Tech Tips

RESUME

La multiplication des périphériques compatibles Ethernet sur les sites d'exploitation (des automates programmables aux modules E/S jusqu'aux capteurs) pour supporter l'Internet industriel des objets (IIoT), les communications et les autres besoins de données exigent une vigilance constante contre les perturbations du trafic Ethernet pouvant avoir de graves conséquences pour un réseau de contrôle/commande. Cette Astuce Technique fournit un aperçu général des types de « traffic storms » (tempêtes de trafic) sur Ethernet et de certaines techniques pouvant être utilisées pour prévenir et atténuer chaque type de tempête.

Comme les réseaux de contrôle de commande dépendent de plus en plus d'Ethernet pour les communications, il est plus important que jamais de configurer et d'exploiter correctement vos réseaux Ethernet afin d'éviter les problèmes potentiellement graves que peuvent causer les « traffic storms » Ethernet. Bien que les tempêtes de diffusion soient la principale préoccupation des entreprises, le trafic multidiffusion et monodiffusion peut parfois atteindre des niveaux susceptibles de compromettre les performances du système de contrôle. La mesure la plus importante que vous puissiez prendre pour assurer le bon fonctionnement de votre réseau est de le configurer correctement dès le début. Mais même si vous avez configuré votre réseau correctement, il existe d'autres raisons pour lesquelles vous risquez de rencontrer des problèmes de trafic réseau.

Cette Astuce Technique vous aidera à comprendre les types de trafic Ethernet, les problèmes que peut engendrer un trafic excessif et certains moyens d'atténuer les problèmes potentiels.

Les différents types de trafic Ethernet

Pour diagnostiquer les problèmes de fiabilité du réseau, il est important de comprendre les types de paquets Ethernet pouvant être transportés par le réseau. Il existe trois types de trafic réseau Ethernet communs à tous les réseaux Ethernet et indispensables à leur bon fonctionnement : monodiffusion, multidiffusion et diffusion.

- Trafic de monodiffusion (Unicast) : paquets Ethernet adressés directement à l'adresse MAC d'un périphérique spécifique.
- Trafic de multidiffusion (Multicast) : paquets Ethernet dont l'adresse de destination est une adresse de groupe de multidiffusion. Les périphériques Ethernet qui souhaitent traiter ces paquets sont configurés pour écouter une adresse de groupe particulière.
- Trafic de diffusion (Broadcast) : paquets Ethernet dont l'adresse de destination est l'adresse de diffusion. Tous les appareils connectés au même réseau Ethernet reçoivent des paquets de diffusion.

Bien que les trois types de trafic Ethernet soient communs à tous les réseaux Ethernet, un trafic excessif, quel qu'il soit, peut causer des problèmes pour un réseau Ethernet, en particulier pour un réseau de contrôle de commande industriel avec de grands volumes de messages.

Peut-il y avoir trop d'une bonne chose ?

Le trafic Ethernet excessif est souvent appelé «tempête de trafic» ou « traffic storm ». Le type le plus courant de tempête de trafic est une tempête de diffusion, mais le trafic de multidiffusion et de monodiffusion peuvent également poser problème à votre réseau de contrôle.

Plusieurs protocoles modernes d'E/S Ethernet reposent sur des messages de multidiffusion et, lorsqu'un réseau contient un grand nombre d'appareils utilisant des protocoles de multidiffusion, la charge du réseau peut augmenter considérablement. Lorsque plusieurs systèmes SCADA interrogent de grandes quantités de données, même le trafic de monodiffusion peut parfois atteindre un niveau où des problèmes peuvent survenir.

Les paragraphes suivants abordent les différents types de tempêtes de trafic réseau et les moyens de les prévenir et de les atténuer. Afin de déterminer quel type de trafic (et quel périphérique) est à l'origine de votre tempête de trafic, il est généralement nécessaire d'utiliser un analyseur de protocole ou un «renifleur de paquets» (packet sniffer) pour capturer et analyser le trafic réseau. Chez CTI, nous préférons utiliser Wireshark, un analyseur de protocole réseau gratuit à code source ouvert. Bien que cet article ne tente pas de fournir d'autres informations sur l'utilisation de Wireshark ou de tout autre analyseur de protocole réseau, il existe une multitude d'informations disponibles sur Internet. Nous vous recommandons la lecture de l'article de Brian Hill www.arstechnica.com/information-technology/2016/09/the-power-of-protocol-analyzers/.

Trafic en envoi individuel (Unicast) : comment les niveaux élevés peuvent-ils affecter le système de contrôle?

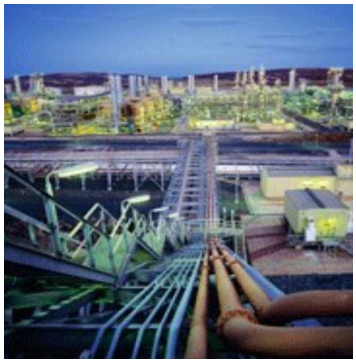
L'API compatible Ethernet typique détecte plusieurs sources de trafic Unicast, notamment :
- Systèmes SCADA interrogeant l'automate pour obtenir des données
- Panels IHM interrogeant l'automate pour obtenir des données
- Autres automates interrogeant des données
- PC exécutant des opérations de programmation

Chaque paquet Ethernet reçu par l'automate provoque une «interruption», nécessitant des ressources processeur pour supprimer le paquet du tampon de réception et l'enregistrer pour traitement ultérieur au cours de la tâche de communication. Lorsque des débits de monodiffusion élevés surviennent, le processeur de l'automate peut passer un temps considérable dans ce traitement d'interruption. Si le débit de paquets devient excessif, des temps de traitement plus importants et plus longs sont nécessaires, entraînant une dégradation des tâches de contrôle de processus et la perte de paquets Ethernet.

Les switch Ethernet apprennent l'adresse MAC des périphériques communiquant avec chaque port du switch. Une fois que l'adresse MAC est connue, le switch transmet uniquement les paquets de monodiffusion avec une destination de monodiffusion donnée au port correspondant. L'interface réseau d'un périphérique Ethernet bloque la réception de tous les paquets de monodiffusion, à l'exception de ceux dont l'adresse de destination est égale à l'adresse MAC de l'interface. Pour ces raisons, un chargement excessif dû à des paquets de monodiffusion est moins probable. Néanmoins, il est toujours possible sous certaines conditions, y compris les suivantes :
- Un grand nombre de périphériques, tels que les systèmes SCADA/IHM, interrogent rapidement les données. Alors que le débit moyen des paquets est souvent acceptable, le trafic de ces systèmes a tendance à être en rafales - une rafale de paquets suivie d'une période sans paquets. À mesure que le nombre de périphériques augmente, les rafales de plusieurs périphériques se chevauchent, entraînant des pics de trafic importants.
- Périphériques mal configurés envoyant par erreur à l'adresse IP du périphérique.
- Des attaques par déni de service (DoS), dans lesquelles une multitude de paquets sont envoyés à l'adresse Unicast afin de dégrader le fonctionnement.

Atténuation des problèmes de trafic monodiffusion (Unicast)

Selon votre cas, les actions suivantes peuvent résoudre les problèmes de trafic monodiffusion:
- Réduisez le taux d'interrogation des systèmes SCADA/IHM, si possible. La plupart de ces systèmes interrogent plus rapidement que nécessaire (deux fois plus rapidement que la période de mise à jour requise).
- Localisez et reconfigurez / désactivez les périphériques incriminés.
- Connectez l'appareil à un commutateur capable de limiter le débit. Configurez le commutateur pour limiter le transfert de paquets à un débit de paquets acceptable. Comme la limitation du débit peut mettre en mémoire tampon les paquets Ethernet, elle peut être utilisée pour niveler les pics de trafic.
- Utilisez un module de communication CTI, tel qu'un module 2572-B ou 2500P-ECC1 pour les communications réseau.



Trafic de multidiffusion (Multicast) : une cause fréquemment ignorée des problèmes de réseau de contrôle

Correctement implémentée, la messagerie multicast est une méthode de communication efficace pour votre système de contrôle lorsque les mêmes données doivent être transmises à plusieurs destinataires. Ethernet/IP utilise souvent la multidiffusion pour les communications entre l'automate et les périphériques d'E/S.
Cependant, dans certaines circonstances, le trafic de multidiffusion peut créer des problèmes. Le trafic de multidiffusion (Multicast) a tendance à avoir des débits de paquets plus élevés que le trafic monodiffusion (Monocast), car il n'est pas nécessaire d'attendre que le périphérique réponde.
Par défaut, Ethernet bascule les paquets de multidiffusion sur tous les ports du switch, propageant ainsi ces paquets sur le réseau Ethernet. Combiné à des débits élevés de trafic de multidiffusion (par exemple, avec des E/S Ethernet/IP), ce comportement peut avoir un impact négatif sur le fonctionnement des périphériques réseau.
La plupart des périphériques permettent toujours au trafic de multidiffusion de passer par l'interface Ethernet. Ce trafic comprend des paquets avec des adresses de multidiffusion liées au contrôle du réseau et à la gestion du groupe de multidiffusion. Par conséquent, le trafic multidiffusion peut toujours provoquer des interruptions sur le périphérique.

Atténuation des problèmes de réseau en multidiffusion (Multicast)

Le trafic multicast ne posera pas de problème pour le processeur CTI 2500-Cxxx: il ne prend pas en charge la multidiffusion et est configuré pour bloquer la réception de tous les messages multicast. Pour empêcher le trafic de multidiffusion indésirable d'inonder d'autres produits CTI, vous disposez de plusieurs solutions. Si vous ne souhaitez pas utiliser vos produits compatibles CTI Ethernet pour les communications multidiffusion, vous pouvez les connecter à un switch supportant la surveillance IGMP (Internet Group Management Protocol). Cette fonctionnalité détecte les requêtes IGMP pour rejoindre un groupe de multidiffusion particulier et transmet le flux de multidiffusion associé uniquement au port connecté au périphérique demandeur. La plupart des switch supportant IGMP peuvent être configurés pour ignorer les flux de multidiffusion inconnus du commutateur. Si vous souhaitez que votre produit CTI reçoive un flux de multidiffusion, cette solution ne fonctionnera pas correctement, car le produit CTI doit répondre à une requête IGMP provenant d'un routeur. Les produits CTI actuels ne répondront pas à une requête IGMP car ils ont été conçus pour les communications multicast sur le réseau local uniquement.

Si vous souhaitez que votre produit CTI reçoive des messages de multidiffusion, vous pouvez également utiliser un switch Ethernet supportant le filtrage de multidiffusion par ponts. Cette fonctionnalité vous permet de définir de manière statique comment les paquets de multidiffusion sont transférés. Si vous souhaitez recevoir des paquets de multidiffusion avec une adresse de groupe particulière, vous pouvez attribuer de manière statique l'adresse du groupe au port. Vous pouvez également choisir d'empêcher tous les paquets de multidiffusion d'être transférés vers les ports désignés.

Si vous ne souhaitez pas ajouter de switch externe, vous pouvez également utiliser un produit CTI tel que le 2500P-ECC1 et / ou le 2500P-ACP1 qui utilise des switch intégrés qui limitent le taux de paquets de multidiffusion (et de diffusion). Bien que cette solution soit souvent efficace, il existe un risque de perte de paquets que vous souhaitez recevoir, car l'algorithme de limitation commence à ignorer les paquets lorsque le seuil maximal est dépassé.

Une solution plus globale consiste à segmenter votre réseau Ethernet, comme indiqué ci-dessous.

Trafic de diffusion (Broadcast) : le coupable le plus courant des perturbations de réseau

Le trafic de diffusion est nécessaire au bon fonctionnement de TCP/IP sur Ethernet. Par exemple, le protocole ARP (Address Resolution Protocol), qui détecte l'adresse MAC d'un périphérique avec une adresse IP connue, est requis pour transmettre des messages de monodiffusion TCP/IP via une liaison Ethernet. Comme indiqué précédemment, tous les périphériques d'un réseau Ethernet doivent consommer des ressources pour traiter le paquet de diffusion. Comme de plus en plus de périphériques sont ajoutés au réseau, le nombre de diffusions augmente naturellement.

Les tempêtes de diffusion se produisent lorsqu'un nombre anormalement élevé de messages de diffusion est envoyé dans un court laps de temps, ce qui congestionne les périphériques sur le réseau et provoque souvent des encombrements et des paquets perdus dans les commutateurs réseau.

Bien que les tempêtes de diffusion puissent simplement être une nuisance dans un réseau de bureau, elles peuvent être catastrophiques dans un réseau de contrôle/commande. En raison des contraintes de taille, de coût et d'alimentation, les périphériques d'un réseau de contrôle/commande ont généralement une puissance de traitement limitée par rapport à un ordinateur de bureau. De plus, ces ressources limitées doivent rester dédiées à la tâche de contrôle primaire pour assurer le bon fonctionnement des équipements.

Quelles sont les causes d'une tempête de diffusion (Broadcast) ?

Bien que plusieurs facteurs puissent contribuer à une tempête de diffusion, les causes les plus courantes sont les suivantes:

Combiner le réseau de l'usine avec le réseau informatique

Les réseaux informatiques génèrent souvent beaucoup de trafic de diffusion. Bien que ce niveau de diffusion soit acceptable pour le réseau informatique, il peut sérieusement dégrader les performances des systèmes de contrôle, qui nécessitent un fonctionnement en temps réel.

Réseaux de contrôle excessivement grands.

Même isolés du réseau informatique, les grands réseaux de contrôle eux-mêmes peuvent générer un trafic de diffusion trop important en raison du nombre de périphériques connectés au réseau et des protocoles utilisés.

Protocoles de contrôle mal conçus

Il n'est pas rare de trouver des communications Ethernet et des protocoles d'E/S non autorisés qui utilisent la diffusion Broadcast comme principal moyen de transmission de données. Ce sont généralement des protocoles hérités qui ont été développés lors les premières étapes de l'adoption d'Ethernet.

Défaillance Hardware/Schwith défectueux

Un commutateur, un routeur ou une interface réseau informatique défectueux peuvent inonder le réseau avec du trafic de diffusion. Cela vaut la peine d'investir dans un équipement de réseau de qualité équipé de fonctions de prévention contre les tempêtes.

Erreur humaine

Une erreur humaine courante se produit lorsqu'une boucle est créée par inadvertance, ce qui entraîne une répétition continue du trafic de diffusion sur le réseau. Une boucle peut être créée en connectant les deux extrémités d'un câble sur deux ports du même switch ou en créant une boucle entre plusieurs switch.

Prévention ou atténuation des tempêtes de diffusion

Il existe plusieurs manières de réduire l'apparition de tempêtes et / ou d'atténuer les perturbations du réseau causées par un orage.

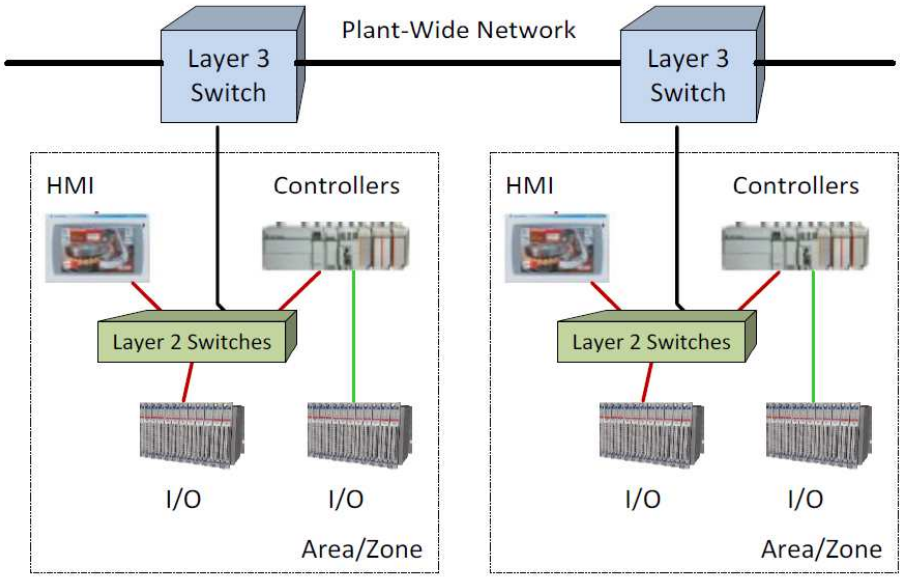
1. Isolez le réseau informatique du réseau de contrôle

Assurez-vous que votre réseau informatique d'entreprise est physiquement isolé de votre réseau de contrôles ou séparé de celui-ci par des routeurs et des pare-feu correctement configurés. Les routeurs acheminent les paquets TCP/IP monodiffusion et multidiffusion désignés, mais ne transmettent pas le trafic de diffusion. Les pare-feu limitent davantage les paquets TCP/IP qui seront acceptés. Ces composants réseau permettent des communications entre les bureaux administratifs et l'usine tout en empêchant les paquets de diffusion / multidiffusion / multidiffusion indésirables d'entrer dans le réseau de contrôle.

2. Divisez votre réseau de production en plus petits segments

L'un des meilleurs moyens de maîtriser le trafic de diffusion et de multidiffusion consiste à subdiviser le réseau en domaines de diffusion plus petits. La plupart des environnements de production peuvent naturellement être divisés en zones de travail automatisées par un ou plusieurs contrôleurs et les E/S associées. Chaque domaine de diffusion consisterait en un réseau local Ethernet (LAN) isolé, connecté au réseau de l'usine, via un commutateur de couche 3. Le commutateur de couche 3 assure le routage des paquets TCP/IP entre le réseau local et le réseau principal tout en fournissant des fonctions de commutation Ethernet (couche 2). Par conséquent, les paquets de diffusion provenant d'un réseau plus important ne sont pas transmis au réseau local. (voir la figure 1 ci-dessous).

Figure 1: Subdivided plant network.



3. Installez le contrôle de tempête de diffusion

L'un des moyens les plus simples et les plus efficaces pour minimiser les effets des tempêtes et des taux de paquets élevés consiste à installer un commutateur géré (managed switch). Tous les commutateurs gérés peuvent définir des limites de débit pour le trafic de diffusion. Beaucoup d'autres permettent également de limiter le débit du trafic multidiffusion et monodiffusion. À titre d'exemple, l'illustration ci-dessous (Figure 2) montre la page Web de configuration de Storm Control pour un commutateur géré Cisco à 8 ports. Ce commutateur permet de définir des limites de débit de paquets indépendantes pour le trafic de diffusion, multidiffusion et monodiffusion. Les limites de débit sont définies en % de la bande passante totale du réseau ou en paquets par seconde (pps). Pour les ports connectés aux produits CTI, il est recommandé de limiter le port à 1 000 paquets de diffusion / multidiffusion par seconde (1% d'une liaison de 100 Mo).

5. Formation du personnel

Pour réduire les erreurs humaines, il est important de former correctement tout le personnel qui interviendra sur le réseau. Avoir des connaissances de base sur le fonctionnement du réseau, y compris une compréhension des types de tempêtes et des moyens de les limiter/ atténuer, peut permettre de prévenir les erreurs, identifier les problèmes typiques et améliorer la capacité à signaler avec précision les anomalies au personnel. Avoir des techniciens qui peuvent utiliser un programme de capture réseau, tel que Wireshark, pour enregistrer des événements réseau peut considérablement améliorer la capacité du personnel du support client CTI à aider à résoudre un problème de communication.

Figure 2 : Page de configuration de contrôle de tempête d'un commutateur géré Cisco à 8 port

Storm Control

Storm Control Table

			Broadcast Storm Control			Multicast Storm Control			Unicast Storm Control		
	Entry No.	Port	Mode	Threshold	Threshold Type	Mode	Threshold	Threshold Type	Mode	Threshold	Threshold Type
○	1	g1	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	2	g2	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	3	g3	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	4	g4	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	5	g5	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	6	g6	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	7	g7	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps
○	8	g8	Enable	1000	pps	Enable	1000	pps	Enable	1000	pps

4. Protection contre les boucles de commutateur d'outil

De nombreux switch Ethernet modernes offrent une fonction de détection de bouclage qui empêche la création accidentelle d'une boucle. La fonctionnalité fonctionne en transmettant périodiquement des paquets de protocole de boucle à partir d'un port activé pour la détection de bouclage. Si le même paquet est reçu ultérieurement par le port, le port est automatiquement désactivé, ce qui arrête la propagation en boucle de paquets. La plupart des commutateurs d'aujourd'hui prennent en charge le protocole RSTP (Rapid Spanning Tree Protocol) pour conserver la topologie du réseau sans boucles lors de l'utilisation de réseaux redondants. RSTP, les boucles et la redondance réseau sont des sujets avancés qui ne sont pas abordés par cette Astuce Technique.

Conclusion

Ethernet continue de révolutionner les systèmes de contrôle industriels. À mesure que les fabricants explorent «l'Internet des objets industriel» (IIoT) et implémentent de plus en plus de périphériques Ethernet, il est de plus en plus important de comprendre et de gérer les risques de tempêtes de trafic Ethernet. Cette astuce technique a fourni une vue d'ensemble des risques liés aux tempêtes de trafic et des mesures à prendre pour les prévenir ou les atténuer.

Contactez-nous si vous avez besoin de plus d'information sur ce sujet