Les protocoles

Protocoles WEB

HTTP (HyperText Transfer Protocol) TCP port 80

HTTP est un protocole de **chouche application** permet aux utilisateurs de se connecter aux sites Web sur Internet

HTTPS (Http Secure) TCP port 443

HTTPS est un protocole de **chouche application** peut procéder à l'authentification et au chiffrement pour sécuriser les données pendant qu'elles circulent entre le client et le serveur

Protocole de transfert des fichiers

FTP (File Transfer Protocol) TCP port 20 , 21

FTP est un protocole de **couche application** pour permettre le transfert de données entre un client et un serveur

Protocoles de messagerie

SMTP (Simple Mail Transfer Protocol) TCP port 25

SMTP est un protocole de **couche application** permet de transférer les e-mails de manière fiable et efficace vers le destinataire

POPv3 (Post Office Protocol) TCP port 110

POP est un protocole de **couche application** permet à un ordinateur de récupérer des e-mails à partir d'un serveur de messagerie. Avec POP, l'e-mail est téléchargé du serveur au client, puis supprimé du serveur.

IMAPv4 (Internet Message Access Protocol) TCP port 143

IMAP est un protocole de **couche application** décrit une autre méthode de récupération des messages électroniques (sauvegarde centralisée). l'e-mail est téléchargé du serveur au client et Les messages originaux sont conservés sur le serveur jusqu'à ce qu'ils soient supprimés manuellement.

Protocole de résolution des noms

DNS (Domain Name System) TCP and UDP port 53

DNS est un protocole de **couche application** permettre la résolution de nom pour ces réseaux.

- ✓ **ipconfig /displaydns** : afficher toutes les entrées DNS mises en cache sur un système Windows.
- ✓ **ipconfig /flushdns** : effacer cache DNS

- ✓ **nslookup (name server lookup) :** Cet utilitaire permet également de résoudre les problèmes de résolution de noms et de vérifier l'état actuel des serveurs de noms.

LLMNR (Link-local Multicast Name Resolution) UDP port 5355

LLMNR est un protocole permet la résolution de noms sur un réseau local. (pour les requêtes en multicast adresse 224.0.0.252 en IPv4 et ff02 ::1 :3 en IPv6).

- Windows va effectuer les recherches via plusieurs mécanisme pour tenter de trouver \\srvinconnu :

  - Recherche en utilisant le HOST local de la machine (C:\Windows\System32\drivers\etc\hosts);
  - S'il ne trouve rien: recherche dans le cache DNS local (ipconfig /displaydns);
  - S'il ne trouve rien: recherche dans le/les DNS configuré(s) dans la carte réseau;
  - S'il ne trouve rien: recherche NetBIOS en utilisant NBT-NS et en broadcastant le subnet;
  - Si personne ne lui répond: recherche en utilisant LLMNR et en diffusant sur l'adresse multicast;
  - Si personne ne lui répond: échec de la recherche. Partage réseau introuvable.

NetBIOS (NETwork Basic Input Output System) UDP port 137, 138, 139

NetBIOS un système de nommage de **couche application** et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau. NetBIOS fonctionne sur le principe des diffusions (broadcast)

Protocole d'attribution Automatique des Adresses

BOOTP (Bootstrap Protocol) UDP port 67, 68

BOOTP pour fournir une adresse IP pendant le processus d'amorçage ou pendant le démarrage de l'ordinateur

DHCP (Dynamic Host Configuration Protocol) UDP port 67, 68

DHCP est un protocole de **couche application** permet aux périphériques d'un réseau d'obtenir d'un serveur DHCP des paramètres TCP/IP pour une durée définie

Fonctionnement de protocole DHCP :

- **DHCPDISCOVER :** le client diffuse un message de détection DHCP pour identifier les serveurs DHCP disponibles sur le réseau
- **DHCPOFFER :** Un serveur DHCP répond par un message d'offre DHCP , qui offre un bail (lease sur windows 8j .sur cicso : 1j) au client
- **DHCPREQUEST :** Le client peut recevoir plusieurs messages DHCPOFFER, Il doit donc effectuer un choix qui identifie explicitement le serveur et l'offre de bail qu'il accepte
- **DHCPACK :** le serveur renvoie un message DHCP confirmant au client que le bail est conclu.

Protocoles d'accès à distance

Telnet (Terminal Network) TCP port 23 (Remote login)

Telnet protocole de **couche application** utilisé pour permettre un accès distant aux serveurs et aux périphériques réseau. Les données contenues dans un paquet Telnet sont transmises en clair.

SSH (Secure Shell) TCP port 22

SSH protocole de **couche application** fournit une connexion à distance plus sécurisés. SSH fournit une authentification et emploie un chiffrement lors du transport des données de la session

Protocole de partage

SMBv3 (Server Message Block) TCP port 445

SMB est un protocole de **couche application** de partage de fichiers client/serveur, décrit l'accès au système de fichiers et la manière dont les clients peuvent demander des fichiers.

Protocole de sauvegarde des fichiers

TFTP (Trivial File Transfere Protocol) UDP port 69

TFTP ce protocole de **couche application** est utilisé pour le transfert actif de fichiers sans connexion. Les copies des fichiers de configuration doivent être stockées en tant que fichiers de sauvegarde pour parer à toute éventualité. Les fichiers de configuration peuvent être stockés sur un serveur TFTP (Trivial File Transfer Protocol) ou sur un périphérique de stockage USB

Protocoles de transport

TCP (Transmission Control Protocol)

TCP est un protocole fiable de **couche transport** permettant d'assurer un acheminement fiable des données entre les applications par l'utilisation d'accusés de réception

- Acheminement Fiable
- Orienté "connexion"
- une reconstitution ordonnée des données
- le contrôle de flux (Flow control)

UDB (User Datagram Protocol)

UDP est un protocole de **couche transport** très simple qui ne permet pas de garantir la fiabilité

- Acheminement non fiable
- Orienté Sans connexion "non connexion"
- Aucune reconstitution ordonnée des données
- Aucun contrôle de flux

Protocoles réseaux

ICMP (Internet Control Message Protocol) N° de protocole 1

ICMP esy un protocole de **couche réseau** Permet de gérer les informations relatifs aux erreurs générées au sein d'un réseau IP

IGMP (Internet Group Management Protocol) N° de protocole 2

IGMP est un protocole de **couche réseau** qui permet à des routeurs IP de déterminer de façon dynamique les groupes multicast qui disposent de clients dans un sous-réseau.

Ipv4 (Internet Protocol) N° de protocole 4

Ip est protocole de **couche réseau** Il permet de mettre en œuvre la transmission de données entre des hôtes situés sur un même réseau ou sur des réseaux différents

Protocoles de liaison de données

ARP (Address Resolution Protocol)

ARP est un protocole de couche **lialison de données** qui permet de trouvez les adresses MAC à partir des adresses IP

RARP (Reverse Address Resolution Protocol)

RARP est un protocole de couche **lialison de données** qui permet de trouvez les adresses IP à partir des adresses MAC

LLC (Link Layer Control)

LLC fournit l'adressage et le contrôle de la liaison de données. Il spécifie quels mécanismes doivent être utilisés pour adresser des stations sur le support de transmission et pour le contrôle de l'échange des données entre la machine

MAC (Media Access Control)

MAC aussi appelée adresse physique de **lialison de données** , Utilisée pour identifier de manière unique un périphérique réseau,

Protocoles de découverte des voisins

CDP (Cisco Discovery Protocol) port 161 , 162 are used by SNMP

CDP est un protocole de couche **liaison de données** propriétaire détecte tous les autres périphériques Cisco connectés directement

LLDP (Link Layer Discovery Protocol)

LLDP est un protocole open standard de couche **liaison de données** détecte tous les autres périphériques Cisco connectés directement

Protocoles de routage

RIP (Routing Information Protocol)UDP port 520

RIP est protocole de routage de couche **réseau** à vecteur de distance par classe, (RIPv2 protocole sans classe)

RIPng : RIP next generation UDP port 521

RIP est protocole de routage Ipv6 de couche **réseau** à vecteur de distance sans classe

OSPF (Open Shortest Path First) N° de protocole 89

OSPF est un protocole de routage de **couche réseau** libre à état de lien et sans classe

EIGRP (Enhanced Internet Gateway Rounting Protocol) RTP N° de protocole 88

EIGRP est un protocole de routage de **couche réseau** de type vecteur de distance avancé utilise le protocole (RTP)

RTP (Real-time Transport Protocol)

RTP est un protocole pour l'acheminement et la réception des paquets EIGRP

IS-IS (Intermediate System - Intermediate System)

IS-IS est un protocole de routage de couche à état de liens sans classe

Protocole de Trunking

ISL (Inter-Switch Link)

ISL est un protocole propriétaire qui permet de transférer des trames ethernet avec leur numéro de VLAN entre deux commutateurs ethernet ou entre un commutateur et un routeur.

802.1Q (dot1q)

802.1q C'est le rôle du marquage ou de l'étiquetage de trames : il attribue à chaque trame un code d'identification de VLAN unique

Protocoles de négociation

DTP (Dynamic Trunking Protocol)

DTP est un protocole de **couche réseau** propriétaire de Cisco, permettant de gérer dynamiquement l'activation/désactivation du mode trunk d'un port sur un commutateur réseau par la négociation entre les commutateurs

Protocoles de VOIP

SIP (Session Initiation Protocol)

SIP est un protocole de signalement utilisé pour établir une "session" entre deux ou plus de participants

Types des protocoles STP

Le protocole STP IEEE 802.1D

STP utilise l'algorithme Spanning Tree (STA, Spanning Tree Algorithm) pour déterminer quels sont les ports de commutation d'un réseau à bloquer (état de blocage) pour empêcher la formation de boucles.

PVST+ (Per Vlan Spanning Tree)

PVST+ version améliorée du protocole STP proposée par Cisco, qui offre une instance Spanning Tree 802.1D séparée pour chaque VLAN configuré dans le réseau

RSTP (Rapid Spanning Tree Protocol) ou IEEE 802.1w

RSTP version évoluée du protocole STP, qui offre une convergence plus rapide.

Rapid PVST+ (Rapid Per Vlan Spanning Tree)

Rapid PVST+ version améliorée du protocole RSTP proposée par Cisco et utilisant PVST+. **Rapid PVST+** offre une instance 802.1w séparée pour chaque VLAN.

MSTP (Multiple Spanning Tree Protocole)

MSTP version IEEE standard inspirée par l'implémentation propriétaire de Cisco MISTP (Multiple Instance STP). MSTP mappe plusieurs VLAN dans une même instance Spanning Tree

Protocoles Etherchannel

PAgP (port aggregation protocol)

PAgP est un protocole propriétaire qui facilite la création automatique de liaisons EtherChannel.

LACP (link aggregation control protocol)

LACP 802.3ad qui permet de regrouper plusieurs ports physiques pour former un seul canal logique.

Protocoles VLAN

VTP (Vlan Trunking Protocol)

VTP est un protocole **couche liaison de données** utilisé pour configurer et administrer les VLAN sur les périphériques Cisco.

Protocoles d'authentification

AAA (Authentication Authorization Accounting)

AAA est un protocole qui réalise trois fonctions : l'authentification, l'autorisation, et la traçabilité

LDAP (Lightweight Directory Access Protocol)

LDAP permet d'accéder à des bases d'informations sur les utilisateurs d'un réseau, via l'interrogation d'annuaires

802.1x (dot1x) suite de protocole

802.1x Le protocole 802.1x est une extension du protocole EAP aux environnements LAN. Ce

protocole est utilisé pour transporter les informations d'authentification entre deux équipements.

EAP (Extensible Authentication Protocol)

EAP est utilisé pour le transport et la gestion de l'authentification entre le Supplicant et le serveur d'authentification.

Protocoles Sans fil

WEP (Wired Equivalent Privacy)

WEP 802.11 offrir un degré de confidentialité similaire à une connexion réseau filaire.

WPA (Wi-Fi Protected Access)

WPA norme Wi-Fi Alliance utilisant la technologie WEP, mais qui sécurise les données à l'aide d'un algorithme de chiffrement **TKIP** (Temporal Key Integrity Protocol)

TKIP (Temporal Key Integrity Protocol)

TKIP modifie la clé pour chaque paquet, rendant très difficile son piratage.

WPAv2 (Wi-Fi Protected Access Version 2)

WPAv2 utilisent toutes deux l'Advanced Encryption Standard (**AES**). Le mode de chiffrement **AES** est actuellement considéré comme étant le protocole de chiffrement le plus puissant.

Protocoles Point-to-Point

SLIP (Serial Line Internet Protocol)

SLIP est un protocole normalisé pour les connexions série point à point sur TCP/IP. SLIP a été largement remplacé par PPP.

PPP (Point-to-Point Protocol)

PPP fournit les connexions routeur à routeur et hôte à réseau sur les réseaux synchrones et asynchrones. Ce protocole PPP fonctionne avec différents protocoles de couche réseau

LCP (Link Control Protocol)

LCP fonctionne avec la **couche de liaison de données** et joue un rôle dans l'établissement, la configuration et le test de la connexion de liaison de données. Il établit la liaison point à point. Il négocie également et configure les options de contrôle sur la liaison de données de réseau étendu, qui sont gérées par les protocoles NCP.

NCP (Networl Control Protocol)

Les NCP comportent des champs fonctionnels contenant des codes standardisés indiquant le type de protocole de couche réseau encapsulé par le protocole PPP

PAP (Password Authentication Protocol)

PAP est un processus bidirectionnel simple. Il ne comporte pas de chiffrement. Le nom d'utilisateur et le mot de passe sont envoyés en texte clair. S'ils sont acceptés, la connexion est autorisée.

CHAP (Challenge Handshake Authentication Protocol)

CHAP est plus sécurisé que le protocole PAP. Il implique un échange en trois étapes d'un secret partagé.

Protocoles de tunneling utilisés pour la connexion VPN

GRE (Generic Routing Encapsulation)

GRE est un exemple de protocole de tunneling VPN de site à site de base, non sécurisé.

PPTP (Point-to-Point Tunneling Protocol)

PPTP Permet de chiffrer et d'encapsuler le trafic multiprotocole qui est ensuite envoyé sur un réseau IP ou sur réseau IP public comme Internet. Vous pouvez utilisez PPTP pour les connexions d'accès à distance et les connexions VPN de site à site.

- **Encapsulation :** PPTP utilise le protocole GRE pour encapsuler des trames PPP pour les données en tunnel
- **Chiffrement :** PPTP crypte le trafic avec le chiffrement Microsoft Point-to-Point (MPPE, Microsoft Point-to-Point Encryption) à l'aide des clés de chiffrement générées par le processus d'authentification MS-CHAPv2 ou EAP-TLS

L2TP (Layer 2 Tunneling Protocol) UDP 500

L2TP est une combinaison des protocoles PPTP et L2F (Layer 2 Forwarding), il regroupe les meilleures fonctionnalités des deux. L2TP s'appuie sur IPsec pour le chiffrement des données. La combinaison des protocoles L2TP et IPsec est appelée L2TP/IPsec

- **Encapsulation :** l'encapsulation de paquets L2TP/IPsec est formée de deux couches : l'encapsulation L2TP et l'encapsulation IPsec
- **Chiffrement:** l'encapsulation de paquets L2TP est chiffré avec l'algorithme DES ou 3DES

IPsec (IP Secure)

IPsec c'est un suite de protocole (open standard) Les VPN IPsec offrent une connectivité à la fois flexible et évolutive. Les connexions de site à site peuvent assurer une connexion à distance fiable, rapide et sécurisée.

SSTP (Secure Socket Tunneling Protocol)

SSTP utilise le protocole HTTPS (Secure Hypertext Transfer Protocol) pour faire transister le trafic à travers des pare-feux et des proxy Web qui peuvent bloquer le trafic PPTP et L2TP/IPsec. Le SSTP propose un mécanisme permettant d'encapsuler le trafic PPP sur le canal SSL du protocole HTTPS

- **Encapsulation :** SSTP encapsule des trames PPP dans un datagramme IP en vue de la transmission sur le réseau.
- **Chiffrement :** le message SSTP est chiffré avec le canal SSL du protocole HTTPS

SSL (Secure Socket Layer) / TLS (Transport Layer Security)

SSL est le protocole de sécurité le plus répandu qui crée un canal sécurisé entre deux machines communiquant sur Internet ou un réseau interne.
Le SSL est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web.

IKEV2 (Internet Key Exchange version 2)

IKEV2 est un protocole de cryptage VPN qui gère les actions de requête et de réponse. Il s'assure que le trafic est sécurisé en établissant et en gérant l'attribut SA (Security Association) au sein d'une suite d'authentification, généralement IPSec, car IKEv2 est basé sur celui-ci et y est intégré. C'est un protocole idéal pour les appareils mobiles.

Protocole de Temps

NTPv4 (Network Time Protocol) : UDP 123

NTP est un protocole de **couche application** qui permet de synchroniser à travers le réseau l'horloge locale des ordinateurs sur une date et une heure de référence. Il existe d'autre protocoles comme (SNTP ET PNTP)

SNTP est le protocole de distribution et de synchronition de l'heure. Il est impératif que toutes les machines du domaine Windows disposent de la meme heure afin de sycnhroniser leurs actions

Protocoles de gestion

SNMP (Simple Network Managment Protocol) : UDP 161 and 162 open standard

SNMP est le protocole de gestion de réseaux complexe. Il est actuellement le plus utilisé pour la gestion des équipements de réseaux et de diagnostiquer les problèmes de réseau.

Il est aussi utilisé pour la gestion à distance des applications: les bases de données, les serveurs, les logiciels, etc.

Les protocoles d'Active Directory

TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP/IP c'est le protocole de **transport réseau**

DNS (Domain Name System)

DNS l'espace de noms Active Directory s'appuie sur ce service

DHCP (Dynamic Host Configuration Protocol)

DHCP va permettre de distribuer les adresses IP et de configurer les clients dans DNS

SNTP (Single Network Time Protocol) :

SNTP est le protocole de distribution et de synchronition de l'heure. Il est impératif que toutes les machines du domaine Windows disposent de la meme heure afin de sycnhroniser leurs actions

LDAP (Lightweight Directory Access Protocol) :

LDAP permet de gérer l'annuaire d'Active Directory et d'opérer des recherches dans sa base de données

Les types de cables

Media Type	Ethernet Standard	Bandwidth	Distance
Co-axial	10 base2 (thin)	10Mbit/s	185 m
	10 base5 (thick)	10 Mbit/s	500 m
UTP (unshielded TP)	10 base-T (cat 3)	10 Mbit/s	100 m
	100 base-TX (cat 5)	100 bit/s	100 m
	1000 base-T (cat 5e)	1G bit/s	100 m
	1000 base-T (cat 6)	1G bit/s	100 m
	10G base-T (cat 6a)	10G bit/s	100 m
Fibre Optique	MMF	100 Mbit/s	2 km