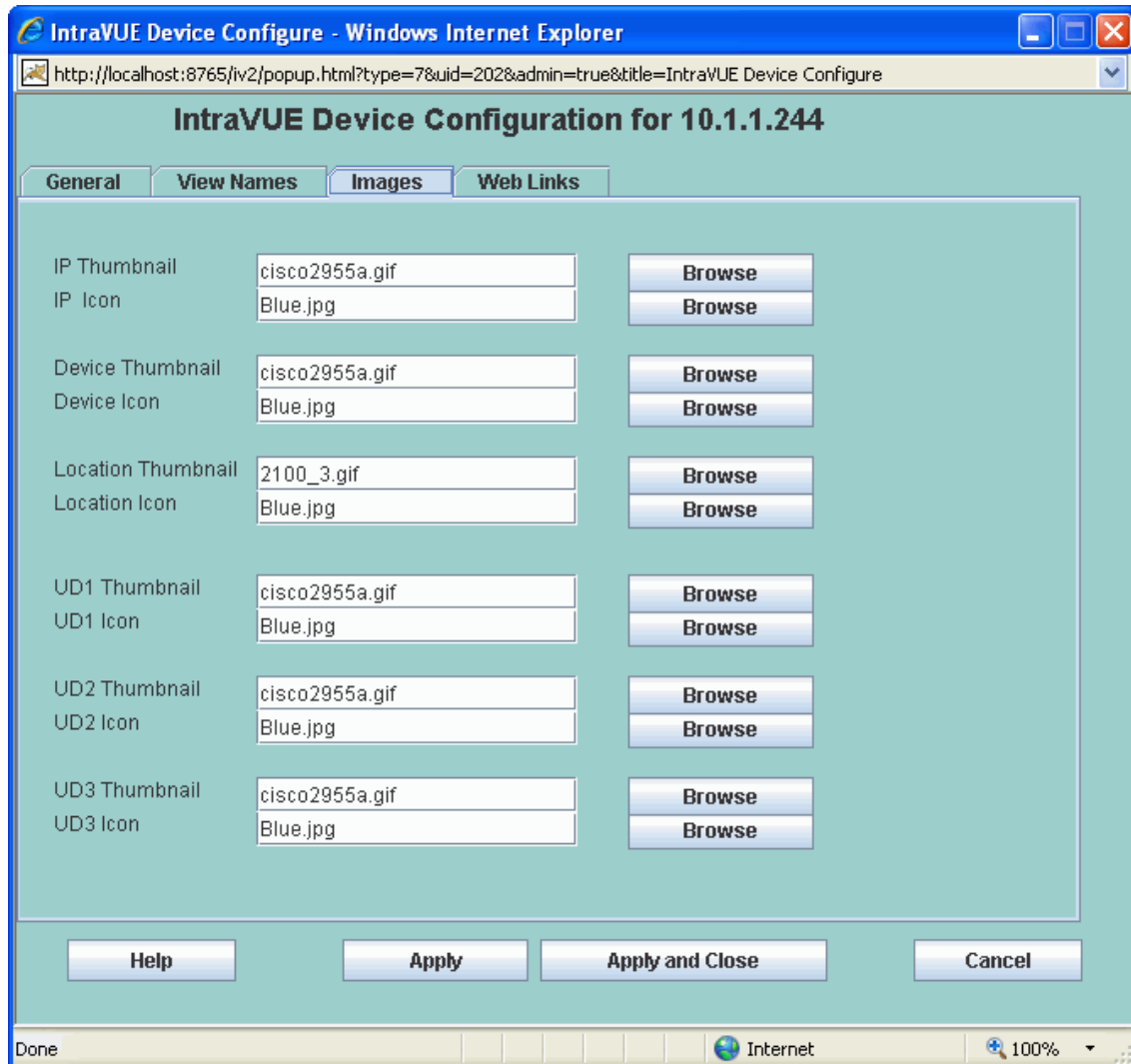
Le nom de l'équipement et sa localisation pourront avoir **Ignore SNMP** de cocher. Dans ce cas le scanner n'utilisera pas le SNMP pour avoir ces informations

Cochez **Ignore SNMP** puis entrez une valeur pour chaque paramètres.

*Ceci permet de personnaliser le nom manuellement. Cochez le « ignore SNMP » et renseignez le nom.*

## Configuration des équipements - Onglet Images

Cet onglet permet de spécifier les images à afficher dans la vue correspondante.



Chaque vue possède une image et un icône configurable par équipement.

L'affichage des images et des icônes peut se désactiver dans le " Menu Système " ou en agissant dans le fichier ivserver.properties.



Ces images se trouvent par défaut dans le répertoire :

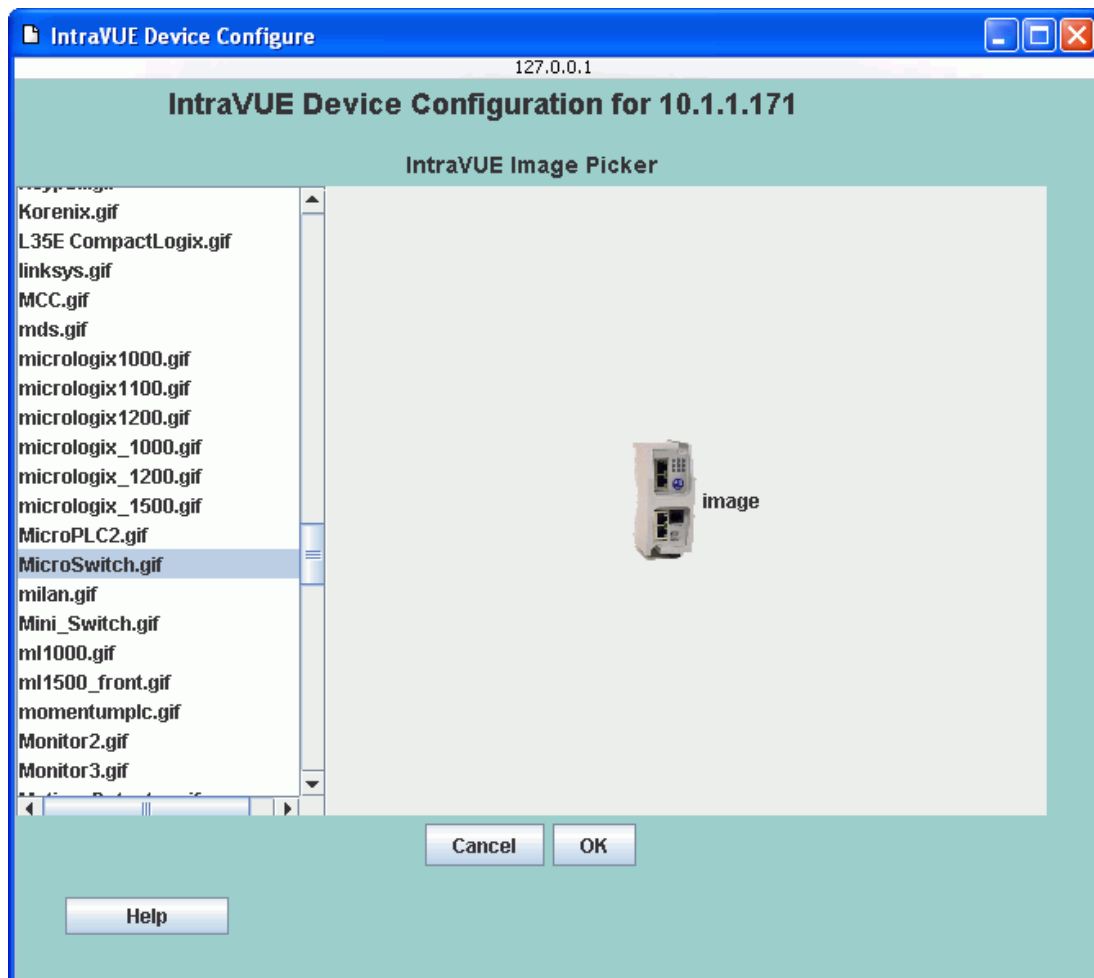
**c:\Program Files\IntraVUE\auotip\tomcat6\webapps\ROOT\IntraVUE\images**

## Images personnalisées

Vous pouvez utiliser des images personnalisées en les copiant directement dans le répertoire.

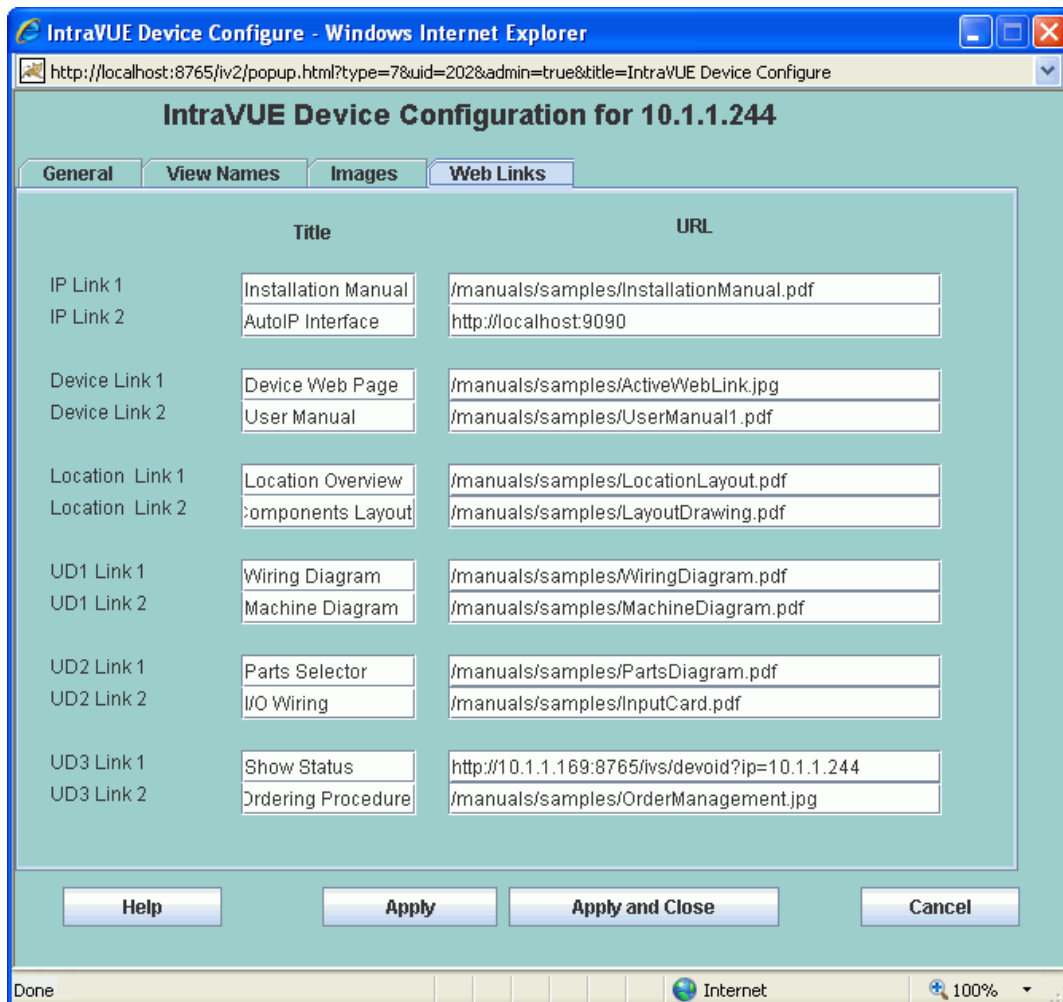
## Browse

Le bouton “Browse” permet de parcourir les images et de les sélectionner directement dans l’interface de configuration. Un aperçu est également disponible.



## Configuration des équipements - Onglet Web Links

2 liens web peuvent être configurés par vue.



	Title	URL
IP Link 1	Installation Manual	/manuals/samples/InstallationManual.pdf
IP Link 2	AutoIP Interface	http://localhost:9090
Device Link 1	Device Web Page	/manuals/samples/ActiveWebLink.jpg
Device Link 2	User Manual	/manuals/samples/UserManual1.pdf
Location Link 1	Location Overview	/manuals/samples/LocationLayout.pdf
Location Link 2	Components Layout	/manuals/samples/LayoutDrawing.pdf
UD1 Link 1	Wiring Diagram	/manuals/samples/WiringDiagram.pdf
UD1 Link 2	Machine Diagram	/manuals/samples/MachineDiagram.pdf
UD2 Link 1	Parts Selector	/manuals/samples/PartsDiagram.pdf
UD2 Link 2	I/O Wiring	/manuals/samples/InputCard.pdf
UD3 Link 1	Show Status	http://10.1.1.169:8765/ivs/devoid?ip=10.1.1.244
UD3 Link 2	Ordering Procedure	/manuals/samples/OrderManagement.jpg

La ligne "title" donne le nom du lien lorsqu'un clic droit est effectué sur l'équipement.

La ligne URL donne l'adresse vers laquelle le lien doit se diriger.

Il peut y avoir 2 types de liens : Si la donnée se trouve dans le répertoire par défaut d'IntraVUE (c:\program files\IntraVUE\AutoIP\tomcat6\webapps\ROOT) un lien relatif peut être appliqué. Sinon il est possible de spécifier le lien complet.

c:\program files\IntraVUE\AutoIP\tomcat6\webapps\ROOT

Copiez ou déplacez les documents que vous voulez utiliser dans des liens web. Vous pouvez créer des sous répertoires. Dans l'exemple ci-dessous, le lien 1 est stocké dans :

c:\program files\IntraVUE\AutoIP\tomcat6\webapps\ROOT>manuals\samples\InstallationManual.pdf

et l'adresse renseignée est :

/manuals/samples/InstallationManual.pdf



**NOTE:** Les noms de fichiers sont sensibles à la casse.

## Liens Web vers d'autres hôtes IntraVUE

Il y a un paramètre dans le fichier ivserver.properties qui contrôle le lien web qui est envoyé vers le destinataire de l'e-mail. Ceci établit la vue IntraVUE qui sera utilisée et si les images et icônes seront affichées ou non lors de l'ouverture du navigateur IntraVUE. Voir à la fin du fichier.

Ce paramètre peut être remplacé par les paramètres dans l'URL utilisée pour accéder à IntraVUE. Le lien Internet ci-dessous ouvrira le navigateur IntraVUE sur l'ordinateur en 10.2.3.44 sur la vue de localisation avec des icônes cachées et des images affichées. Le I et T majuscule affichent les icônes et les images (Thumbnails), le I et T minuscules cachent les icônes et les images (Thumbnails). Les numéros de vue sont définis dans le fichier ivserver.properties

<http://10.2.3.44:8765/iv2/ivue.jsp?v=3iT>

Ceci est particulièrement utile lorsque vous utilisez l'édition IntraVUE Supervisor.

## Déplacement Manuel

Il existe plusieurs raisons pour lesquelles vous voudriez changer manuellement les rapports entre les dispositifs représentés dans le navigateur IntraVUE.

- Vous voulez montrer des périphériques non IP tels qu'un convertisseur cuivre/fibre.
- Vous voulez un périphérique non Ethernet tels que des dispositifs série qui sont connectés à travers d'un convertisseur Ethernet/série.
- Des switches non managés peuvent être déplacés manuellement, mais partir de la version 2.0.5 peuvent être configurés facilement.

Lorsque vous êtes connecté en tant qu'Administrateur, le menu de l'équipement fournit deux fonctions pour accomplir ce qui précède: Ajouter "Add Child" et "Move".

### Add Child

Cela ajoute un nouveau nœud sous le périphérique sélectionné. Il est généralement utilisé pour les appareils connectés via des dispositifs de liaison. Les propriétés du nouveau nœud peuvent être modifiées pour refléter un dispositif qui est dans le réseau, mais pas visible pour le moteur d'analyse. Typiquement, les autres appareils qui sont physiquement connectés au nœud inséré seront déplacés graphiquement vers le nouveau nœud en utilisant la fonction MOVE. Une entrée de journal des événements est générée pour cette opération.

Il y aura une ligne noire reliant le nouveau nœud. Il va rester en noir, sauf si une IP de l'appareil est déplacé en dessous. Le nom initial du nouveau nœud sera "N/A"(en majuscule pour faire la différence avec les nœuds qui sont insérés automatiquement nommés "n/a" en minuscules).

### Move

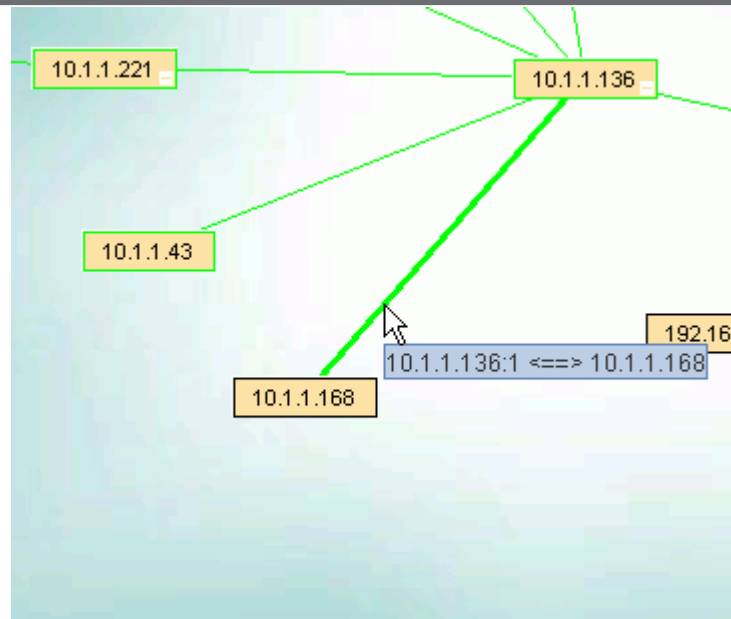
Move permet à l'utilisateur de changer le parent d'un appareil.

Pour faire un mouvement, d'abord sélectionner le périphérique que vous souhaitez déplacer. Il obtiendra un contour bleu. Alors que l'appareil est toujours sélectionné, cliquez à droite sur le périphérique parent sous lequel vous souhaitez déplacer l'appareil et sélectionnez **Move** . Une entrée de journal des événements est générée pour cette opération.

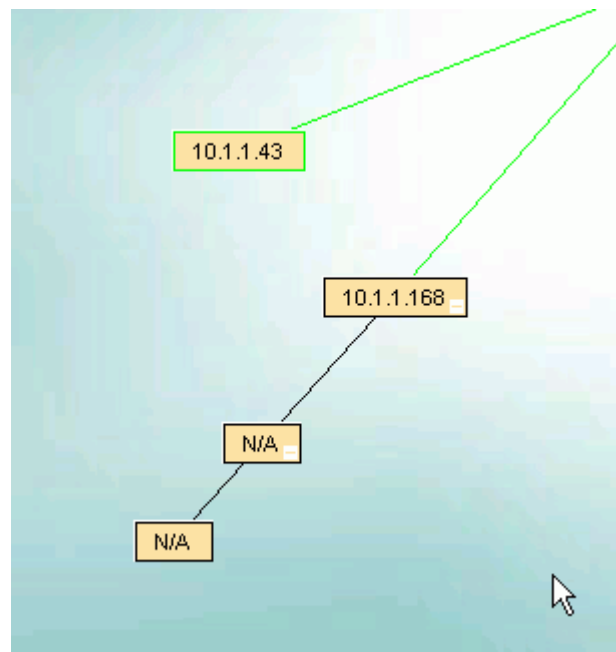
### Exemple d'ajout de convertisseurs de média

Les convertisseurs de média n'ont généralement pas les adresses IP. Ils peuvent prendre le câble cuivre de CAT5 et de le convertir en fibre ou même en sans fil. Un deuxième appareil reconvertis généralement le signal en cuivre.

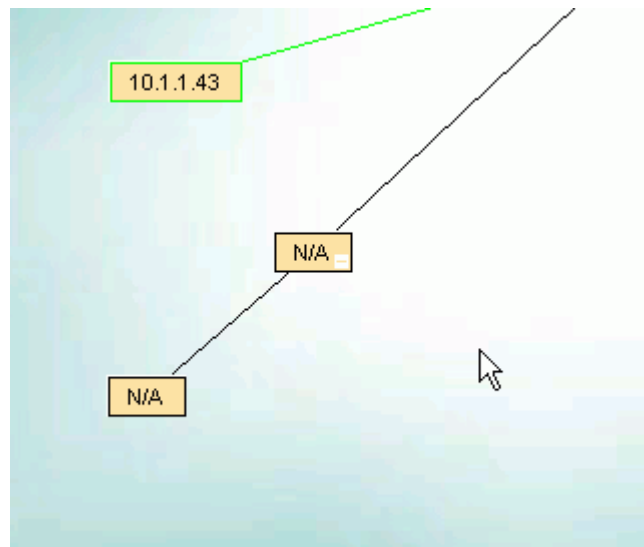
En faisant cela, il est souhaitable d'avoir le port du switch. Dans l'image ci-dessous il y a un numéro de port pour la ligne reliant le périphérique.



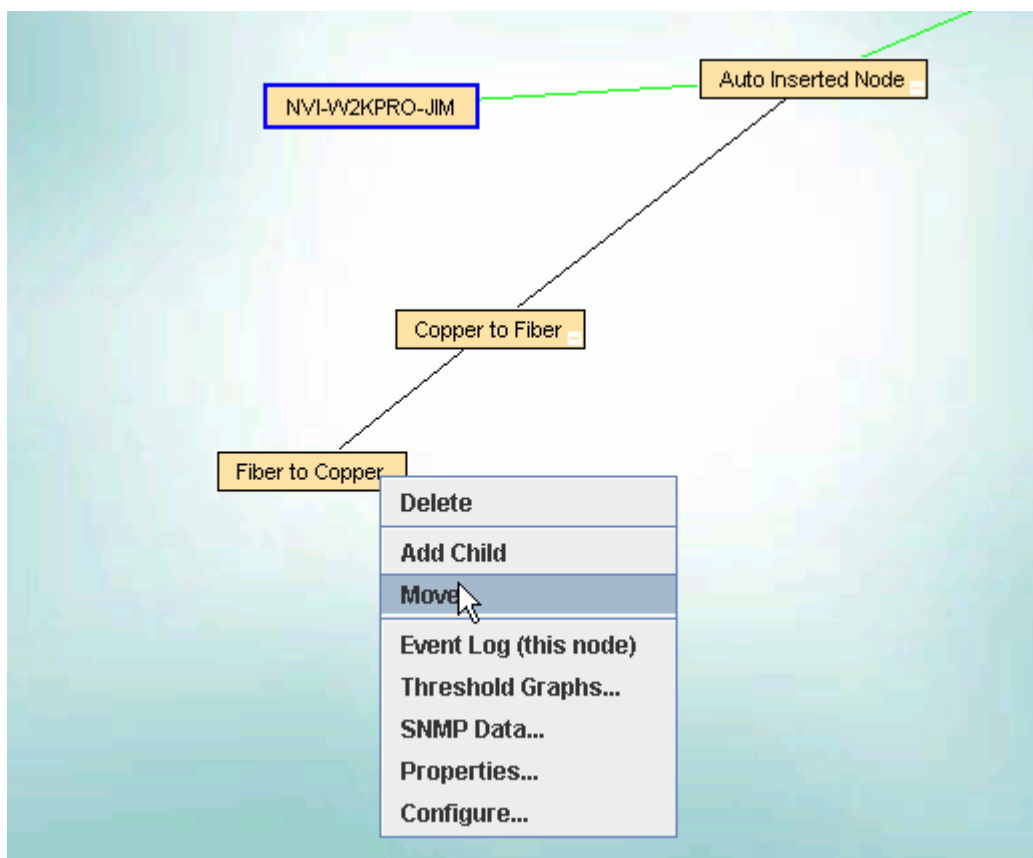
Utilisez Add Child et d'ajouter un premier enfant à l'appareil, et à côté de l'enfant qui vient d'être ajouté. Vous avez maintenant deux périphériques enfants sans nom sous le dispositif d'origine



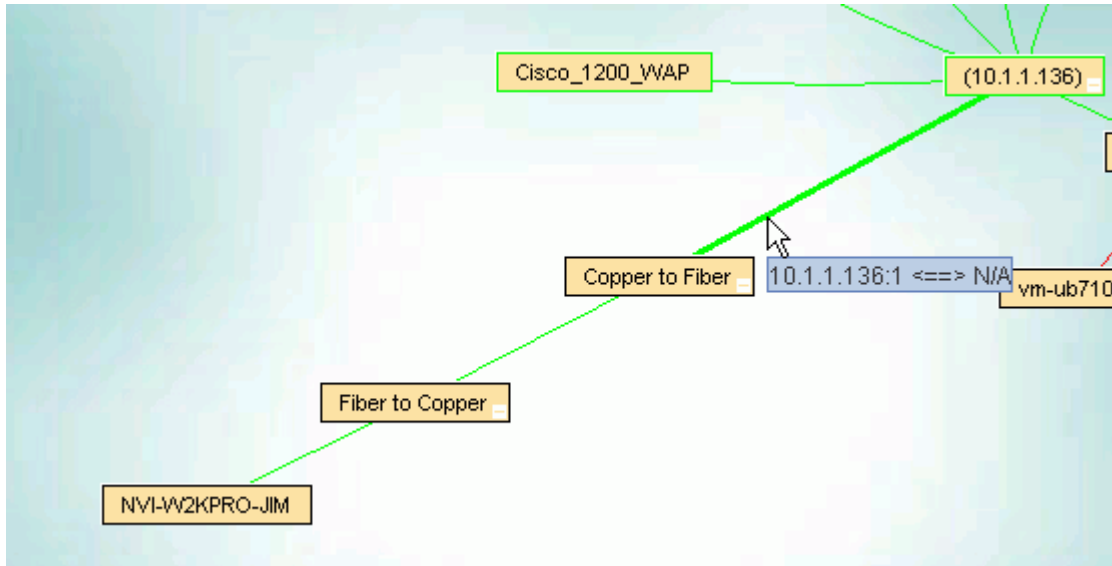
Supprimez maintenant l'appareil avec l'adresse IP.



Il sera redécouvert et deviendra un enfant d'un nouveau nœud inséré automatiquement, à son emplacement d'origine. Ensuite, choisissez le périphérique (il obtient un contour bleu) et choisissez "configure" pour le bouger sous ce nœud.



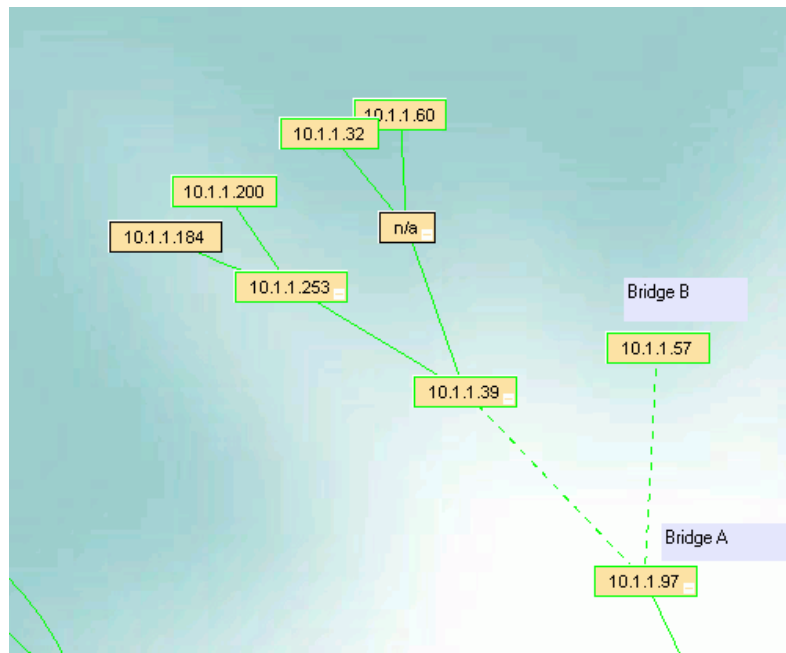
Le nœud inséré automatiquement va s'en aller, la ligne reliant au premier nœud auront encore un numéro de port, et le nœud de périphérique supplémentaire vous aidera à comprendre votre réseau lorsque des problèmes surgissent.



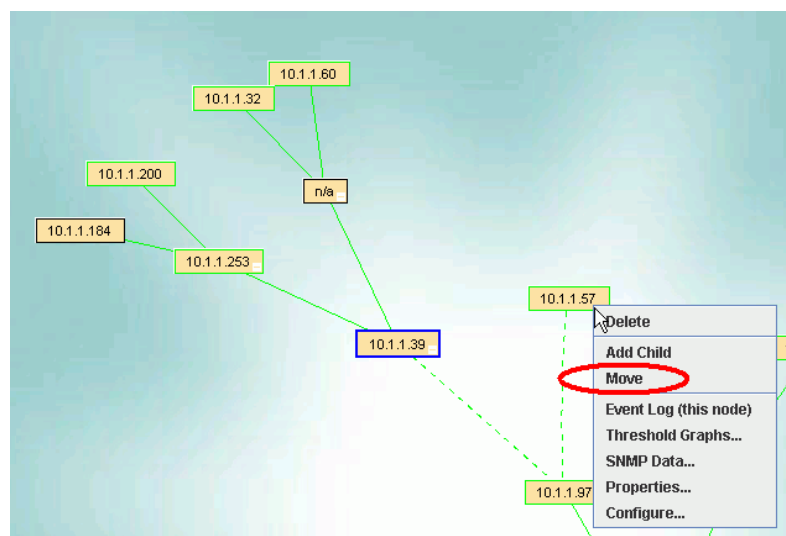
### Exemple de configuration d'un pont

Dans l'image ci-dessous, les dispositifs .97 et .57 ont été découverts comme des ponts sans fil. IntraVUE ne saura pas quelle adresse IP est du côté du réseau IntraVUE de sorte que vous pourriez trouver un ou l'autre en tant que le parent.

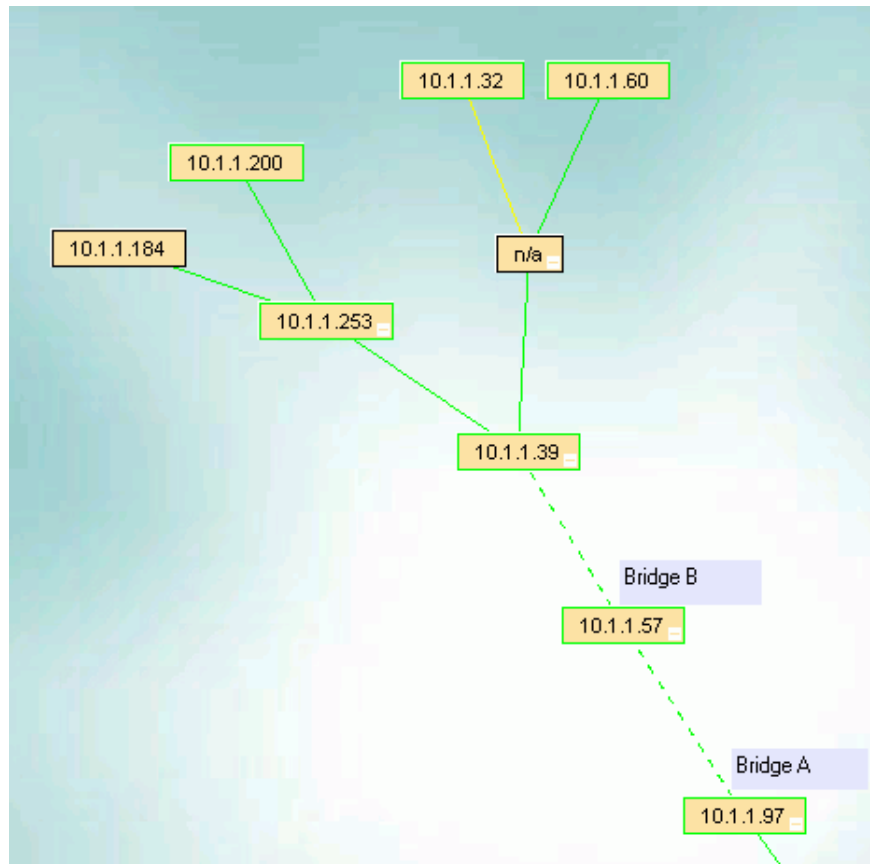
Les dispositifs de l'autre côté du pont apparaîtront sous le pont supérieur, avec l'autre extrémité du pont.



Dans ce cas, le .97 est du côté IntraVUE et nous voulons que les appareils, en commençant par le .39, apparaissent en dessous. Le Pont B, le .57, a besoin d'obtenir les appareils et nous utilisons l'instruction Move ci-dessus. Sélectionnez le .39 donc il a un contour bleu, puis faites un clic droit sur le périphérique où vous souhaitez le déplacer (vers le .57) et choisissez Move.



Les dispositifs de l'autre côté du pont seront maintenant sous le .57.



## Module : Mode Avancé

### Description répertoire IntraVUE

Le répertoire dans lequel a été installé IntraVUE contient les dossiers suivants:

- AutoIP - contient des éléments de IntraVUE, y compris le serveur Web utilisé par IntraVUE.
- CleanDbBackup - des fichiers pour la création d'une base de données propre. Il contient également un fichier batch pour créer une nouvelle base de données sans navigateur.
- DbBackup - stockage des bases de données créées et enregistrées par les utilisateurs et automatiquement créées
- Log - dossier détaillé de trace interne
- QuickStart\_files - les fichiers de support pour le Guide de démarrage rapide.
- Tools - programmes utilitaires.

Le dossier AutoIP contient de nombreux fichiers. L'intérêt de ces fichiers pour un utilisateur /administrateur de IntraVUE sont:

- bootpdata.xml - L'équivalent XML de l'option AutoIP dans l'interface utilisateur. Les données sont stockées dans ce dossier.
- ivserver.properties - contient les paramètres qui ne sont normalement pas modifiées par les utilisateurs. Les détails se trouvent sous ivserver.properties.
- ivserver.properties.new - Les mises à jour d'IntraVUE n'écrasent pas le fichier courant, les mise à jour sont stockés ici.
- ivserver.xml - contient les paramètres et les données de configuration du SNMP et du serveur Modbus /TCP . Les détails se trouvent sous ivserver.xml.
- scanner.log - un journal de toutes les demandes bootp et dhcp vu par AutoIP et de toutes les réponses faites par AutoIP.
- trapmailer.xml - un fichier de configuration pour interpréter les Traps envoyés à l'hôte IntraVUE et réorienter les Traps vers un serveur de messagerie. Détails dans le fichier.

Le dossier "tomcat6" sous AutoIP contient tous les fichiers d'Apache Tomcat eTomcat Web server. Il est utilisé pour fournir une interface utilisateur à la base de données IntraVUE. Le seul dossier qui a de l'intérêt pour les utilisateurs est le dossier racine du serveur Web. Le dossier racine peut être consulté à partir d'un ordinateur en parcourant le serveur Web de IntraVUE. Les utilisateurs sont libres de créer leur propre contenu en dessous de ce dossier, y compris la création de nouveaux dossiers. Le chemin vers le dossier racine est:

```
...\IntraVUE\autoip\tomcat6\webapps\ROOT
```

Lire Configuring Web Links et Configuring Icons and Thumbnails Pour plus d'information sur la création de vos propres images ou pour l'ajout de contenu web mis à disposition par le serveur web d'IntraVUE.

## Sauvegarder des fichiers ne se trouvant pas dans la base de données MySQL.

Lorsque vous effectuez une sauvegarde à partir du menu ou de la boîte de dialogue système de configuration, vous sauvegardez la base de données MySQL qui contient toutes les **données** d'IntraVUE. Cette sauvegarde ne contient pas de **contenu** référencé par IntraVUE.

Dans le cas d'une catastrophe, installer une nouvelle copie de IntraVUE depuis le CD d'installation, puis rétablir l'enregistrement d'une sauvegarde vous permet de revenir à l'endroit où vous étiez au moment de la sauvegarde. Le contenu ajouté par l'utilisateur ne sera pas dans la sauvegarde.

D'autres dossiers qui pourraient être sauvegardés par l'intermédiaire de la fenêtre de sauvegarde d'application ou les tâches planifiées peuvent inclure:

- La base MySQL active.
- Contenu créé par l'utilisateur
- Les modifications utilisateur des fichiers par défaut d'IntraVUE.

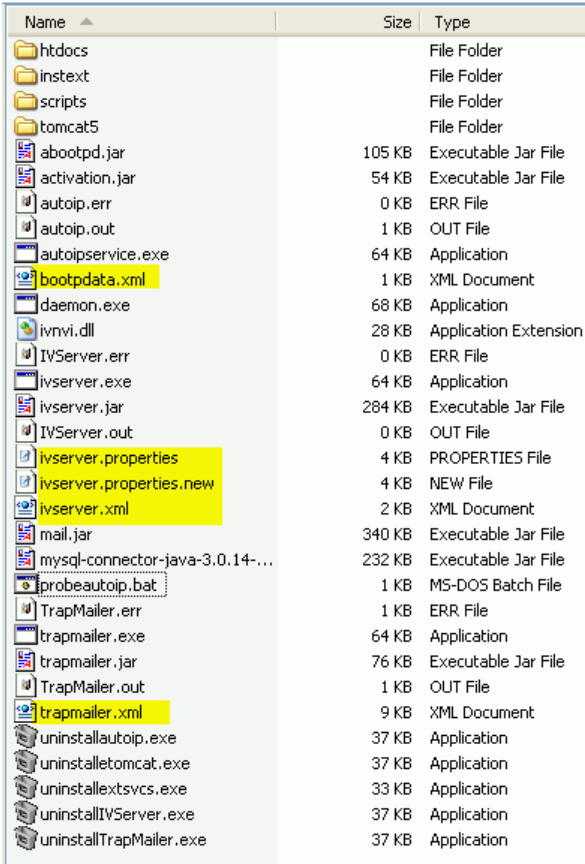
Les fichiers de données MySQL sont généralement situés sur le disque dur sur lequel IntraVUE a été installé dans le répertoire \ MySQL \ data \ IntraVUE. La meilleure approche pour maintenir la base de données sur un autre ordinateur pour copier les fichiers dans ... \ IntraVUE \ dbBackup \ autoBackups.

Le contenu créé par l'utilisateur peut uniquement se trouver dans le répertoire racine. Tout le contenu est conservé lors d'une mise à jour. Sauvegardez le dossier racine pour sauver le contenu que vous avez ajouté.

## Fichiers de configuration avancés

La plus grande partie de la configuration des données se trouve dans la base MySQL. Il y a également quelques fichiers additionnels qui contiennent quelques informations. La modification des fichiers par défaut d'IntraVUE se trouve uniquement dans un des fichiers suivants, dans le dossier c:\program files\IntraVUE\autoip\:

- bootpdata.xml
- ivserver.properties
- ivserver.xml
- trapmailer.xml



Name	Size	Type
htdocs		File Folder
instext		File Folder
scripts		File Folder
tomcat5		File Folder
aboutpd.jar	105 KB	Executable Jar File
activation.jar	54 KB	Executable Jar File
autoip.err	0 KB	ERR File
autoip.out	1 KB	OUT File
autoip-service.exe	64 KB	Application
bootpdata.xml	1 KB	XML Document
daemon.exe	68 KB	Application
ivnvi.dll	28 KB	Application Extension
IVServer.err	0 KB	ERR File
ivserver.exe	64 KB	Application
ivserver.jar	284 KB	Executable Jar File
IVServer.out	0 KB	OUT File
ivserver.properties	4 KB	PROPERTIES File
ivserver.properties.new	4 KB	NEW File
ivserver.xml	2 KB	XML Document
mail.jar	340 KB	Executable Jar File
mysql-connector-java-3.0.14-...	232 KB	Executable Jar File
probeautoip.bat	1 KB	MS-DOS Batch File
TrapMailer.err	1 KB	ERR File
trapmailer.exe	64 KB	Application
trapmailer.jar	76 KB	Executable Jar File
TrapMailer.out	1 KB	OUT File
trapmailer.xml	9 KB	XML Document
uninstallautoip.exe	37 KB	Application
uninstalltomcat.exe	37 KB	Application
uninstalltxtsvcs.exe	33 KB	Application
uninstallIVServer.exe	37 KB	Application
uninstallTrapMailer.exe	37 KB	Application

### bootpdata.xml

Contient la configuration des programmes optionnels AutoIP. Les données de ce fichier proviennent normalement de l'interface utilisateur AutoIP, via la configuration 'Enable Autoip' disponible dans la configuration de l'équipement, ou directement par édition du fichier xml. Notez qu'en cochant 'Enable Autoip' une entrée est générée dans ce fichier mais qu'en décochant l'entrée n'est pas supprimée. Pour supprimer une entrée AutoIP vous pouvez utiliser l'interface utilisateur ou éditer le fichier.

**ivserver.properties** Contient les paramètres de réglage fin du scanner qui ne sont pas encore présents dans l'interface utilisateur. Chaque paramètre est précédé d'une explication

Notez que lors d'une mise à jour, le fichier `ivserver.properties` n'est pas changé. Cependant un fichier `ivserver.properties.new` est copié dans le dossier. Il appartient à l'administrateur de copier ou non le nouveau fichier.

### **ivserver.xml**

Ce fichier contient la configuration pour les données Modbus/TCP ainsi que les informations SNMP affichées dans le menu 'SNMP Data ...' des équipements

**trapmailer.xml** Ce fichier fournit des fonctionnalités étendues pour récupérer et envoyer des informations concernant les messages Trap. Toute la configuration est faite dans ce fichier qui est également auto documenté. Remarque: l'ensemble des possibilités trapmailer sont complexes et demande un effort pour être comprises

## **Le fichier ivserver.properties**

Ce fichier se trouve dans le dossier de AutoIP IntraVUE, normalement `...\\program files\\IntraVUE\\autoip` (les détails des fichiers système) .

Chacun des paramètres qui peuvent être définies dans ce fichier contient une description du paramètre et une ligne d'exemple indiquant la valeur par défaut. Ils sont représentés par des lignes de commentaires dans le fichier. LE FICHIER EST AUTO-DOCUMENTE.

Les lignes de commentaires commencent par un caractère "#" et n'ont aucun effet.

Ce fichier contient généralement des éléments de configuration qui ne sont normalement pas modifiées par les utilisateurs ou les administrateurs d'IntraVUE. Il est habituellement seulement changé après consultation du support technique IntraVUE.

Ouvrez le fichier avec le Bloc-notes ou WordPad pour afficher les diverses options ou de faire des changements.

Notez que ce fichier n'est jamais écrasé lors d'une installation ou réinstallation/upgrade. Au lieu de cela, un fichier nommé `ivserver.properties.new` est stocké dans le dossier AutoIP et peut être utilisé pour mettre à jour les paramètres dans le fichier actif.

## Le fichier ivserver.xml

### Configuration Modbus/TCP et des données SNMP

IntraVUE fournit une information de connexion et SNMP à travers un serveur de communication intégré Modbus / TCP sur le port 502.

En outre, toutes les données SNMP configurées sont visibles dans le navigateur IntraVUE en sélectionnant SNMP Data... dans le menu de l'équipement

Les informations à fournir sont configurées dans le fichier "ivserver.xml», qui se trouve sous ...\\IntraVUE\\autoip (détaille du fichier système).

IntraVUE rend l'information disponible pour les SCADA de la même manière qu'ils auraient accès à l'information dans un automate. ivServer peut également être configuré pour fournir toutes les variables SNMP par l'intermédiaire de l'interface Modbus/TCP.

Le fichier commence et se termine avec une ligne dataserver.

```
<dataserver mysql="127.0.0.1">  
.....  
</dataserver>
```

Il existe trois autres types de lignes dans le fichier ivServer.xml, situé entre les deux lignes ci-dessus.

### Ping ou état de Connexion

Les lignes qui commencent par "ping" créent des registres Modbus/TCP pour l'état courant de la connexion de l'équipement.



*Note: Le registre 0 dans ivserver.xml file est le 1er registre 40000 ou 4X dans Modbus qui a un offset de 1 et qui est en réalité le registre 4:0001.*

```
<ping reg="0" ip="192.168.100.2" />  
<ping reg="10" ip="10.1.1.45" />
```

Dans l'exemple ci-dessus, l'état de Ping du dispositif 192.168.100.2 sera stocké dans le 0ème ou premier registre 4X Modbus. Celui-ci est généralement dénommé 4:00001 ou 400001. Le statut de Ping 10.1.1.45 sera stocké dans le registre Modbus 4:00011.

## Données SNMP

Les lignes qui commencent par "SNMP" créent des valeurs dans la base MySQL qui sont affichées comme des données supplémentaires dans le menu de l'équipement sous *SNMP Data...*

Le scanner fait de simples requêtes de lecture snmp pour chaque définition faite dans ce fichier à chaque cycle du scanner (un cycle dure entre 5 et 10 secondes).

```
<snmp reg="2:ts" ip="192.168.100.254" oid="1.3.6.1.2.1.1.3.0" c="public" disptext="uptime"/>
<snmp reg="10:s10" ip="10.1.1.100" oid="1.3.6.1.2.1.1.1.0" c="public" disptext="description"/>
<snmp ip="192.168.100.254" oid="1.3.6.1.2.1.2.2.1.5.1" c="public" disptext="Port 1 Speed"/>
```

Si on fixe reg="" ou si reg est manquant, alors il n'y a pas de registre Modbus/TCP d'attribué dans le serveur et l'information sera simplement affichée dans *SNMP Data*.

L'attribut c= permet de fixer la communauté snmp de l'équipement

L'attribut disptext= permet de fixer le texte à afficher dans la boîte de dialogue *SNMP Data*.

La valeur de l'OID peut être une valeur publique ou une valeur très spécifique attribuée par le fabricant d'un dispositif comme une alarme de température pour une pompe à eau.

L'information après le numéro du registre indique le début d'une définition du type de données pour l'information qui va être récupérée. Les registres Modbus font 2 octets de long.

```
reg = "10:i" signifie que le registre 10 est un entier sur 16 bits
reg = "11:d" signifie que le registre 11 est un entier sur 32 bit est occupe 2 registres
reg = "13:s10" signifie que le registre 13 est une chaîne de caractère qui occupe 10 registres ou 20 octets.
```

Dans le deuxième exemple ci-dessus la valeur stockée dans les registres Modbus occupe les registres 11 et 12, car il s'agit d'un nombre sur 32 bits.

Dans le 3e exemple ci-dessus la chaîne occupe les registres 13 à 22 - un total de 20 octets.



### Remarques importantes

1. Lorsque de la configuration des registres vous devez être conscient de la taille des données à écrire dans les registres et faire attention de ne pas superposer les données. Dans le cas des données de chaîne, si les données récupérées est plus long que la taille configurée, les données seront tronquées à la taille configurée. La syntaxe complète des types de données est dans les commentaires du fichier *ivServer.xml*.

2. chaque fois qu'une requête à un dispositif SNMP échoue, a une erreur, ou arrive à expiration alors le caractère unique "0" sera stocké pour les données de type texte et le numéro 0 sera stockée pour les données numériques. Les clients du serveur Modbus tels que les SCADA doivent être programmés pour gérer ou ignorer ces Etats.

## Informations d'état du Réseau

Les lignes qui commencent par "networkstatus" fournir un WordBit dans un registre. L'état de chacun des bits du registre restera à 1 pendant un temps noté "durationmsec" millisecondes et puis reviendra à 0.

```
<networkstatus reg="60" durationmsec="15000"/>
```

"networkstatus" définit un registre qui aura 4 bits, dont chacun va générer une «impulsion» à chaque fois qu'un événement associé est détecté dans la base de données IntraVUE. Le bit passe de 0 à 1, reste à 1 pendant la durée configurée, puis revient à 0. Chaque bit est manipulé et datés de manière indépendante. Si un nouvel événement du même type se produit alors que le bit est défini, une nouvelle période commence.

Les événements détectés et signalés dans ce registre sont

- bit 0: un nouvel appareil rejoint le réseau
- bit 1: appareil déconnecté
- bit 2: appareil reconnecté
- bit 3: seuil dépassé

## Conseil important

Chaque fois que vous modifiez le fichier ivserver.xml il est judicieux d'ouvrir le fichier dans Internet Explorer une fois les modifications terminées. S'il y a une erreur XML, Internet Explorer vous indiquera le numéro de ligne où se trouve l'erreur. S'il y a une erreur dans le fichier, IntraVUE va ignorer le fichier et continuer à fonctionner avec les derniers bons paramètres.

## Désactivation Modbus TCP

A cause d'autres logiciels, il faut parfois désactiver dans IntraVUE le serveur Modbus/TCP. Dans ce cas, éditez le fichier ivserver.properties et changez la valeur ci-dessous à "false"

```
modbus.service=true
```

## Utilisation du Trunking dans les Switchs

### Généralité

Certains switchs peuvent être configurés pour le traitement de deux ou plusieurs ports, comme s'ils étaient un seul port. L'une des raisons de cette solution est d'obtenir davantage de bande passante entre les deux switchs. Une autre raison est "l'équilibrage de charge" ou "load balancing".

IntraVUE demande à un "switch managable" pour un numéro de port les différentes adresses MAC des dispositifs connectés. Dans le cas du trunking, la réponse pourrait être l'un des ports utilisés pour le raccordement au réseau. En retour IntraVUE pourra voir le switch «bas» comme se déplaçant fréquemment entre les ports dont les ressources sont partagées, et l'affichage de IntraVUE va être redessiné chaque fois qu'il y a un tel changement.

Un fichier de configuration a été créé qui permet à l'administrateur IntraVUE d'informer le scanner de l'utilisation du trunking pour les switchs en cours de scanne.

Le nom par défaut du fichier est 'trunkingdefs.txt'. Il se trouve sous ...\\IntraVUE\autoip folder (Détails du fichier système). Le véritable nom utilisé est configurable par l'utilisateur dans le fichier ivserver.properties dans la propriété 'scanner.trunk.data.file'. Un administrateur pourrait alors avoir plusieurs fichiers de configuration différents de trunking pour faire des essais ou à d'autres fins.

Un autre avantage d'utiliser le fichier 'trunkingdefs.txt' est l'aptitude à renuméroter les ports en fonction de ce que les utilisateurs visualisent sur les switchs, voir l'exemple 3.

### Le fichier 'trunkingdefs.txt'

Ce fichier est lu et interprété à la fois pour combiner les ports (trunking) et pour modifier les numéros de port attribué à un interrupteur à des fins d'affichage.

Le format est simple. Un switch est désignée à l'aide des crochets [], autour de son adresse IP. Elle est suivie par une ou plusieurs lignes d'affectations de port jusqu'à ce que la prochaine série de crochets.

Les affectations de ports sont faits en utilisant un séparateur de deux caractères "->". Sur la gauche, le port connu du switch. Sur la droite, comment IntraVUE devraient traiter et d'afficher ce port.

De nombreux ports sur la gauche peuvent être attribués au même numéro sur la droite. Si un numéro est répété sur la gauche, seul le dernier sera utilisé.

#### Exemple 1 - Cas général

Le switch 10.1.2.3 possède des ports 2 et 3 à ressources partagées et connectés aux ports 5 et 6 du switch 10.1.2.4. Nous voulons que IntraVUE considère les ports 2 et 3 sur 10.1.2.3 comme le port 2 et les ports 5 et 6 sur l'autre switch comme port 5.

[10.1.2.3]  
2->2  
3->2

[10.1.2.4]  
5->5  
6->5

### Exemple 2 - Liste des numéros de port différents pour les interrupteurs empilés

Lorsque deux switch 24 ports sont empilés, les numéros de port du second switch sont changés en interne afin qu'ils n'entrent pas en conflit avec le premier switch. Sur certains switch, le premier port du deuxième switch peut être numéroté 25, ou 27 si il ya des ports internes, ou même avec un grand nombre comme 950.

Cet exemple montre comment le second switch empilé à 8 ports a été renuméroté à des fins d'affichage.

[10.1.2.3]  
10->1  
11->2  
12->3  
13->4  
14->5  
15->6  
16->7  
17->8

### Exemple 3 - un commutateur avec des ports mal numérotés

Dans cet exemple, l'étiquette sur le switch numérote les ports de 1 à 12, mais à l'intérieur des ports sont disposés de 12 à 1. IntraVUE indique le numéro de port utilisé par le switch en interne, ce qui conduit à une confusion. C'est le cas du switch Cisco 2955.

[10.1.2.3]  
1->12  
2->11  
3->10  
4->9  
5->8  
6->7  
7->6  
8->5  
9->4  
10->3  
11->2  
12->1

## Comment ajouter Numéro de port supplémentaire au serveur web

IntraVUE utilise le port 8765 pour afficher des pages web et communiquer en interne. Certains utilisateurs désirent utiliser un autre numéro de port en raison de serveurs proxy ou pour traverser un pare-feu. IntraVUE peut être configuré pour "écouter" des numéros de port supplémentaires, mais sera TOUJOURS à l'écoute du port 8765 qui DOIT être disponibles pour l'utilisation de IntraVUE.

Voici comme un exemple les étapes pour configurer le serveur Web Tomcat et utiliser le port 80.

1. Assurez-vous que le port 80 n'est pas utilisé déjà avec un autre serveur web (par exemple, IIS, Apache) À partir d'une ligne de commande, faite

```
netstat -an
```

Vous **ne devez pas** voir de ligne comme

```
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
```

Si vous visualisez cette ligne, il faut savoir quel serveur web utilise ce port et l'arrêter avant de continuer. Regardez la liste des services et de regardez s'il ya quelque chose comme httpd, apache, IIS, ... L'autre serveur Web doit être configuré pour utiliser un autre port ou ne doit pas fonctionner pour éviter une course pour accéder au port lors d'un redémarrage.

2. En utilisant l'Explorateur Windows, naviguez jusqu'au répertoire

```
C:\Program Files\IntraVUE\AutoIP\tomcat6\conf
```

3. Faites une copie de sécurité du fichier server.xml en le sélectionnant, puis copiez (Ctrl-C) et collez (Ctrl-V)

4. Ouvrez le fichier server.xml avec notepad (c'est un fichier assez court - environ 30 lignes)

5. Ajouter une ligne supplémentaire après la définition au port 8765. VOUS NE DEVEZ PAS RETIRER LE LINE 8765. Ainsi,

```
Connector port="8765"
```

devient

```
Connector port="8765"  
Connector port="80"
```

6. Dans la liste des services, arrêtez et puis démarrez le service 'Apache Tomcat etomcat'



7. Confirmez que vous pouvez toujours communiquer avec le serveur IntraVUE en pointant votre navigateur à l'URL

`http://127.0.0.1:8765/iv2/list`

8. Confirmez EGALEMENT le fonctionnement sur le port 80 en utilisant l'URL

`http://127.0.0.1:80/iv2/list`  
`http://127.0.0.1/iv2/list`

9. Vous devriez maintenant être en mesure de voir IntraVUE sur le port 80

`http://127.0.0.1`

Notez que vous ne pouvez pas supprimer le port 8765 à partir du fichier `server.xml`, parce que certaines fonctions internes s'attendent à trouver le serveur sur ce port. Cependant, tous les applets utilisent le même port que la connexion d'origine, donc cela devrait fonctionner correctement à travers les firewalls qui bloquent le port 8765.

Bien qu'il soit possible en principe d'accueillir un serveur Web existant sur le port 80 sans l'arrêter, les procédures sont beaucoup plus complexe, surtout si l'objectif est de passer à travers les firewalls. Nous suggérons donc d'installer IntraVUE sur une machine dédiée de façon à éviter ces questions.

## Module : Intégration SCADA

Intravue peut être intégré de deux manières dans un logiciel de supervision : soit en intégrant uniquement la partie graphique, soit en établissant une communication entre Intravue et le SCADA.

Ces deux méthodes d'intégration peuvent bien évidemment être cumulées.

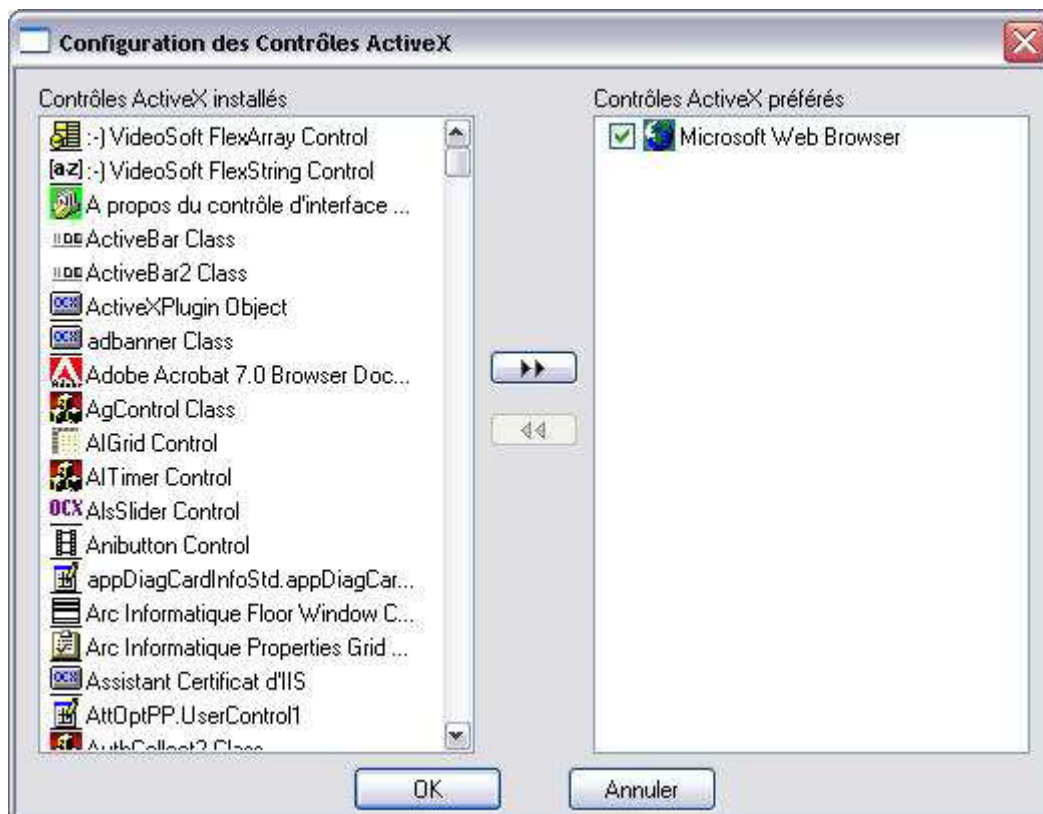
A titre d'exemple, nous présenterons ici comment intégrer Intravue dans le logiciel PcVue.

### Intégration de la partie Graphique d'Intravue.

Comme nous l'avons vu, Intravue est une application entièrement basée sur la technologie WEB. Il est donc possible d'insérer dans le synoptique d'un SCADA, un activeX web tel que « MicrosoftWebBrowser » afin d'autoriser l'accès et l'utilisation d'Intravue depuis ce synoptique.

Ajouter l'ActiveX « Microsoft Web Browser » aux ActiveX préférés PcVue

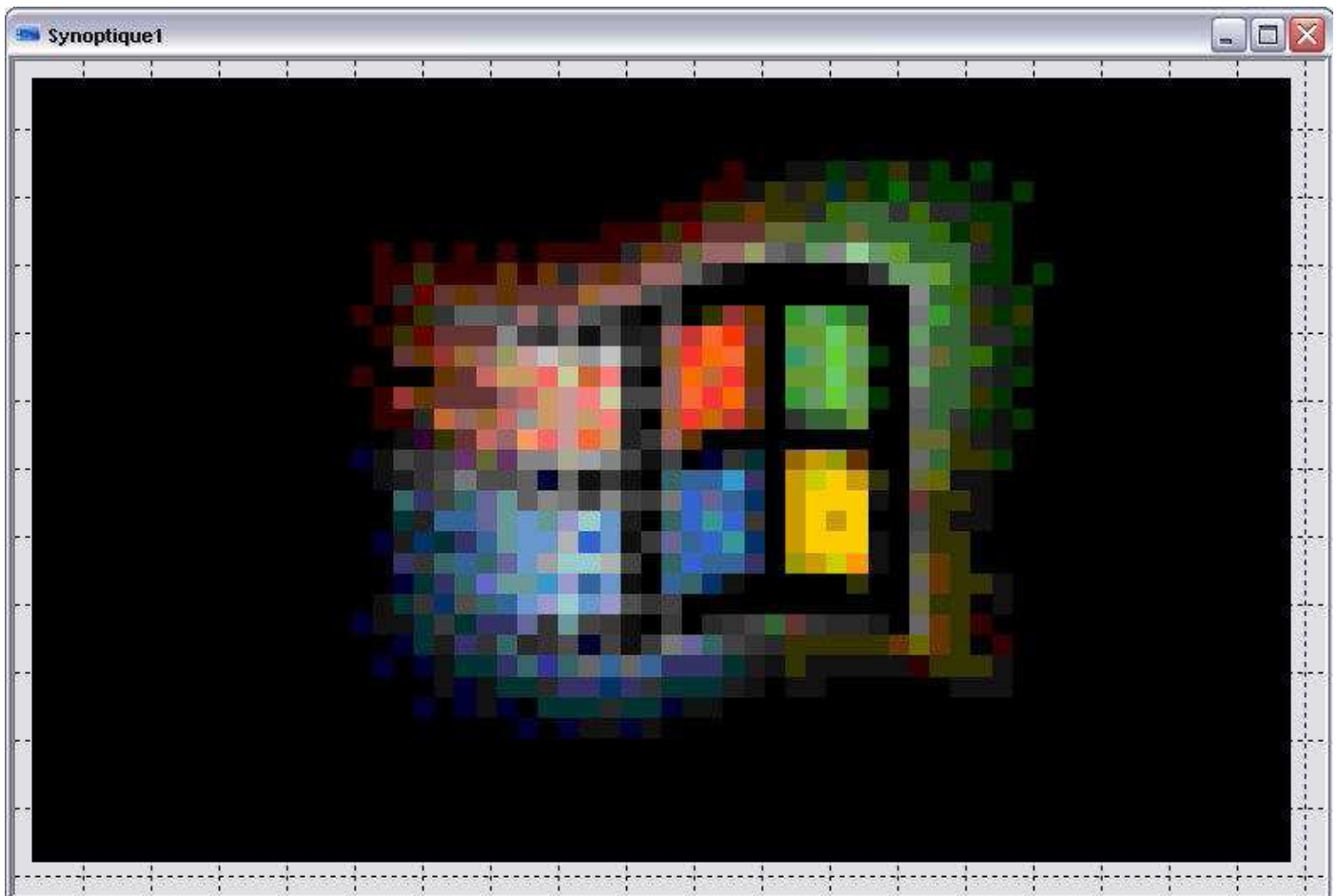
Dans PcVue, sélectionnez l'option « Contrôles ActiveX » dans le menu Configuration/Ergonomie



Ajouter le contrôle « Microsoft Web Browser » aux contrôles ActiveX préférés.

Créer un synoptique contenant l'ActiveX

Créez un nouveau synoptique PcVue et insérez le contrôle ActiveX « Microsoft Web Browser » par le menu Insertion > Contrôles ActiveX préférés > Microsoft Web Browser



Ajustez le positionnement et la taille du contrôle activeX

Paramétrage de l'ActiveX

Validez l'option « Contrôle VBA » par le menu contextuel affiché lors d'un clic droit sur l'ActiveX. Cette option vous autorise à piloter l'activex par l'éditeur Visual Basic intégré à PcVue.

Affichez l'éditeur Visual basic par le menu Affichage/Editeur Visual Basic

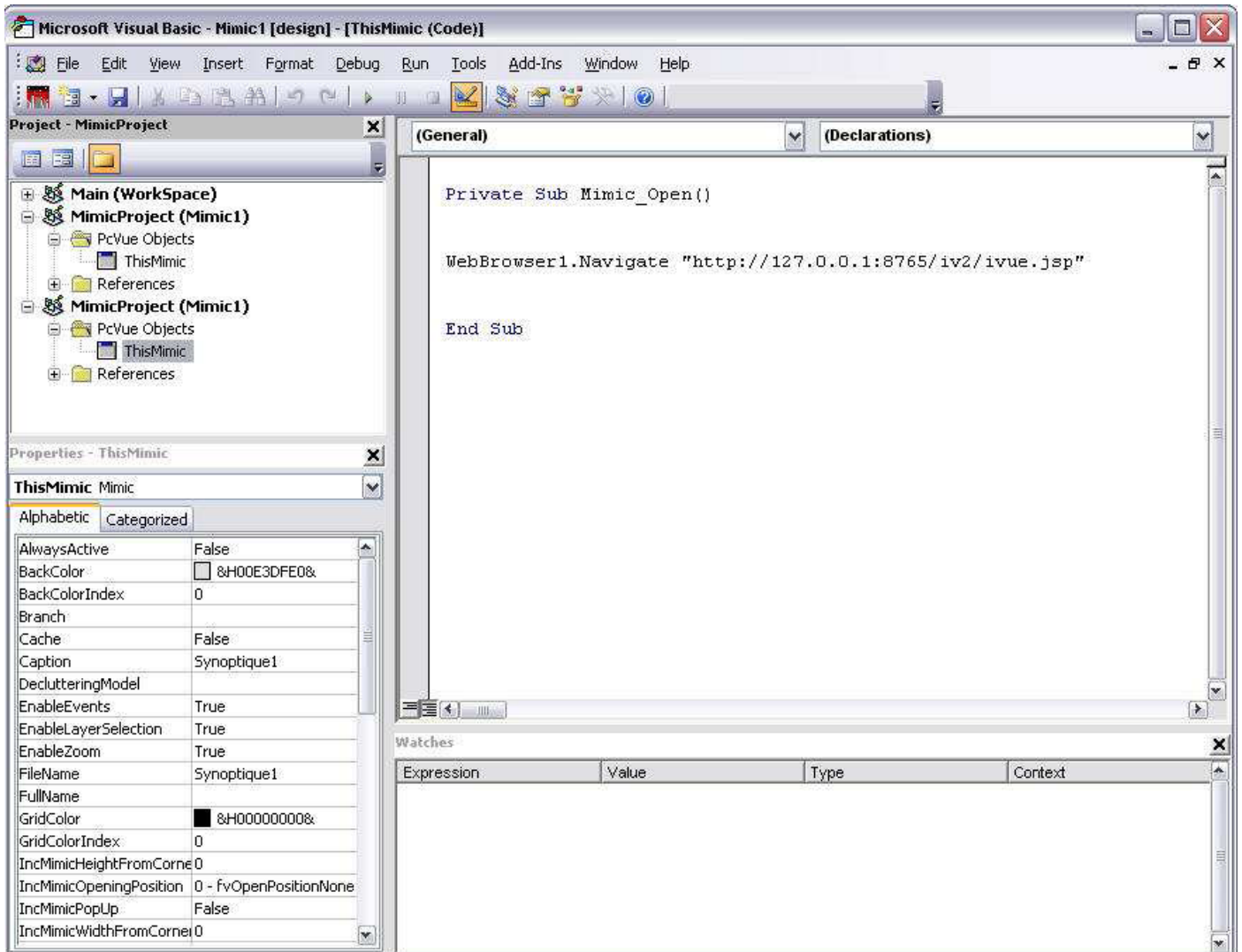
Sélectionnez dans l'arborescence du Projet : Mimic1 > PcVue Objects > ThisMimic

Ce chemin peut être différent selon le nom de votre synoptique.

Créez un sous programme appelé Mimic\_open() : ce sous programme sera exécuté au chargement du synoptique

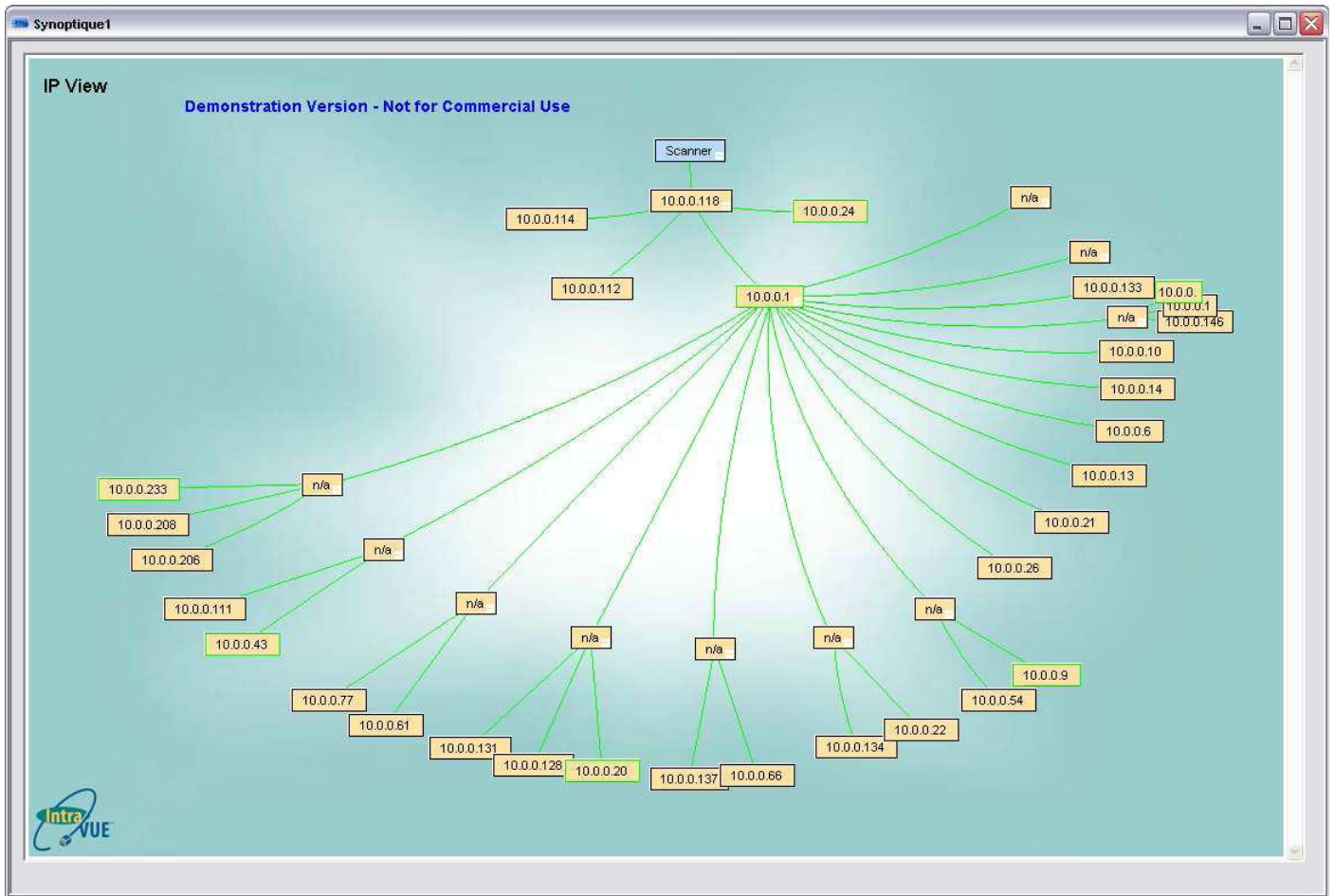
Enfin, saisissez l'adresse pointée par le contrôle ActiveX par l'instruction :

WebBrowser1.Navigate <http://127.0.0.1:8765/iv2/ivue.jsp>



Sauvegardez tout, fermez et ouvrez le synoptique concerné dans PcVue.

Le synoptique doit maintenant afficher la fenêtre principale d’Intravue :



## Établissement une communication entre Intravue et le SCADA

Cette communication nécessite dans un 1<sup>er</sup> temps de configurer Intravue afin de définir quelles sont les informations à mettre à disposition puis dans un 2<sup>nd</sup> temps de paramétrer dans le SCADA l'emplacement où allez chercher les informations.

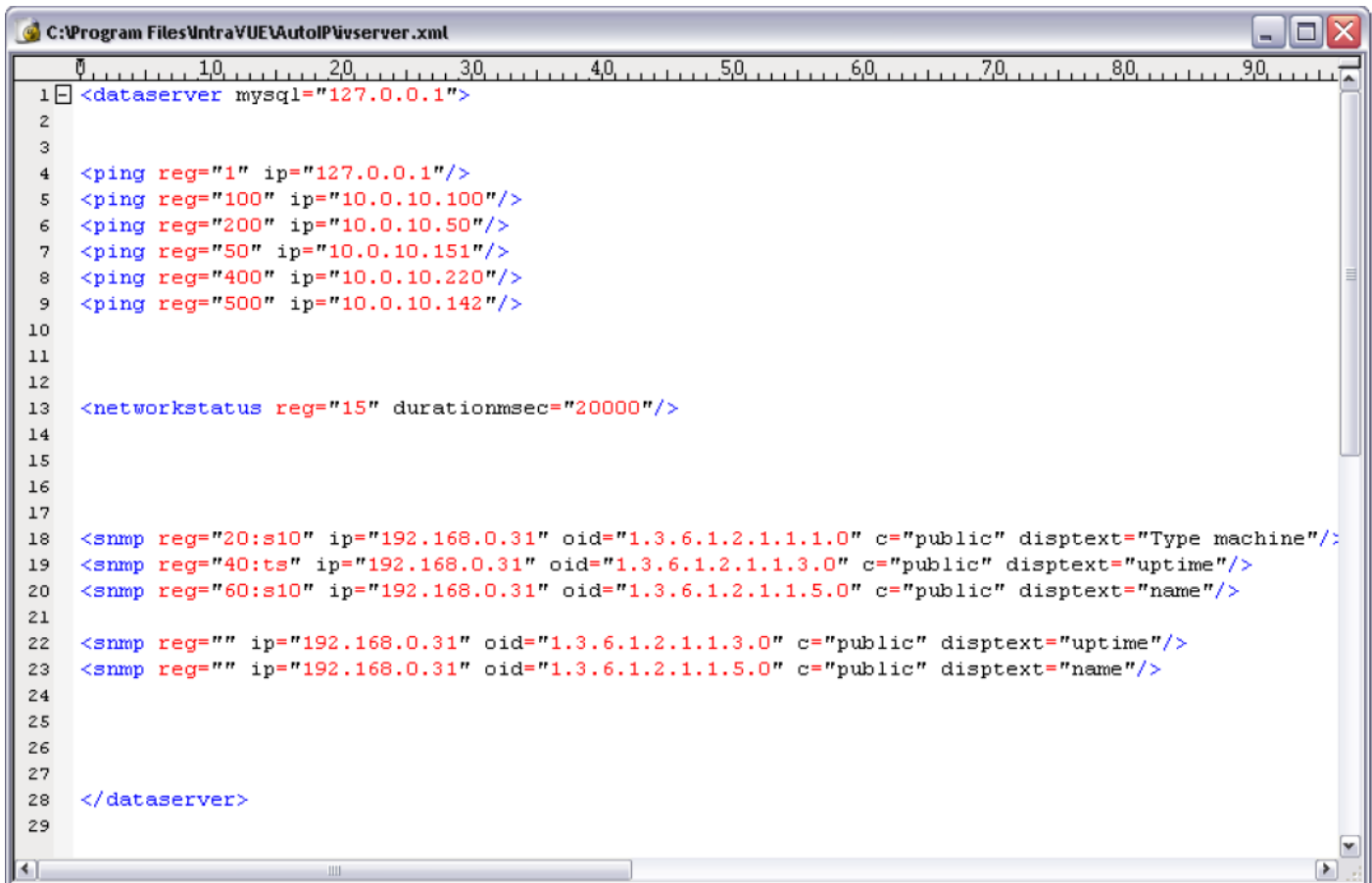
### Configuration d'Intravue

Pour partager des informations entre Intravue et PcVue, éditez le fichier ivserver.xml qui se trouve dans le répertoire d'installation d'Intravue  
(Par défaut : C:\Program Files\IntraVUE\AutoIP)

Ce fichier permet de renseigner le statut des périphériques réseau (Ping) et des variables SNMP dans des mots qui seront accessibles par PcVue via MODBUS TCP/IP.

Il permet donc de spécifier les variables à surveiller ainsi que leurs adresses réceptrives.

Ce fichier est en .xml et se compose ainsi :



```
1 <dataserver mysql="127.0.0.1">
2
3
4 <ping reg="1" ip="127.0.0.1"/>
5 <ping reg="100" ip="10.0.10.100"/>
6 <ping reg="200" ip="10.0.10.50"/>
7 <ping reg="50" ip="10.0.10.151"/>
8 <ping reg="400" ip="10.0.10.220"/>
9 <ping reg="500" ip="10.0.10.142"/>
10
11
12
13 <networkstatus reg="15" durationmsec="20000"/>
14
15
16
17
18 <snmp reg="20:s10" ip="192.168.0.31" oid="1.3.6.1.2.1.1.1.0" c="public" disptext="Type machine"/>
19 <snmp reg="40:ts" ip="192.168.0.31" oid="1.3.6.1.2.1.1.3.0" c="public" disptext="uptime"/>
20 <snmp reg="60:s10" ip="192.168.0.31" oid="1.3.6.1.2.1.1.5.0" c="public" disptext="name"/>
21
22 <snmp reg="" ip="192.168.0.31" oid="1.3.6.1.2.1.1.3.0" c="public" disptext="uptime"/>
23 <snmp reg="" ip="192.168.0.31" oid="1.3.6.1.2.1.1.5.0" c="public" disptext="name"/>
24
25
26
27
28 </dataserver>
29
```

Chaque balise **ping** se compose de deux attributs :

**reg** : Adresse du mot où sera placé l'information (0 pas de réponse, 1 OK),

**ip** : Adresse IP du périphérique réseau à surveiller

Chaque balise **networkstatus** se compose de deux attributs :

**reg** : Adresse du mot où sera placé l'information

**durationmsec** : Temporisation avant passage à 1

Les informations détectées et stockées dans ce registre sont les suivantes :

Bit 0 : nouveau périphérique connecté

Bit 1 : périphérique déconnecté

Bit 2 : périphérique reconnecté

Bit 3 : seuil dépassé

Chaque balise **snmp** se compose de cinq attributs :

**reg** : Adresse du mot où sera placé l'information + un champ optionnel donnant le type de l'information. Attention, certains types de données peuvent utiliser plus d'un seul mot.

:i entier sur 16 bits (utilise 1 mot)

:d entier sur 32 bits (utilise 2 mots)

:f flottant sur 32 bits (utilise 2 mots)

:ts format particulier du :f (utilise 2 mots)

:s<nombre> chaîne de caractères conforme aux standards MODBUS TCP/IP (utilise <nombre> mots)

Si ce champ optionnel n'est pas renseigné :i sera pris en compte par défaut.

**ip** : Adresse IP du périphérique réseau à surveiller.

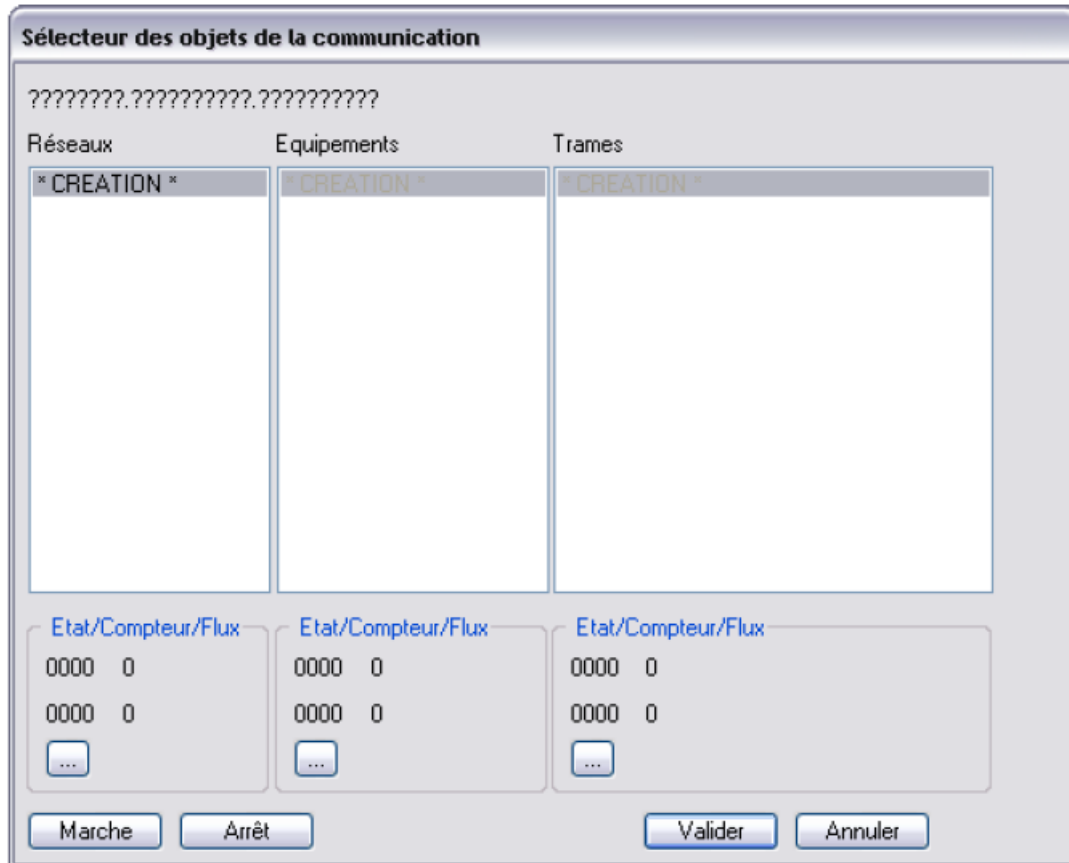
**oid** : ID de l'objet fournie par le constructeur.

**c** : Nom du groupe SNMP pouvant accéder au données.

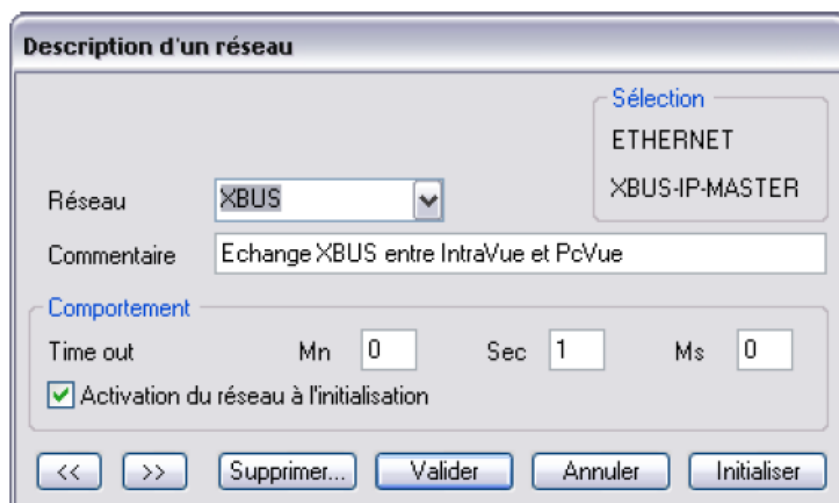
**disptext** : Champ texte optionnel pour affichage dans IntraVue

## Configuration PcVue

Premièrement, vous devez configurer un nouveau réseau par le menu Configuration > Communications/Equipements



Dans la partie « Réseaux », sélectionner « CREATION » et créez le réseau ETHERNET > XBUS-IP-MASTER comme ceci :



Puis un nouvel équipement :  
L'adresse IP doit être celle de la machine qui héberge IntraVue.

### Description d'un équipement

Réseau	XBUS	Sélection	
Équipement	INTRAVUE	SCHNEIDER	
		XBUS-IP-MASTER	
Commentaire	Machine IntraVue		

**Caractéristiques**

Type d'équipement	JBUS_DEC	<input type="checkbox"/> Virtuel	
Délai de retour	Mn 0	Sec 0	Ms 0

**Horodatage**

<input type="checkbox"/> Activer	Adresse Erreur	0
----------------------------------	----------------	---

**Point de connexion**

Adresse sur le réseau	10	0	0	118
Numéro de port	502	Adresse de l'esclave	1	

Redondance...

**Comportement**

<input type="checkbox"/> Utiliser uniquement fonctions d'écriture 15 et 16			
Time out spécifique	Mn 0	Sec 1	Ms 0
<input checked="" type="checkbox"/> Activation de l'équipement à l'initialisation			

Options avancées...

<< >> Supprimer... Valider Annuler Initialiser

Enfin les différentes trames :

Exemple 1 : Trame de Word bits afin de récupérer les Statuts du réseau à l'adresse 15

**Description d'une trame**

Réseau	XBUS	<b>Sélection</b>	
Equipement	INTRAVUE	SCHNEIDER	
Trame	T_NETWORK_STATUS	XBUS-IP-MASTER	
Commentaire	<input type="text"/>		

**Caractéristiques**

Format de la trame	BIT		
Autorisations d'accès	<input checked="" type="checkbox"/> Lecture	<input type="checkbox"/> Ecriture	
Adresse : ...	de	WordBit I/O LM 00015	<input type="button" value="↓"/>
	à	WordBit I/O LM 00015	

**Comportement**

<input type="checkbox"/> Mode prioritaire			
<input checked="" type="checkbox"/> Accès répétitif	<input checked="" type="radio"/> Lecture	<input type="radio"/> Ecriture	
Intervalle de répétition	Mn	0	Sec 1 Ms 0

<< >> Supprimer... Valider Annuler Initialiser

# Module : Outils Complémentaires

## Aide en Ligne

Une aide en ligne très complète est disponible dans Intravue. Veuillez-vous y référer concernant toutes questions que vous auriez concernant le fonctionnement d'un point particulier de configuration ou d'utilisation d'Intravue.

## Forum

Un forum utilisateur est disponible sous <http://www.NetworkVisionSoftware.com/forum>. Il contient de l'aide additionnel et des outils. Les utilisateurs disposant d'un contrat de maintenance peuvent poser des questions et télécharger des mises à jour.

## Vidéos

Des fichiers vidéo d'Aide sont disponibles en téléchargement sur <http://i-vue.com/IntraVUE/IntraVUECD2.iso>



Notez que ce fichier fait de plus de 200 Mo et peut prendre un certain temps à être télécharger. Le téléchargement est fait sous la forme d'un fichier ISO qui peut être gravé sur un CD. Après le téléchargement, utilisez les instructions de votre graveur de CD pour créer un CD à partir de la norme ISO-9660 de fichier d'image. Le résultat est exactement le même que le CD 2.