

Guide Complet de Revision

A propos de ce Guide

Ce guide couvre TOUS les modules du programme Cisco Networking Academy (NetAcad) qui apparaissent dans les examens de controle et de fin de module. Les examens Cisco sont **cumulatifs** : une seule question peut combiner des contenus de plusieurs modules. Maitriser chaque module ci-dessous vous donnera les meilleures chances de reussite.

Comment fonctionnent les examens Cisco

- Les examens NE sont PAS limites a un seul module — ils couvrent tout le contenu etudié jusqu'a la date de l'examen
- Une seule question peut combiner IPv4 + Routage + ICMP
- L'examen final melange tous les modules : ICMP, Transport, Application, Securite, etc.
- Vous devez reviser TOUS les modules presentes dans ce guide

Priorite des Modules pour l'Examen

Priorite	Module	Pourquoi c'est Important
CRITIQUE	Module 11 - Adressage IPv4	Plusieurs questions de sous-reseaux a chaque examen
CRITIQUE	Module 8 - Couche Reseau	Logique de routage dans presque chaque examen
CRITIQUE	Module 9 - ARP	Concept tres souvent evalue
CRITIQUE	Module 10 - CLI du Routeur	Questions de configuration pratique
ELEVE	Module 7 - Commutation Ethernet	Fondamentaux LAN
ELEVE	Module 14 - Couche Transport	TCP vs UDP toujours present
ELEVE	Module 3 - Modeles OSI / TCP-IP	Base de tout le reste
MOYEN	Module 12 - IPv6	Moins que IPv4 mais toujours evalue
MOYEN	Module 13 - ICMP	Ping et messages d'erreur
MOYEN	Module 15 - Couche Application	Association protocole-port
FAIBLE	Module 4 - Couche Physique	Questions simples
FAIBLE	Module 5 - Systemes Numeriques	Conversions binaires
FAIBLE	Module 6 - Couche Liaison	Bases MAC/trame
FAIBLE	Module 16 - Securite Reseau	Questions directes
FAIBLE	Module 17 - Conception Reseau	Topologies et planification

Module 3 - Modeles Reseau et Protocoles

Role et Objectif

Les modeles reseau definissent comment les donnees transitent d'un appareil a un autre a travers un reseau. Ils expliquent aussi comment les protocoles interagissent et comment la communication est structuree couche par couche.

Modele OSI - 7 Couches (Tres Important)

N°Nom de la Couche</th><th>Fonction</th><th>Protocoles / Equipements</th></tr><tr><td>7</td><td>Application</td><td>Interface utilisateur / reseau</td><td>HTTP, FTP, DNS, DHCP, SMTP</td></tr><tr><td>6</td><td>Presentation</td><td>Formatage, chiffrement</td><td>SSL/TLS, JPEG, ASCII</td></tr><tr><td>5</td><td>Session</td><td>Gestion des sessions</td><td>NetBIOS, RPC</td></tr><tr><td>4</td><td>Transport</td><td>Livraison fiable/non fiable</td><td>TCP, UDP</td></tr><tr><td>3</td><td>Reseau</td><td>Routage entre reseaux</td><td>IP, ICMP, Routeur</td></tr><tr><td>2</td><td>Liaison de donnees</td><td>Livraison de trames en LAN</td><td>Ethernet, MAC, Commutateur</td></tr><tr><td>1</td><td>Physique</td><td>Bits sur cable/sans fil</td><td>Cables, Hubs, Repeteurs</td></tr></table>
--

Modele TCP/IP - 4 Couches

Couche TCP/IP</th><th>Couches OSI Equivalentes</th><th>Protocoles</th></tr><tr><td>Application</td><td>Application + Presentation + Session (7,6,5)</td><td>HTTP, FTP, DNS, DHCP, SMTP</td></tr><tr><td>Transport</td><td>Transport (4)</td><td>TCP, UDP</td></tr><tr><td>Internet</td><td>Reseau (3)</td><td>IP, ICMP, ARP</td></tr><tr><td>Acces Reseau</td><td>Liaison + Physique (2,1)</td><td>Ethernet, Wi-Fi</td></tr></table>

Protocoles Courants a Connaitre

- HTTP (80) - Navigation web
- HTTPS (443) - Web securise
- FTP (21) - Transfert de fichiers
- DNS (53) - Resolution de noms (nom d'hote -> IP)
- DHCP (67/68) - Attribution automatique d'adresse IP
- SMTP (25) - Envoi d'e-mails
- SSH (22) - Acces distant securise
- Telnet (23) - Acces distant (non securise)

Points Essentiels a Retenir - Module 3

OK Memoriser les couches OSI dans l'ordre : Physique -> Liaison -> Reseau -> Transport -> Session -> Presentation -> Application

OK Moyen mnemotechnique (bas vers haut) : 'Pour De Nouvelles Technologies Sans Peur Avancer'

OK TCP/IP a 4 couches - OSI en a 7

OK Savoir quel protocole appartient a quelle couche

OK Unites de donnees : Bits (C1), Trames (C2), Paquets (C3), Segments (C4)

Module 4 - Couche Physique

Role et Objectif

La couche physique est responsable de la transmission des bits bruts (0 et 1) sur un support physique tel qu'un câble en cuivre, un câble à fibre optique ou des ondes radio sans fil.

Concepts Cles

- Bande passante - Quantité maximale de données transmises par seconde (bps, Kbps, Mbps, Gbps)
- Débit - Données réellement transmises (toujours inférieur ou égal à la bande passante)
- Latence - Délai dans la transmission des données
- Câbles en cuivre (UTP/STP) - Signaux électriques, sensibles aux interférences
- Câbles à fibre optique - Signaux lumineux, très rapides, immunes aux interférences, longues distances
- Sans fil - Ondes radio, 2,4 GHz / 5 GHz

Types de Câbles

Type de Câble	Support	Distance Max	Utilisation
UTP Cat5e/6	Cuivre	100 m	LAN, réseaux domestiques/bureaux
STP	Cuivre (blindé)	100 m	Environnements avec fortes interférences
Coaxial	Cuivre	Variable	Câble TV, anciens réseaux
Fibre monomode	Lumière (laser)	40-80 km	Longue distance, WAN
Fibre multimode	Lumière (LED)	~2 km	Campus, centres de données

Points Essentiels à Retenir - Module 4

- OK Couche physique = bits (0 et 1) - couche la plus basse du modèle OSI
- OK La fibre optique est plus rapide et porte plus loin que le cuivre
- OK Bande passante ≠ Débit - le débit est la vitesse réellement mesurée
- OK UTP est le câble LAN le plus courant (maximum 100 m)
- OK Le sans fil utilise des ondes radio - sensible aux interférences

Module 5 - Systemes Numeriques

Role et Objectif

Comprendre les systemes numeriques binaire, decimal et hexadecimal est essentiel pour travailler avec les adresses IP, les adresses MAC et les calculs de sous-reseaux.

Conversion Binaire <-> Decimal

- Chaque adresse IPv4 = 32 bits = 4 octets (groupes de 8 bits)
- Chaque octet va de 0 a 255 en decimal
- Valeurs de position binaire : 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1
- Exemple : 11000000 = 128+64 = 192
- Exemple : 192.168.1.1 -> 11000000.10101000.00000001.00000001

Binaire	Decimal		Binaire	Decimal
00000000	0		10000000	128
00000001	1		10101000	168
11111111	255		11000000	192
11111110	254		00000001	1

Hexadecimal (utilise dans IPv6 et adresses MAC)

- Base 16 : 0-9 puis A(10) B(11) C(12) D(13) E(14) F(15)
- Exemple d'adresse MAC : FF:AA:00:1B:2C:3D
- IPv6 utilise des groupes hex : 2001:0db8:85a3::8a2e:0370:7334
- Chaque chiffre hexadecimal = 4 bits

Points Essentiels a Retenir - Module 5

- OK IPv4 utilise le binaire (32 bits = 4 octets)
- OK Memoriser les puissances de 2 : 1, 2, 4, 8, 16, 32, 64, 128
- OK Le binaire est essentiel pour le sous-reseautage - pratiquer les conversions
- OK L'hexadecimal est utilise dans les adresses MAC et IPv6
- OK Chaque chiffre hexadecimal = 4 bits binaires

Module 6 - Couche Liaison de Donnees

Role et Objectif

La couche Liaison de donnees (Couche 2) est responsable de la communication noeud a noeud au sein du meme reseau. Elle emballe les bits dans des trames et utilise des adresses MAC pour la livraison locale.

Concepts Cles

- Trame - Unite de donnees en couche 2 (contient MAC source, MAC dest, donnees, FCS)
- Adresse MAC - Adresse physique 48 bits gravee dans la carte reseau (ex: AA:BB:CC:DD:EE:FF)
- MAC = 6 octets = 12 chiffres hex - 3 premiers octets = fabricant (OUI), 3 derniers = ID appareil
- Detection d'erreurs - FCS (Frame Check Sequence) detecte les trames corrompues
- Full-duplex - Envoi et reception simultanement; Half-duplex - une direction a la fois
- Deux sous-couches : LLC (Logical Link Control) et MAC (Media Access Control)

Points Essentiels a Retenir - Module 6

OK Couche Liaison = adresses MAC + Trames

OK L'adresse MAC fait 48 bits (6 octets), ecrite en hexadecimal

OK Les trames encapsulent les paquets de la couche 3

OK Le FCS est utilise pour la detection d'erreurs

OK LLC gere la communication avec les couches superieures; MAC gere l'accès au support

Module 7 - Commutation Ethernet

Role et Objectif

Ethernet est la technologie LAN la plus utilisée. Les commutateurs (switches) utilisent des tables d'adresses MAC pour transmettre intelligemment les trames uniquement vers le port de destination correct.

Fonctionnement d'un Commutateur

- 1. Le commutateur reçoit une trame sur un port
- 2. Il lit l'adresse MAC SOURCE et l'enregistre dans la table MAC
- 3. Il recherche la MAC DESTINATION dans la table
- 4. Si trouvée -> transmet vers ce port spécifique (unicast)
- 5. Si NON trouvée -> inonde la trame sur TOUS les ports sauf la source (flood unicast inconnu)
- 6. Les trames de diffusion (FF:FF:FF:FF:FF:FF) sont toujours inondées sur tous les ports

Types de Communication

Type	Destination	Description
Unicast	Un seul appareil	Communication directe entre deux appareils
Broadcast	Tous les appareils du LAN	Envoyé à FF:FF:FF:FF:FF:FF - chaque appareil le reçoit
Multicast	Groupe d'appareils	Envoyé à un groupe spécifique (ex: streaming)

Points Essentiels à Retenir - Module 7

- OK Le commutateur utilise les adresses MAC (couche 2) - PAS les adresses IP
- OK La table MAC associe adresse MAC <-> numéro de port
- OK Destination inconnue = inondation; Destination connue = transfert direct
- OK Adresse de diffusion = FF:FF:FF:FF:FF:FF
- OK Chaque port de commutateur = son propre domaine de collision (pas de collision)
- OK Le commutateur est meilleur que le hub car il transfère intelligemment

Module 8 - Couche Reseau (Couche 3)

Role et Objectif

La couche Reseau achemine les paquets entre differents reseaux en utilisant des adresses IP. Les routeurs operent a cette couche et prennent des decisions de transfert basees sur les tables de routage.

Concepts Cles

- Paquet IP - Unite de donnees en couche 3 (contient IP source, IP dest, TTL, donnees)
- Routage - Processus de recherche du meilleur chemin pour transmettre les paquets entre reseaux
- Routeur - Appareil qui connecte plusieurs reseaux et achemine les paquets entre eux
- Table de routage - Base de donnees dans le routeur listant les destinations reseau connues
- Passerelle par default - L'adresse IP du routeur utilisee par les appareils pour atteindre d'autres reseaux
- TTL (Temps de Vie) - Decremente de 1 a chaque routeur; paquet abandonne quand TTL = 0
- Encapsulation - A chaque saut, la trame couche 2 est reconstruite mais le paquet couche 3 reste identique

Types de Routage

Type	Description	Exemple
Routage Statique	Configure manuellement par l'admin - ne change pas automatiquement	ip route 10.0.0.0 255.255.255.0 255.255.255.0 10.0.0.1
Routage Dynamique	Les routeurs partagent l'info automatiquement via des protocoles	RIP, OSPF, EIGRP
Route par Default	Utilisee quand aucune route specifique n'est trouvee - permet de courir	ip route 0.0.0.0 0.0.0.0 10.0.0.1

Points Essentiels a Retenir - Module 8

- OK Couche reseau = adresses IP + Paquets + Routage
- OK Le routeur utilise la table de routage pour decider ou transmettre les paquets
- OK Passerelle par default = l'IP du routeur utilisee pour quitter un reseau local
- OK Le TTL empeche les paquets de boucler indefiniment
- OK Routage statique : manuel - Routage dynamique : automatique (RIP, OSPF)
- OK L'encapsulation en couche 3 cree des paquets; la couche 2 les enveloppe dans des trames

Module 9 - Resolution d'Adresse (ARP)

Role et Objectif

ARP (Address Resolution Protocol) resout une adresse IP en adresse MAC au sein d'un reseau local. Un appareil connait l'IP de la destination mais a besoin de l'adresse MAC pour construire une trame de couche 2 correcte.

Fonctionnement d'ARP - Etape par Etape

- Etape 1 : L'appareil A veut envoyer des donnees a 192.168.1.5 mais ne connait pas sa MAC
- Etape 2 : L'appareil A envoie une Requete ARP (diffusion) - 'Qui a 192.168.1.5 ? Dites a 192.168.1.1'
- Etape 3 : La diffusion va a TOUS les appareils du LAN (MAC dest = FF:FF:FF:FF:FF:FF)
- Etape 4 : Seul l'appareil avec l'IP 192.168.1.5 repond avec sa MAC (Reponse ARP = unicast)
- Etape 5 : L'appareil A stocke le resultat dans sa Table ARP (cache)
- Etape 6 : Les futurs paquets utilisent la MAC en cache - plus besoin de diffusion

Table ARP

- Stocke temporairement les associations IP <-> MAC
- Les entrees expirent apres un delai (pour gerer les changements d'appareils)
- Afficher la table ARP : arp -a (Windows) ou arp -n (Linux)
- ARP Gratuit - Un appareil annonce sa propre MAC (mise a jour des tables ARP des autres)
- Usurpation ARP - Attaque de securite : fausses reponses ARP pour intercepter le trafic

Points Essentiels a Retenir - Module 9

OK ARP resout adresse IP -> adresse MAC

OK Requete ARP = diffusion (FF:FF:FF:FF:FF:FF)

OK Reponse ARP = unicast (directement vers le demandeur)

OK ARP fonctionne uniquement dans le meme LAN (reseau local)

OK Les resultats sont mis en cache dans la table ARP pour reduire les diffusions

OK Pour les reseaux distants : ARP est fait pour l'IP de la passerelle par default, pas l'hote distant

Module 10 - Configuration de Base du Routeur

Role et Objectif

Les routeurs Cisco sont configurés via une interface en ligne de commande (CLI). Ce module couvre les commandes essentielles pour configurer les interfaces, les mots de passe et le routage de base.

Modes du Routeur

Mode	Invite	Commande d'Acces	But
Utilisateur EXEC	Router>	(par défaut à la connexion)	Surveillance de base uniquement
Privilege EXEC	Router#	enable	Surveillance et gestion complètes
Config Globale	Router(config)#	configure terminal	Modifications globales
Config Interface	Router(config-if)#	interface g0/0	Configurer une interface spécifique
Config Ligne	Router(config-line)#	line console 0	Configurer console/VTY

Commandes Essentielles

```
Router> enable ! Entrer en mode privilege
Router# configure terminal ! Entrer en config globale
Router(config)# hostname R1 ! Définir le nom du routeur

! Configurer une interface :
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown ! Activer l'interface
Router(config-if)# description Lien LAN ! Description optionnelle

! Securite - Définir les mots de passe :
Router(config)# enable secret cisco123 ! Mot de passe privilege chiffré
Router(config)# line console 0
Router(config-line)# password cisco ! Mot de passe console
Router(config-line)# login ! Exiger mot de passe sur console

! Ajouter une route statique :
Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

! Sauvegarder la configuration :
Router# copy running-config startup-config

! Commandes de verification :
Router# show ip interface brief ! Voir toutes les interfaces et leur état
Router# show running-config ! Voir la configuration actuelle
Router# show ip route ! Voir la table de routage
```

Points Essentiels à Retenir - Module 10

OK Toujours utiliser 'enable' d'abord pour entrer en mode EXEC privilege

OK Utiliser 'configure terminal' pour entrer en mode config globale

OK TOUJOURS taper 'no shutdown' lors de la configuration d'une interface (elle est desactivee par default)

OK 'show ip interface brief' = moyen le plus rapide de verifier l'etat des interfaces

OK 'copy running-config startup-config' sauvegarde la config de facon permanente

OK 'enable secret' est plus securise que 'enable password' (il chiffre le mot de passe)

OK Syntaxe route statique : ip route [reseau] [masque] [IP prochain saut]

Module 11 - Adressage IPv4 (CRITIQUE !)

Role et Objectif

L'adressage IPv4 est le sujet LE PLUS evalue dans les examens Cisco NetAcad. Vous devez etre capable de calculer des sous-reseaux, identifier les adresses reseau/diffusion et determiner les plages d'hotes.

Structure d'une Adresse IPv4

- 32 bits de long, ecrite sous forme de 4 octets decimaux : 192.168.1.100
- Chaque octet = 8 bits, plage de 0 a 255
- Le masque de sous-reseau separe la partie RESEAU de la partie HOTE
- Notation CIDR : /24 = 255.255.255.0 (24 bits pour le reseau)
- Adresse reseau - Premiere IP dans un sous-reseau (tous les bits hote = 0) - NON assignable
- Adresse de diffusion - Derniere IP dans un sous-reseau (tous les bits hote = 1) - NON assignable
- Hotes utilisables = $2^{(\text{bits hote})} - 2$

Reference des Masques de Sous-Reseaux Courants

CIDRMasque	Nb HotesBloc	Exemple de Plage		
/24	255.255.255.0	254	256	192.168.1.0 - 192.168.1.255
/25	255.255.255.128	126	128	192.168.1.0 - 192.168.1.127
/26	255.255.255.192	62	64	192.168.1.0 - 192.168.1.63
/27	255.255.255.224	30	32	192.168.1.0 - 192.168.1.31
/28	255.255.255.240	14	16	192.168.1.0 - 192.168.1.15
/29	255.255.255.248	6	8	192.168.1.0 - 192.168.1.7
/30	255.255.255.252	2	4	192.168.1.0 - 192.168.1.3
/16	255.255.0.0	65534	65536	172.16.0.0 - 172.16.255.255
/8	255.0.0.0	16777214	16777216	10.0.0.0 - 10.255.255.255

Exemple de Calcul de Sous-Reseau Etape par Etape

Exemple : Trouver le reseau, la diffusion et la plage d'hotes

- Donne : IP = 192.168.1.100 / 26
- Etape 1 : /26 -> masque = 255.255.255.192, taille de bloc = 64
- Etape 2 : Trouver le bon bloc : 0-63 / 64-127 / 128-191 / 192-255
- Etape 3 : 100 est dans la plage 64-127
- Etape 4 : Adresse reseau = 192.168.1.64
- Etape 5 : Adresse de diffusion = 192.168.1.127
- Etape 6 : Hotes utilisables = 192.168.1.65 a 192.168.1.126 (62 hotes)

Adresses Speciales

- Plages IP privées (non routables sur Internet) :
- Classe A : 10.0.0.0 - 10.255.255.255
- Classe B : 172.16.0.0 - 172.31.255.255
- Classe C : 192.168.0.0 - 192.168.255.255
- Adresse de bouclage : 127.0.0.1 (utilisée pour tester TCP/IP sur l'appareil local)

Points Essentiels à Retenir - Module 11

OK IPv4 = 32 bits / 4 octets - plage de 0.0.0.0 à 255.255.255.255

OK Le masque de sous-réseau sépare les bits réseau des bits hôte

OK Hôtes utilisables = $2^{\text{(bits hôte)}} - 2$ (soustraire réseau + diffusion)

OK Adresse réseau = première IP (bits hôte tous à 0)

OK Adresse de diffusion = dernière IP (bits hôte tous à 1)

OK Memoriser CIDR /24=254 hôtes, /25=126, /26=62, /27=30, /28=14, /29=6, /30=2

OK Plages privées : 10.x.x.x, 172.16-31.x.x, 192.168.x.x

Module 12 - Adressage IPv6

Role et Objectif

IPv6 a été créé pour résoudre le problème d'épuisement des adresses IPv4. Il utilise des adresses de 128 bits, offrant un espace d'adressage quasi illimité.

Différences Principales avec IPv4

Caractéristique	IPv4	IPv6
Taille adresse	32 bits	128 bits
Format	Décimal pointé (192.168.1.1)	Groupes hexadécimaux (2001:db8::1)
Diffusion	Oui (FF:FF:FF:FF:FF:FF)	Non - utilise le multicast
Espace adresses	~4,3 milliards	340 undécillions
Config	Statique / DHCP	Statique / DHCPv6 / SLAAC
Bouclage	127.0.0.1	::1

Types d'Adresses IPv6

- Unicast - Communication un-a-un (comme l'unicast IPv4)
- Unicast global - Routable sur Internet, commence par 2000::/3
- Lien local - Utilisée uniquement dans le lien local, commence par FE80::/10 (auto-configurée)
- Bouclage - ::1 (équivalent à 127.0.0.1 en IPv4)
- Multicast - Un-a-plusieurs, commence par FF00::/8
- Anycast - Envoyé au plus proche d'un groupe (pas de diffusion en IPv6 !)

Règles d'Abréviation IPv6

- Règle 1 : Les zéros de tête dans un groupe peuvent être omis -> 0db8 = db8
- Règle 2 : Un groupe de groupes consécutifs tous à zéro peut être remplacé par :: (double deux-points)
- Exemple : 2001:0db8:0000:0000:0000:0000:0001 -> 2001:db8::1
- IMPORTANT : :: ne peut apparaître qu'UNE SEULE FOIS dans une adresse

Points Essentiels à Retenir - Module 12

- OK IPv6 = 128 bits (beaucoup plus long que les 32 bits d'IPv4)
- OK Écrit en hexadécimal, 8 groupes de 4 chiffres hex, séparés par des deux-points
- OK Pas de diffusion en IPv6 - utilise le multicast à la place
- OK Les adresses lien-local (FE80::) sont auto-configurées sur chaque interface
- OK :: signifie un ou plusieurs groupes de zéros (utilise une seule fois par adresse)
- OK SLAAC permet aux appareils de s'auto-configurer leur propre adresse IPv6

Module 13 - ICMP

Role et Objectif

ICMP (Internet Control Message Protocol) est utilise pour le diagnostic reseau et le signalement d'erreurs. Il fonctionne en couche 3 aux cotes d'IP et est utilise par des outils comme ping et traceroute.

Types de Messages ICMP Courants

Type de Message	Code	Signification
Echo Request	Type 8	Envoye par ping pour tester la connectivite
Echo Reply	Type 0	Reponse a Echo Request (destination joignable)
Destination Inaccessible	Type 3	Le paquet n'a pu atteindre la destination
Temps Depasse	Type 11	TTL a atteint 0 (utilise par traceroute)
Redirect	Type 5	Meilleure route disponible - mettre a jour le routage
Reseau Inaccessible	Type 3, Code 0	Pas de route vers le reseau de destination
Port Inaccessible	Type 3, Code 3	Port de destination non ouvert

Ping vs Traceroute

- ping - Teste si une destination est joignable. Envoie des Echo Requests ICMP et attend des Echo Replies
- ping 8.8.8.8 - teste la connectivite au serveur DNS de Google
- traceroute (tracert sous Windows) - Montre le chemin emprunte par les paquets vers la destination
- traceroute utilise la manipulation du TTL - chaque routeur qui abandonne (TTL=0) renvoie Type 11
- Ping reussi = ICMP Type 8 envoye + ICMP Type 0 reçu
- Ping echoue = ICMP Type 3 (Destination Inaccessible) ou Requete expiree

Points Essentiels a Retenir - Module 13

- OK ICMP = protocole de diagnostic, fonctionne en couche 3**
- OK Ping utilise Echo Request ICMP (Type 8) et Echo Reply (Type 0)**
- OK Destination Inaccessible (Type 3) = le paquet ne peut pas etre livre**
- OK Temps Depasse (Type 11) = TTL a atteint 0, utilise par traceroute**
- OK ICMP ne transporte pas de donnees utilisateur - il transporte des messages de controle/erreur**
- OK ICMPv6 gere aussi la Decouverte de Voisins (remplace ARP en IPv6)**

Module 14 - Couche Transport

Role et Objectif

La couche Transport (Couche 4) est responsable de la communication de bout en bout entre les applications. Elle utilise des numeros de port pour identifier quelle application doit recevoir les donnees.

Comparaison TCP vs UDP

Caracteristique	TCP	UDP
Connexion	Orienté connexion (poignée de main à 3 voies)	Sans connexion (pas de poignée de main)
Fiabilité	Fiable - garantit la livraison	Non fiable - pas de garantie de livraison
Vérification erreurs	Oui - retransmet les segments perdus	Somme de contrôle basique
Vitesse	Plus lent (plus de surcharge)	Plus rapide (moins de surcharge)
Ordre	Oui - les données arrivent dans l'ordre	Aucun ordre garanti
Contrôle de flux	Oui (fenêtrage)	Non
Cas d'usage	HTTP, FTP, SSH, Email	DNS, DHCP, VoIP, Video, Jeux en ligne
Taille en-tête	Minimum 20 octets	8 octets

Poignée de Main TCP à 3 Voies

- Etape 1 : Client -> Serveur : SYN (Je veux me connecter)
- Etape 2 : Serveur -> Client : SYN-ACK (OK, je suis prêt)
- Etape 3 : Client -> Serveur : ACK (Super, c'est parti !)
- Après la poignée de main : la connexion est établie, les données peuvent circuler
- Fin de connexion : FIN -> ACK -> FIN -> ACK (4 étapes)

Ports Bien Connus (à Memoriser)

Port	Protocole	Service
20/21	TCP	FTP (Protocole de Transfert de Fichiers)
22	TCP	SSH (Shell Sécurisé)
23	TCP	Telnet (accès distant non sécurisé)
25	TCP	SMTP (Envoi d'e-mails)
53	TCP/UDP	DNS (Système de Noms de Domaine)
67/68	UDP	DHCP (Attribution d'adresse IP)
80	TCP	HTTP (Navigation web)
110	TCP	POP3 (Reception d'e-mails)
143	TCP	IMAP (Reception d'e-mails)
443	TCP	HTTPS (Web sécurisé)
3389	TCP	RDP (Protocole Bureau à Distance)

Points Essentiels à Retenir - Module 14

OK TCP = fiable, ordonne, oriente connexion (utilise une poignée de main)

OK UDP = rapide, non fiable, sans connexion (pas de poignée de main)

OK Les numeros de port identifient l'application/service (0-65535)

OK Ports bien connus : 0-1023 | Enregistres : 1024-49151 | Dynamiques : 49152-65535

OK Poignée de main TCP a 3 voies : SYN -> SYN-ACK -> ACK

OK Memoriser les ports : HTTP=80, HTTPS=443, DNS=53, FTP=21, SSH=22, DHCP=67/68

Module 15 - Couche Application

Role et Objectif

La couche Application (Couche 7) est la où les services reseau interagissent directement avec les utilisateurs finaux et les applications. Elle fournit l'interface entre le logiciel de l'utilisateur et le reseau.

Protocoles Cles de la Couche Application

Protocole	Port	Fonction
HTTP	80	HyperText Transfer Protocol - navigation web non chiffrée
HTTPS	443	HTTP Sécurisé - navigation web chiffrée (utilise SSL/TLS)
DNS	53	Resout les noms de domaine en adresses IP (google.com -> 8.8.8.8)
DHCP	67/68	Attribue automatiquement IP, masque, passerelle, DNS aux appareils
FTP	20/21	File Transfer Protocol - téléchargements/envois de fichiers
SMTP	25	Envoie les e-mails du client vers le serveur
POP3	110	Télécharge les e-mails du serveur (les supprime du serveur)
IMAP	143	Lit les e-mails du serveur (les conserve, synchronise sur tous appareils)
SSH	22	Accès distant en ligne de commande chiffré
Telnet	23	Accès distant non chiffré (non sécurisé - à éviter)
SNMP	161	Surveillance et gestion réseau
TFTP	69	FTP simplifié - transfert de fichiers léger, utilise UDP

Fonctionnement du DNS

- Etape 1 : Vous tapez 'www.google.com' dans le navigateur
- Etape 2 : Votre appareil vérifie d'abord son cache DNS local
- Etape 3 : Si non trouvé, interroge le serveur DNS (configure par DHCP ou manuellement)
- Etape 4 : Le serveur DNS retourne l'adresse IP : 142.250.185.78
- Etape 5 : Le navigateur se connecte à cette adresse IP

Fonctionnement du DHCP (processus DORA)

- D - Discover : Le client diffuse 'Y a-t-il un serveur DHCP ?' (port UDP 67)
- O - Offer : Le serveur répond avec une adresse IP disponible
- R - Request : Le client diffuse 'J'accepte cette IP'
- A - Acknowledge : Le serveur confirme l'attribution de l'IP

Points Essentiels à Retenir - Module 15

- OK DNS traduit les noms de domaine -> adresses IP (port 53)
- OK DHCP configure automatiquement : adresse IP, masque, passerelle par défaut, serveur DNS
- OK HTTP (80) = non chiffré / HTTPS (443) = chiffré
- OK SMTP envoie les e-mails; POP3/IMAP reçoivent les e-mails

OK SSH (22) = securise; Telnet (23) = non securise - toujours preferer SSH

OK DHCP utilise DORA : Discover -> Offer -> Request -> Acknowledge

Module 16 - Securite Reseau

Role et Objectif

La securite reseau implique de proteger les reseaux, appareils et donnees contre les acces non autorises, les attaques et les dommages. Ce module couvre les menaces courantes et les mecanismes de defense.

Menaces Reseau Courantes

Menace	Description
Malware	Logiciel malveillant (virus, ver, cheval de Troie, ransomware, spyware)
Hameconnage	Faux e-mails/sites web pour voler des identifiants ou infos personnelles
Attaque DoS	Deni de Service - inonde une cible pour la rendre indisponible
Attaque DDoS	DoS distribue - utilise de nombreux ordinateurs compromis (botnet)
Homme du Milieu	L'attaquant intercepte la communication entre deux parties
Usurpation ARP	Faussees reponses ARP pour rediriger le trafic via l'attaquant
Empoisonnement DNS	Corrompt le cache DNS pour rediriger les utilisateurs vers des sites malveillants
Force Brute	Essaie tous les mots de passe possibles jusqu'a en trouver un qui fonctionne
Ingenierie Sociale	Manipule les gens pour qu'ils revelent des infos sensibles
Ecoute Clandestine	Interception du trafic reseau non chiffre (sniffing)

Mecanismes de Defense

- Pare-feu - Filtre le trafic selon des regles (bloque les acces non autorises)
- IDS (Systeme de Detection d'Intrusion) - Surveille et alerte sur les activites suspectes
- IPS (Systeme de Prevention d'Intrusion) - Surveille ET bloque les activites suspectes
- VPN (Reseau Prive Virtuel) - Chiffre le trafic sur les reseaux publics
- Antivirus/Anti-malware - Detecte et supprime les logiciels malveillants
- AAA (Authentification, Autorisation, Comptabilite) - Controle qui peut acceder a quoi
- Chiffrement - Rend les donnees illisibles sans la cle correcte (SSL/TLS, AES)
- Mots de passe forts + MFA - Reduit les risques de force brute et d'accès non autorise
- Mises a jour/correctifs logiciels - Corrige les vulnerabilites de securite connues

Points Essentiels a Retenir - Module 16

OK Types de malware : virus (auto-replique), ver (se propage seul), cheval de Troie (deguise), ransomware (chiffre fichiers)

OK DoS = un attaquant / DDoS = plusieurs attaquants (botnet)

OK Pare-feu = premiere ligne de defense - filtre les paquets selon des regles

OK VPN chiffre la communication sur des reseaux publics/non fiables

OK AAA : Authentification (qui etes-vous?) -> Autorisation (que pouvez-vous faire?) -> Comptabilite (qu'avez-vous fait?)

OK La securite physique fait aussi partie de la securite reseau (salles serveurs verrouillee, etc.)

Module 17 - Conception de Reseau

Role et Objectif

La conception reseau implique de planifier et construire des reseaux qui repondent a des exigences specifiques. Cela comprend le choix des topologies, la selection des equipements et la planification de l'adressage IP.

Topologies Reseau

Topologie	Description	Avantages	Inconvenients
Etoile	Tous les appareils se connectent a un commutateur central	Facile a gerer, cables isolees	Panne du commutateur = reseau en panne
Bus	Tous les appareils partagent un cable	Simple, economique	Collisions, point de defaillance unique
Anneau	Appareils en boucle	Acces equitable	Une rupture = tout le reseau tombe
Maillage	Chaque appareil connecte a tous les autres	Redondant, tolerant aux pannes	Couteux, complexe
Hybride	Combinaison de topologies	Flexible, evolutif	Conception complexe
Etoile etendue	Etoile d'etoiles (hierarchique)	Evolutif pour grands reseaux	Plus complexe que l'etoile simple

Types de Reseaux

- LAN (Reseau Local) - Petite zone geographique (maison, bureau, campus scolaire)
- WAN (Reseau Longue Distance) - Grande zone geographique (connecte villes/pays) - Internet est un WAN
- MAN (Reseau Metropolitain) - Reseau a l'echelle d'une ville
- WLAN (LAN Sans Fil) - Reseau Wi-Fi
- PAN (Reseau Personnel) - Tres petite zone (appareils Bluetooth autour d'une personne)
- VPN (Reseau Prive Virtuel) - Etend un reseau prive sur Internet public

Points Essentiels a Retenir - Module 17

- OK La topologie en etoile est la plus courante dans les reseaux modernes (utilise des commutateurs)
- OK La topologie maillage offre la plus haute redondance
- OK LAN = local / WAN = longue distance / WLAN = sans fil
- OK Toujours planifier l'adressage IP avant le deploiement
- OK Considerer l'evolutivite - concevoir pour la croissance future
- OK Conception hierarchique : Coeur -> Distribution -> Acces

Resume Final - Reference Rapide pour l'Examen

Top 10 Choses a Memoriser pour le Jour de l'Examen

N°	Sujet	Ce qu'il Faut Savoir
1	Couches OSI	Physique, Liaison, Reseau, Transport, Session, Presentation, Application
2	Calcul Sous-Reseau	Hotes utiles = $2^{(\text{bits hote}) - 2}$; /24=254, /25=126, /26=62, /27=30
3	Processus ARP	IP->MAC; Requete=diffusion; Reponse=unicast; LAN uniquement
4	TCP vs UDP	TCP=fiable+lent; UDP=rapide+non fiable; TCP utilise poignee de main
5	CLI Routeur	enable -> conf t -> interface -> ip address -> no shutdown -> show ip int brief
6	Ports Cles	80=HTTP, 443=HTTPS, 53=DNS, 22=SSH, 21=FTP, 67/68=DHCP, 25=SMTP
7	IPv6	128 bits, hex, pas de diffusion, lien-local=FE80::, bouclage=::1
8	ICMP	ping=Type8+Type0; inaccessible=Type3; TTL depasse=Type11
9	DHCP DORA	Discover -> Offer -> Request -> Acknowledge
10	IPs Privees	10.x.x.x / 172.16-31.x.x / 192.168.x.x - non routables sur Internet

• Pour les questions CLI : se souvenir du mode (config)# vs # vs >

• Questi