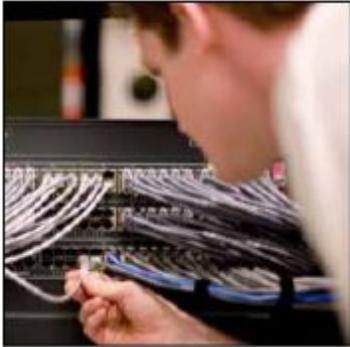


Microtel Training Institute



Catalogue des Formations Cisco 2011



Présentation de Microtel Training Institute

Microtel Training Institute, Etablissement agréé par l'Etat, est le premier institut Cisco Learning Partner Associate (CLPA) en Algérie à dispenser les formations officielles Cisco depuis 2004, en partenariat avec Fast Lane CLSP (Cisco Learning Solutions Partner).

En 2010 *Microtel Training Institute* a obtenu son statut de CLP (Cisco Learning Partner) qui est d'un niveau plus élevé que le CLPA et plus exigeant en terme de ressources humaines certifiées dans différentes technologies (Routing & Switching ; Sécurité ; Voix sur IP ; Wireless ; Data Center etc..)

Microtel Training Institute n'a cessé d'évoluer en termes de chiffre d'affaire, et de monter en compétence. Voici quelques chiffres illustrant cette évolution :

- Chiffre d'affaire 2009 par rapport à 2008 : 62%
- Nombres de stagiaires formés sur les différents Cours Cisco en 2009: Prés de 600
- Plus d'une quarantaine de cours dispensés dans différentes technologies

L'offre Microtel Training Institute :

L'offre *Microtel Training Institute* s'articule principalement autour de trois axes :

- I – Engineering de la formation
- II – Types de formations : Inter-Entreprise, Intra-entreprise et E-Learning
- III – Services Post-formation : Certification et Consulting

I – Engineering de la formation:

Ce service permet d'accompagner le client et d'être en amont des projets de formations pour mettre en place un plan d'action et passer ensuite à la phase concrétisation et évaluations :

- Identification des besoins clients
- Valider les pré-requis des stagiaires ;
- Proposer la formation la plus adaptée aux objectifs et aux participants ;
- Possibilité de valider les acquis à chaud (à la demande du client)
- Réaliser un bilan pédagogique à l'issue d'un stage ou d'un projet de formation

II – Le type de formations :

Formation Inter-Entreprises : Cours dispensés dans les salles du centre de formation équipés de toutes les commodités nécessaires et dans un environnement agréable.

Formation Intra-Entreprise : *Microtel Training Institute* est en mesure de dispenser des cours sur le site client afin de répondre à un besoin spécifique et minimiser les coûts de déplacement des stagiaires.

Formation E-Learning (Classe virtuelle): De nombreux cours du catalogue *Microtel training Institute* peuvent être dispensés en E-Learning en utilisant des outils pédagogiques performants et adaptés. La formation se déroule sur Internet en Live avec le formateur.

Les formations sont assurées par des Instructeurs hautement qualifiés avec des compétences dans le consulting, design et le déploiement des solutions.

Les instructeurs suivent régulièrement des updates technologiques pour être toujours à la page des dernières innovations et maîtriser de nouveaux outils pédagogiques dans le souci d'améliorer la qualité de la formation.

Aucune formation ne peut être complète sans la pratique. Pour cela, tous les cours dispensés par *Microtel Training Institute* comprennent des travaux pratiques (Labs) accessibles sur nos équipements de technologie de dernière génération.

A noter que pour les cours en Intra-Entreprise et E-Learning, les Labs sont accessibles à distance via internet

III - Services Post formation :

Pour être plus complet dans notre offre formation *Microtel Training Institute* propose deux services supplémentaires :

Préparation à la certification : *Microtel Training Institute* propose des sessions spécifiques pour préparer les stagiaires à passer leurs certifications en faisant des synthèses globales sur les modules abordés lors de leur formation et en proposant des examens blancs

Consulting : Les instructeurs conseillent et orientent les stagiaires pour utiliser les bonnes pratiques afin de réussir leurs projets que se soit dans la phase Design, implémentation ou exploitation des solutions réseaux

***Microtel Training Institute*, Centre de Certification Pearson Vue :**

Les formations Cisco entrent également dans un cursus de Certifications. L'obtention d'une certification technique sur les solutions réseaux d'un leader mondial tel que Cisco, a deux avantages:

- Une valeur ajoutée pour l'organisme employeur : Avoir une équipe hautement qualifiée pour prendre en charge d'une manière efficace les solutions du réseau de l'Entreprise.
- Une professionnalisation des compétences et de carrière pour le personnel.

Table des matières

Cursus Routing & Switching	6
ICND PART 1: Interconnecting Cisco Networks Devices Part 1V1.1	6
ICND PART 2: Interconnecting Cisco Networks Devices Part 2 V1.1	7
ROUTE: Implementing Cisco IP Routing V1.0.....	8
SWITCH: Implementing Cisco IP Switched Networks V1.0	10
TSHOOT: Troubleshooting and Maintaining Cisco IP Networks V1.0.....	12
Cursus Sécurité.....	14
IINS: Cisco Implementing IOS Unified Network Security V 1.0	14
SECURE: Securing Networks with Cisco Routers & Switches V1.0	16
FIREWALL: Deploying Cisco ASA Firewall Solutions V1.0.....	18
VPN: Deploying Cisco ASA VPN Solutions V1.0	20
IPS: Implementing Cisco Intrusion Prevention System V 7.0.....	22
Cursus Architecture Réseaux	25
ARCH: Designing Cisco Network Service ArchitecturesV2.1	25
DESIGN: Cisco Designing for Cisco Internetworks Solution V2.1	27
Cursus Management de Réseaux.....	29
CWLMS: Implementing CiscoWorks LMS V 3.1	29
Cursus Téléphonie IP & Communication Unifiée	31
ICOMM: Introducing Cisco Voice and Unified Communications Administration V1.0.....	31
CVOICE: Cisco Voice Over IP V8.0.....	34
CIPT 1: Implementing Cisco Unified Communication Manager PART 1 V 8.0	36
CIPT 2: Implementing Cisco Unified Communication Manager PART 2 V 8.0	38
TVOICE: Troubleshooting Cisco Unified Communications Systems V8.0	40
CAPPS: Integartion Cisco Unified Communications Applications V8.0.....	42
Cursus Réseaux Sans Fil	44
IUWNE: Implementing Unified Wireless Networking Essentials V1.0.....	44
CUWSS: Conducting Cisco Unified Wireless Site Survery V1.0	46
IUWVN: Implementing Cisco Unified Wireless Voice Networks V1.0	48
IUWMS: Implementing Cisco Unified Mobility Service V1.0	50



IAUWS: Implementing Advance Cisco Unified Wireless Security V1.0.....	52
Cursus Data Center.....	54
DCNI-1: Data Center Network Infrastructure -1	54
DCNI-2: Data Center Network Infrastructure -2	56
DCNID: Designing Cisco Data Center Network Infrastructures	58

Cursus Routing & Switching



ICND PART 1: Interconnecting Cisco Networks Devices Part 1V1.1

Ce cours a pour objectif de fournir au stagiaire les compétences et les connaissances nécessaires de nature à installer, maintenir et dépanner un réseau de petite capacité, y compris configurer un routeur, un commutateur, mettre en place une interconnexion de réseaux distants et mettre en œuvre une sécurité.

Durée: 5 jours

Pré-requis: Aucun

Objectifs : A l'issue de ce cours le stagiaire sera en mesure d'accomplir les tâches suivantes:

- Décrire les fonctions d'un réseau, identifier les différents composants, et comprendre les principes de la communication réseau et du modèle OSI.
- Utiliser le processus de délivrance de paquets et décrire les problèmes relatifs au trafic sur Ethernet LAN et en identifier les solutions.
- Décrire les méthodes pouvant être utilisées pour étendre le réseau LAN avec une attention particulière à l'utilisation du réseau sans fil RF.
- Décrire la façon de connecter les réseaux avec les routeurs et comment les réseaux routés transmettent les données à travers TCP/IP.
- Décrire le fonctionnement et les différents composants d'un réseau d'accès distants et configurer l'encapsulation PPP, le routage statique et dynamique avec RIP ainsi que la translation d'adresses PAT.
- Utiliser l'interface de commande en ligne pour découvrir le voisinage réseau et gérer le démarrage du routeur et sa configuration

Contenu :

1. Mettre en place un réseau simple
2. Les réseaux locaux Ethernet
3. Les réseaux LAN sans fil
4. Explorer les fonctions du routage
5. Les réseaux d'accès distants (réseauxWAN)
6. Gestion de l'environnement réseau

Cursus Routing & Switching



ICND PART 2: Interconnecting Cisco Networks Devices Part 2 V1.1

Ce cours a pour objectif de fournir aux stagiaires les compétences et les connaissances nécessaires de nature à installer, maintenir et dépanner un réseau de petite capacité, y compris configurer un routeur, un commutateur, mettre en place une interconnexion de réseaux distants et mettre en œuvre une sécurité

Durée: 5 jours

Pré-requis: Avoir suivi le cours ICND1 ou avoir des connaissances équivalentes.

Objectifs : A l'issue de ce cours les stagiaires seront en mesure d'accomplir les tâches suivantes :

- Rappel sur la configuration et le dépannage d'un réseau simple
- Étendre un réseau avec de multiples commutateurs, supporter les VLANs, le trunking et le spanning-tree
- Décrire les concepts du routage Appliqués à un réseau de moyenne capacité, et les éléments à prendre en compte lors de la mise en œuvre du routage sur le réseau.
- Configurer, vérifier et dépanner OSPF
- Configurer, vérifier et dépanner EIGRP
- Déterminer comment appliquer les Les listes de contrôle d'accès (ACLs) et configurer, vérifier et dépanner les ACLs.
- Décrire quand utiliser NAT et PAT et comment les configurer sur les routeurs.
- Identifier et mettre en œuvre la technologie WAN appropriée

Contenu :

1. Mise en œuvre d'un réseau de petite capacité (rappel ICND1).
2. Mise en place d'un réseau commuté de moyenne capacité.
3. Mise en place d'un réseau routé de moyenne capacité
4. Mise en œuvre du protocole OSPF pour une zone unique
5. Mise en œuvre du protocole EIGRP. Les listes de contrôle d'accès (ACLs).
6. Gestion de l'espace d'adressage.
7. Extension du réseau LAN vers le WAN

Cursus Routing & Switching



ROUTE: Implementing Cisco IP Routing V1.0

Ce cours apportera aux participants les connaissances et compétences nécessaires pour appréhender les concepts avancés de routage lors de la mise en œuvre de routeurs Cisco connectés à un environnement LAN et WAN de petite et grande taille.

Durée: 5 jours

Pré-requis: Avoir suivi les cours ICND1 et ICND2 ou posséder les connaissances équivalentes.

Objectifs :

- Planifier et documenter la configuration, la vérification des protocoles de routage et leur optimisation
- Identifier les technologies, composants et métriques de EIGRP pour mettre en œuvre et vérifier le routage EIGRP
- Identifier et analyser les fonctions de routage multiaires OSPF et les avantages d'un routage efficace dans un réseau d'entreprise complexe.
- Mettre en œuvre et vérifier une solution de redistribution dans un réseau multi-protocoles utilisant les fonctionnalités de l'IOS pour contrôler la sélection de chemins et conserver une topologie «loop free»
- Evaluer les problèmes de performance réseau et identifier les outils nécessaires pour fournir un contrôle de chemin au niveau 3
- Mettre en œuvre le paramétrage de BGP pour connecter un réseau d'entreprise à un fournisseur d'accès à internet

Contenu :

1. Planification des services de routage

- Evaluer les besoins de réseau d'entreprise complexes
- Processus et procédures de maintenance

2. Mettre en œuvre une solution basée sur EIGRP

- Planifier la mise œuvre du routage avec EIGRP
- Mettre en œuvre une configuration basique de EIGRP pour les architectures LAN et WAN
- Mettre en œuvre et vérifier l'authentification EIGRP
- Fonctionnalités avancées de EIGRP

3. Mettre en œuvre un réseau multiaire basé sur une solution OSPF

- Planifier la mise en œuvre d'un protocole de routage extensible avec OSPF
- Traitement des paquets OSPF
- Améliorer la performance du routage dans un réseau d'entreprise complexe
- Configurer et vérifier le routage OSPF
- Configurer l'agrégation de routes en OSPF
- Configurer les différents types d'aires OSPF
- Configurer et vérifier l'authentification OSPF

4. Mise en œuvre de la redistribution en IPv4

- Evaluer les problèmes de performance et de sécurité du routage
- Fonctionnement d'un réseau utilisant de multiples protocoles de routage
- Configurer et vérifier la redistribution de routes

5. Mettre en œuvre le contrôle de chemin

- Evaluer les problèmes de contrôle du chemin réseau

6. Connexion d'un réseau d'entreprise vers un réseau ISP

- Planifier la connexion de l'entreprise vers un ISP
- Considérer les avantages de l'utilisation de BGP
- Comparer les fonctions et l'utilisation de EBGP et IBGP
- Configurer et vérifier les fonctionnalités de base de BGP
- Utiliser les attributs BGP et le processus de sélection des chemins

Cursus Routing & Switching



SWITCH: Implementing Cisco IP Switched Networks V1.0

Ce cours apportera aux participants les connaissances nécessaires pour planifier, configurer et vérifier la mise en œuvre d'infrastructures complexes de réseaux commutés utilisant l'architecture Cisco Enterprise Campus.

Le cours s'appuiera sur de nombreuses mises en pratiques afin de permettre aux participants de les adapter en fonction de leurs expériences professionnelles et de leurs organisations.

Durée: 5 jours

Pré-requis: Avoir suivi les cours ICND1 et ICND2 ou posséder les connaissances équivalentes.

Objectifs :

- Analyser la conception des Réseaux de type Campus
- Mettre en œuvre les VLANs dans des Réseaux de type Campus
- Mettre en œuvre le protocole Spanning-Tree
- Mettre en œuvre le routage inter-vlan dans un réseau de type Campus
- Mettre en œuvre la haute disponibilité dans un réseau de type Campus
- Mettre en œuvre les technologies et techniques de haute disponibilité avec des switchs multi-niveaux
- Mettre en œuvre les fonctionnalités de sécurité dans un réseau commuté
- Intégrer les WLANs dans un réseau de type Campus
- Intégrer la Voix et la Vidéo dans un réseau de type Campus

Contenu :

1. Analyse de la conception d'un Réseau de type campus

- Architecture complexe commutée

2. Mise en œuvre des VLANs dans un Réseau de type campus

- Appliquer les recommandations pour les topologies VLAN
- Configurer les private VLANS
- Configurer l'agrégation de liens avec EtherChannel

3. Mise en œuvre du Spanning-Tree

- Fonctions avancées du protocole Spanning-Tree
- Description des mécanismes STP stability
- Mise en œuvre du routage inter-vlan
- Décrire le routage entre les VLANs
- Déployer les switchs multi niveaux avec Cisco Express Forwarding

4. Mise en œuvre du réseau Haute Disponibilité

- Comprendre la Haute Disponibilité
- Mettre en œuvre la Haute Disponibilité
- Mettre en œuvre la surveillance du réseau

5. Mise en œuvre de la Haute Disponibilité sur la couche 3

- Configurer la redondance sur la couche 3 avec HSRP
- Configurer la redondance sur la couche 3 avec VRRP et GLBP

6. Minimiser la perte de service et le vol de données dans un Réseau de type campus

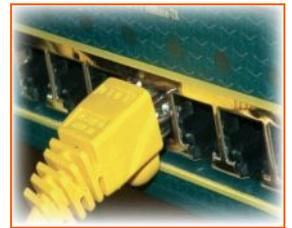
- Comprendre les problèmes de sécurité des switchs
- Protection contre les attaques VLAN
- Protection contre les attaques de type usurpation
- Sécuriser les services réseaux

7. Voix et Vidéo dans un Réseau de type campus

- Planifier le support de la Voix
- Intégrer et vérifier la Voip dans une infrastructure de type Campus
- Travailler avec des spécialistes pour intégrer la VoIP dans un réseau de type Campus

8. Intégration des LANs sans fils dans un Réseau de type campus

- Comparer les WLANs avec les Réseaux de type campus
- Etablir l'Impact des WLANs sur une infrastructure Campus
- Préparer l'infrastructure Campus pour les WLANs



TSHOOT: Troubleshooting and Maintaining Cisco IP Networks V1.0

Ce cours a pour objectif de fournir aux techniciens et aux ingénieurs travaillant sur des réseaux complexes une méthodologie pour maintenir, diagnostiquer et dépanner leurs réseaux le plus rapidement possible. Ce cours fournira des procédures et des outils aussi bien techniques que génériques pour dépanner et diagnostiquer des technologies connues telles que la commutation et le routage entre autre.

La plus large partie du cours s'appuiera sur la mise en pratique (réflexion et manipulation) de ces techniques sur des architectures et des technologies maîtrisées pour permettre aux stagiaires de les adapter en fonction de leurs expériences professionnelles et de leurs organisations.

Durée: 5 jours

Pré-requis: Avoir suivi les cours ICND1, ICND2, ROUTE (BSCI) et SWITCH (BCMSN) ou posséder équivalentes à ces formations.

Objectifs :

- Planifier et documenter les fonctionnalités de maintenance les plus courantes pour des réseaux complexes
- Développer un «process» de dépannage pour identifier et résoudre les problèmes
- Sélectionner les outils nécessaires au dépannage
- Utiliser les procédures de maintenance et de résolution d'erreurs dans les environnements de routage et de commutation
- Mettre en œuvre des procédures de résolution et de maintenance d'infrastructure sécurisée
- Dépanner et maintenir les réseaux complexes hétérogènes

Contenu :

- 1. Planification de la maintenance pour des réseaux complexes**
 - Appliquer les méthodologies de maintenance
 - Procédures courantes de maintenance
 - Outils, applications et ressources pour la maintenance

2. Planification des procédures de dépannage pour des réseaux complexes

- Appliquer les méthodologies de dépannage
- Planifier et mettre en œuvre les procédures de dépannage
- Intégrer le dépannage dans le process de maintenance des réseaux

3. Applications et outils de Maintenance et de dépannage

- Constituer des Outils de Diagnostic à partir de l'IOS Cisco
- Utiliser des outils de maintenance spécialisés

1. Maintenance et dépannage des solutions de Campus switchées

- Dépanner les VLANs
- Dépannage du Spanning-Tree
- Dépanner les interfaces VLAN et le routage inter-vlan
- Dépanner les protocoles FHRPs (First Hop Redundancy Protocols)
- Dépanner les problèmes de performance des commutateurs
- Présentation par le e-learning des technologies de campus switchées

2. Maintenance et dépannage des solutions de routage

- Dépanner les interconnexions de la couche réseau
- Dépanner EIGRP, OSPF, la redistribution des routes, BGP, les problèmes de performance
- Présenter par le e-learning les technologies additionnelles de routage

3. Maintenance et dépannage des solutions de sécurité

- Dépanner les fonctionnalités de sécurité
- Nouvelles commandes et fonctionnalités de sécurité
- Rappels sur les fonctionnalités de sécurité
- Présenter par le e-learning les produits pour le dépannage de la sécurité

4. Maintenance et dépannage des réseaux hétérogènes complexes

- Dépannage d'environnements complexes
- Lab de synthèse

Cursus Sécurité



IINS: Cisco Implementing IOS Unified Network Security V 1.0

Ce cours permettra aux stagiaires de comprendre la nécessité d'appliquer des stratégies de sécurité dans les réseaux. Ils seront capables d'améliorer les tâches pour sécuriser les réseaux à l'aide des fonctionnalités de sécurité disponibles dans l'IOS (Routeur Cisco, SDM, Interface ligne de commande).

Durée: 5 jours

Pré-requis: Avoir suivi les cours ICND1 et ICND2 ou posséder les connaissances équivalentes.

Objectifs :

- Développer une stratégie de sécurité pour se protéger face aux menaces contre la sécurité des informations
- Configurer les routeurs sur les périmètres réseaux avec les fonctionnalités sécurité de l'IOS
- Configurer un pare-feu pour améliorer la sécurité du fonctionnement du réseau
- Configurer les fonctionnalités VPNs Site à site
- Configurer IPS sur les routeurs Cisco
- Configurer les périphériques pour le contrôle d'accès, la résistance aux attaques et protéger l'intégrité et la confidentialité du trafic réseau.

Contenu :

1. Introduction aux principes de sécurité réseau

- Les fondamentaux de la sécurité réseau Méthodologies face aux attaques réseau
- Fonctionnalités de sécurité Descriptif du matériel Cisco.

2. Périmètres sécurité

- Sécuriser l'accès administratif aux routeurs Cisco.
- Présenter Cisco SDM Configurer AAA sur les routeurs Cisco à l'aide de la base de données Local Configurer AAA sur les routeurs en utilisant Cisco Secure ACS
- Mettre en œuvre la gestion de la sécurité et la gestion des rapports Bloquer les routeurs.

3. Sécurité réseau à l'aide des pare-feu

- Technologies pare-feu Créer des filtres statiques à l'aide des ACLs
- Configurer le pare-feu basés sur l'IOS.

4. VPN's Site à site

- Services de cryptographie Cryptage symétrique Signatures digitales et «hashes» cryptés
Cryptage asymétrique et PKI Fondamentaux IPSec
- Créer les VPN IPsec Site à site Configurer IPsec sur les VPNs Site à site à l'aide de SDM

5. Sécurité réseau à l'aide de l'IOS IPS

- Technologies IPS Configurer l'IOS IPS à l'aide de SDM

6. Vue d'ensemble des LAN, SAN, Voix et Endpoint sécurité

- Sécurité des ends points Sécurité des SAN Sécurité de la Voix Voir les attaques de la Couche 2.



SECURE: Securing Networks with Cisco Routers & Switches V1.0

Ce cours apportera aux participants les connaissances nécessaires pour sécuriser les réseaux basés sur des routeurs et les switches Cisco. Il s'agit d'installer et configurer les fonctions Sécurité de Cisco IOS.

Durée: 5 jours

Pré-requis:

Posséder les certifications CCNA (cours ICND1 & ICND2) et CCNA Sécurité (cours complémentaire IINS) ou avoir un niveau équivalent. La connaissance pratique de l'OS Microsoft Windows serait un plus.

Objectifs :

A l'issue de ce stage, les stagiaires seront capables de:

- mettre en œuvre, maintenir et contrôler la protection de l'infrastructure réseau routée ou commutée
- mettre en œuvre et maintenir les contrôles et les technologies d'isolement des menaces dans une infrastructure délimitée par des routeurs Cisco
- mettre en œuvre et maintenir les solutions de VPN sur des routeurs Cisco

Contenu :

1. Déploiement de la protection de Cisco IOS

- Déployer les contrôles de la protection du réseau
- Déployer les contrôles avancés de la sécurité du «Data Plane» des Switches
- Mettre en œuvre les services Cisco IBNS
- Déployer les fonctionnalités 802.1X
- Déployer les contrôles avancés de la sécurité du «Data Plane» des Routeurs
- Déployer les contrôles avancés de la sécurité du «Control Plane»
- Déployer les contrôles avancés de la sécurité du «Management Plane»

2. Déploiement du contrôle des menaces de Cisco IOS

- Déployer la translation d'adresses de Cisco IOS
- Déployer les politiques de pare-feux par Zone
- Déployer les fonctions IPS de Cisco IOS

3. Déploiement de la sécurité des échanges site à site

- Technologies et architecture des VPN site à site
- Déployer les VPNs Site à Site IPSec de type VTI
- Déployer l'authentification dans les VPNs IPSec site à site
- Déployer DMVPNs
- Déployer la haute disponibilité des VPNs IPSec
- Déployer GET VPN

4. Déploiement de l'accès distant sécurisé avec Cisco IOS

- Architectures et technologies de l'accès distant VPN
- Déployer les solutions de l'accès distant à l'aide de SSL VPN
- Déployer les solutions de l'accès distant à l'aide de Cisco Easy VPN

Cursus Sécurité



FIREWALL: Deploying Cisco ASA Firewall Solutions V1.0

Cette formation permettra aux participants de configurer, maintenir et faire fonctionner les pare-feux intégrés sur les Cisco ASA, solution de sécurité informatique.

Durée: 5 jours

Pré-requis:

Avoir suivi les formations Cisco suivantes ou posséder les connaissances équivalentes :

- ICND2 - Interconnecting Cisco Networking Devices Part 2
- IINS - Implementing Cisco IOS Network Security

Objectifs :

A l'issue de ce stage, les stagiaires seront capables de:

- Comprendre les technologies et fonctionnalités Cisco ASA
- De découvrir la famille de produits Cisco ASA
- De comprendre comment les applications de sécurité Cisco PIX et ASA protègent les réseaux contre les attaques
- Préparer les ASA à être configurés via l'interface graphique Cisco Adaptive Security Device Manager (ASDM)
- Configurer les fonctions essentielles à l'aide de ASDM et CLI
- Configurer les translations d'adresses dynamiques et statiques
- Configurer la stratégie d'accès basée sur les ACLs (Listes de contrôle d'accès)
- Utiliser les groupes d'objets pour simplifier la complexité et la maintenance de ACL
- Utiliser des politiques modulaires pour fournir des stratégies spécifiques à certains flux de données
- Prise en main des protocoles avancés avec l'inspection des applications
- Inspection détaillée du trafic sur la couche applications
- Dépanner avec Syslog, Packet tracer et Packet Capture

Contenu :

1. Application de sécurité adaptée Cisco ASA

- Technologie et fonctionnalités
- Famille ASA

2. Connectivité de base et gestion des ASA

- Cisco ASA et Cisco ASDM
- Interfaces et routage statique
- Fonctionnalités de gestion
- Gestion des accès

3. Fonctionnalités de contrôle d'accès Cisco ASA

- Contrôle d'accès basique
- Politique modulaire
- Présentation des fonctionnalités de base de l'inspection
- Stratégies sur la couche d'application
- Contrôles d'accès avancés
- Limites et garanties des ressources
- Stratégies de base utilisateurs

4. Fonctionnalités d'intégration Cisco ASA

- Translation d'adresses réseau
- Fonctionnalités pare-feu en mode transparent

5. Virtualisation des Cisco ASA et fonctionnalités Haute disponibilité

- Fonctionnalités de virtualisation
- Interfaces redondantes
- Haute disponibilité mode actif/standby
- Haute disponibilité en mode actif/actif

6. Modules sécurité Cisco ASA

- Intégration des modules AIP-SSM et AIP-AIP-SSC
- Intégration des modules CSC-SSM

Cursus Sécurité



VPN: Deploying Cisco ASA VPN Solutions V1.0

Ce cours de cinq jours permet de choisir, configuration, et dépannage de la majorité des Cisco ASA adaptive Security appliance, accès distant et de site à site VPN pour réduire les risques IT de l'infrastructure ses applications.

Durée: 5 jours

Pré-requis:

Avoir suivi les formations Cisco suivantes ou posséder les connaissances équivalentes :

- ICND2 - Interconnecting Cisco Networking Devices Part 2
- IINS - Implementing Cisco IOS Network Security
- SECURE
- Avoir les connaissances de Windows Microsoft

Objectifs :

A l'issue de ce stage, les stagiaires seront capables de:

- Evaluer le subsystem VPN d'un ASA
- Déployer les solutions IPSEC VPN d'un ASA
- Déployer les solutions d'accès à distance au VPN Cisco AnyConnect d'un ASA
- Déployer les solutions d'accès à distance Clientless d'un ASA
- Déployer les solutions VPN d'un ASA Avancé

Contenu :

1. Introduction à la prévention et la détection d'intrusion, au logiciel Cisco IPS et aux outils de support.

- Evaluer les systèmes de prévention et de détection d'intrusion
- Choisir les logiciels et matériels Cisco IPS et les applications de support.
- Evaluer les méthodes d'analyse de trafic réseau des sondes IPS, les possibilités d'évasion, et les contremesures anti-évasives.
- Choisir une architecture de déploiement pour une sonde IPS et IDS

2. Installer et maintenir des sondes IPS Cisco

- Intégrer les sondes IPS Cisco dans un réseau
- Rendre performante l'installation initiale d'un IPS
- Gérer les outils IPS Cisco

3. Appliquer les politiques de sécurité d'une sonde IPS Cisco

- Configurer les analyses basiques du trafic
- Implémenter les signatures et les réponses d'une sonde IPS
- Configurer les engins et les bases de données de signature d'une sonde IPS
- Déployer Anomaly-Based Operation

4. Adapter l'analyse de trafic et de réponse à l'environnement

- Customiser l'analyse de trafic
- Gérer les faux positifs et les faux négatifs
- Améliorer la qualité d'alarme et réponse

5. Gérer et analyser les évènements

- Installer et intégrer Cisco IPS Manager Express avec les sondes IPS Cisco
- Gérer et investiguer les évènements utilisant Cisco IPS Manager Express
- Utiliser Cisco IME rapport et notification
- Utiliser les services et la base de données de Cisco IntelliShield

6. Déployer les solutions de virtualisation, de haute disponibilité et de haute performance

- Utiliser les sondes virtuelles Cisco IPS
- Déployer Cisco IPS pour la haute disponibilité et la haute performance

7. Configurer et maintenir le matériel spécifique Cisco IPS

- Configurer et maintenir les modules Cisco ASA AIP-SSM et AIP-SSC-5
- Configurer et maintenir les modules Cisco ISR IPS AIM et IPS NME
- Configurer et maintenir le Cisco IDSM-2



IPS: Implementing Cisco Intrusion Prevention System V 7.0

Ce cours de cinq jours permet aux ingénieurs de la sécurité réseau de déployer des solutions de sécurité basée sur les IPS Cisco. Ils seront en mesure de réduire les risques pour l'infrastructure informatique et ses applications à l'aide des fonctionnalités IPS Cisco, et de fournir le soutien nécessaire.

Durée: 5 jours

Pré-requis:

- Avoir suivi le cours ICND1 & ICND 2.
- Avoir suivi le cours IINS Mettre en œuvre la sécurité des réseaux IOS Cisco.
- Posséder les connaissances de base sur Windows. Connaître la terminologie et les concepts de la sécurité réseau.

Objectifs :

À l'issue de ce cours, le stagiaires sera en mesure de :

- Évaluer les produits et les architectures de déploiement pour la gamme de produits Cisco IPS.
- Effectuer une mise en œuvre initiale d'un capteur de Cisco IPS.
- Mettre en œuvre une politique de sécurité initial à l'aide d'un capteur de Cisco IPS conformément aux politiques locales et des exigences environnementales.
- Déployer des politiques personnalisés pour adapter les IPS Cisco analyse du trafic et la réponse à l'environnement cible.
- Mettre en œuvre une base Cisco IPS données solution de gestion et analyse.
- Mettre en œuvre complexe Cisco IPS politique, haute disponibilité, solutions de virtualisation et haute performance conformément aux politiques et aux exigences environnementales.
- Effectuer la configuration initiale du et maintenir le matériel spécifique de Cisco IPS.

Contenu :

1. Introduction à la prévention et la détection d'intrusion, le logiciel Cisco IPS et les périphériques supportés

- Evaluer la prévention d'intrusion et les systèmes de détection d'intrusion
- Choisir les logiciels et matériel IPS ainsi que les applications supportées
- Evaluer l'analyse du trafic réseau IPS , les méthodes, les possibilités «d'évasion» et «anti-évasive contremesures»
- Choisir l'architecture de déploiement de réseaux IPS et IDS

2. Installation et maintenance des sondes Cisco IPS

- Intégrer la sonde Cisco IPS dans un réseau
- Améliorer la configuration initiale des sondes Cisco IPS
- Gérer les périphériques Cisco IPS

3. Appliquer les stratégies de sécurité Cisco IPS

- Configurer l'analyse de base du trafic
- Mettre en œuvre les signatures Cisco IPS et les réponses*
- Configurer la «signature Engine» et la base de données signatures de Cisco IPS
- Déployer l'opération «anomalie»

4. Adaptation de l'analyse du trafic et des réponses à l'environnement

- Personnaliser l'analyse du trafic
- Gérer les faux positifs et négatifs
- Améliorer la qualité des alarmes et des réponses

5. Gestion et analyse des évènements

- Installer et intégrer Cisco IPS Manager Express avec les sondes Cisco IPS
- Gérer les évènements à l'aide de Cisco IPS Manager Express
 - Utiliser Cisco IME Rapports et notifications
- Intégrer Cisco IPS avec Cisco Security Manager et Cisco Security MARS
- Utiliser la base de données et les services IntelliShield

6. Déploiement de la virtualisation, de la haute disponibilité et les solutions de Haute Performance

- Utiliser les sondes virtuels Cisco IPS
- Déployer Cisco IPS pour la haute disponibilité et la haute performance

7. Configurer et maintenir le matériel spécifique Cisco IPS

- Configurer et maintenir Cisco ASA AIP SSM et les modules AIP SSC
- Configurer et maintenir Cisco ISR IPS AIM et les modules IPS NME
- Configurer et maintenir le module Cisco IDSM-2

Cursus Architecture Réseaux



ARCH: Designing Cisco Network Service ArchitecturesV2.1

Ce cours est conçu pour permettre aux participants d'acquérir les méthodes de design pour concevoir des solutions réseaux complexes, stables et efficaces.

Durée: 5 jours

Pré-requis: avoir suivi les cours

- ICND 1 & 2
- DESIGN
- SWITCH

Objectifs :

À l'issue de ce cours, le stagiaires sera en mesure de:

- Introduire les Architectures de réseau de Cisco pour l'entreprise et d'expliquer comment ce concept d'adresses de l'entreprise réseau à besoins de performances, d'évolutivité et de disponibilité.
- Décrire comment les Architectures de réseau de Cisco de l'entreprise peut être utilisées comme un cadre pour la conception de réseaux d'entreprise.
- Créer des modèles de réseau de campus conceptuel, intermédiaire et détaillée.
- Créer des modèles de centre de données conceptuels, intermédiaire et détaillée.
- Créer des modèles de l'infrastructure distante.
- Créer des réseaux conceptuels, intermédiaires et détaillés pour des raisons de sécurité.
- Créer des modèles VPN conceptuels, intermédiaires et détaillées.

Contenu :

- Introduction
- **Module 1:** Cisco Network Architectures for the Enterprise
- **Module 2:** Enterprise Campus Network Design
- **Module 3:** Advanced Addressing and Routing Design
- **Module 4:** Advanced WAN Services Design Considerations
- **Module 5:** Enterprise Data Center Design
- **Module 6:** E-Commerce Module Design
- **Module 7:** SAN Design Considerations
- **Module 8:** Security Services Design
- **Module 9:** IPsec and SSL VPN Design
- **Module 10:** IP Multicast Design
- **Module 11:** Network Management Capabilities with Cisco IOS Software

Cursus Architecture Réseaux



DESIGN: Cisco Designing for Cisco Internetworks Solution V2.1

Ce cours est destiné aux candidats à la certification CCDA et CCDP, ainsi qu'aux ingénieurs impliqués dans les phases d'avant vente, de conception, de planification et de déploiement de réseaux. Ce cours permettra aux stagiaires de concevoir un réseau correspondant aux exigences du client : concevoir un plan d'adressage, sélectionner le protocole de routage approprié, identifier les critères de sécurité, concevoir l'infrastructure de réseau de façon hiérarchisée, évaluer l'impact du transport de la voix sur le réseau, planifier la mise en place et présenter le projet de conception du réseau au client.

Durée: 5 jours

Pré-requis:

Etre CCNA ou avoir une expérience équivalente.

Avoir suivi le cours SWITCH ou BCMSN.

Il est vivement recommandé de posséder une première expérience dans le déploiement et sur des réseaux à base d'équipements Cisco.

Suivi la formation SWITCH.

Objectifs :

- Concevoir un réseau correspondant aux exigences du client .
- Concevoir un plan d'adressage, sélectionner le protocole de routage approprié,
- Identifier les critères de sécurité, concevoir l'infrastructure de réseau de façon hiérarchisée,
- Évaluer l'impact du transport de la voix sur le réseau.
- Planifier la mise en place.
- Présenter le projet de conception du réseau au client.
- Ce cours explique les idées, les notions (Quoi et Pourquoi?) ainsi que la méthode de mise en place (Comment?).

Contenu :

1. Principe de conception de réseaux

- Présentation de la méthodologie.
- Présentation des procédures.
- Présentation du modèle hiérarchisé

2. Concepts d'infrastructure réseau

- Définition détaillée de l'approche modulaire.
- Problématique de la conception des réseaux switchés de campus
- Définition de l'environnement réseau local.
- Choix des systèmes de câblages et des équipements de niveau 2.

3. Problématiques de la conception des réseaux WAN

- Evaluation des offres de transport actuel proposées par les opérateurs.

4. Conception d'un plan d'adressage IP

- Présentation des contraintes et des avantages de différentes solutions et techniques
- Conséquence sur le choix du protocole de routage.

5. Choix du protocole de routage.

- Présentation des protocoles disponibles.
- Evaluation des critères opportuns dans la structure proposée.

6. Introduction aux concepts de réseaux sécurisés

- Evaluation des menaces pesant sur chacun des éléments du réseau.
- Présentation des solutions.

7. Introduction aux concepts de réseaux voix

- Présentation succincte des technologies de transport de la voix sur un réseau de données.
- Présentation des paramètres influençant la conception de l'infrastructure (bande passante, QoS).

8. Introduction aux concepts d'administration de réseaux

- Présentation des protocoles.
- Présentation des fonctions de l'administration.

9. Récapitulatif de l'ensemble de cours

- Etude de cas complète permettant une première mise en pratique des méthodes et techniques acquises durant ce cours.

Cursus Management de Réseaux



CWLMS: Implementing CiscoWorks LMS V 3.1

Ce cours permet de découvrir toute la gamme d'applications CiscoWorks (CiscoWorks 2003 Server, Ressource Manager Essentials, Campus Manager, IPM, DFM, CiscoView, Device Center, CiscoWorks Assistant, CiscoWorks Portal) ainsi que leurs capacités à manager un réseau Cisco.

Durée: 5 jours

Pré-requis: Avoir suivi le cours ICND1 ou posséder les connaissances équivalentes. Il est vivement recommandé de posséder une première expérience dans le déploiement et d'avoir travaillé sur des réseaux à base d'équipements Cisco

Objectifs :

A l'issue du stage les participants seront capables de :

- concevoir un réseau correspondant aux exigences du client
- concevoir un plan d'adressage, sélectionner le protocole de routage approprié,
- identifier les critères de sécurité, concevoir l'infrastructure de réseau de façon hiérarchisée,
- évaluer l'impact du transport de la voix sur le réseau.
- Planifier la mise en place. Présenter le projet de conception du réseau au client.
- Ce cours explique les idées, les notions (Quoi et Pourquoi?) ainsi que la méthode de mise en place

Contenu :

1. Principe de conception de réseaux

- Présentation de la méthodologie.
- Présentation des procédures.
- Présentation du modèle hiérarchisé.

2. Concepts d'infrastructure réseau

- Définition détaillée de l'approche modulaire.

3. Problématique de la conception des réseaux switchés de campus

- Définition de l'environnement réseau local.
- Choix des systèmes de câblages et des équipements de niveau 2.

4. Problématiques de la conception des réseaux WAN

- Evaluation des offres de transport actuel proposées par les opérateurs.

5. Conception d'un plan d'adressage IP

- Présentation des contraintes et des avantages de différentes solutions et techniques
- Conséquence sur le choix du protocole de routage.

6. Choix du protocole de routage.

- Présentation des protocoles disponibles.
- Evaluation des critères opportuns dans la structure proposée.

7. Introduction aux concepts de réseaux sécurisés

- Evaluation des menaces pesant sur chacun des éléments du réseau.
- Présentation des solutions.

8. Introduction aux concepts de réseaux voix

- Présentation succincte des technologies de transport de la voix sur un réseau de données.
- Présentation des paramètres influençant la conception de l'infrastructure (bande passante, QoS).

9. Introduction aux concepts d'administration de réseaux

- Présentation des protocoles.
- Présentation des fonctions de l'administration.

Récapitulatif

- Etude de cas complète permettant une première mise en pratique des méthodes et techniques acquises durant ce cours

Cursus Téléphonie IP & Communication Unifiée



ICOMM: Introducing Cisco Voice and Unified Communications Administration V1.0

Au cours de cette formation, les participants découvriront les fonctionnalités supportées par **CUCM* (Cisco Unified Communications Manager) et CUCM* Express** et d'autres composants (CUCX, CUPS). Ils apprendront à maintenir le système et ils découvriront les tâches quotidiennes d'administration.

Durée: 5 jours

Pré-requis:

Posséder des connaissances de base sur Cisco CUCM, et Unity Connection, ainsi que sur les tâches de base d'administration des routeurs

Objectifs :

A l'issue de cette formation, les stagiaires seront capables de :

- Utiliser les composants et les caractéristiques de la solution Cisco de Communications Unifiées
- Reconstituer le cheminement des appels
- Utiliser les différentes interfaces d'accès aux composants de Communications Unifiées
- Configurer les terminaux téléphoniques
- Mettre en oeuvre et configurer les utilisateurs ainsi des fonctions téléphoniques
- Configurer les boîtes de messagerie vocales des utilisateurs et les options associées
- Configurer Cisco Unified Presence
- Configurer et générer les rapports à partir du Cisco Unified Reporting de CUCM
- Activer et analyser les rapports des tickets de taxation
- Utiliser l'outil Cisco Call Details Records Analysis and Reporting (CAR) et Real-Time Monitoring Tool (RTMT)
- Surveiller l'utilisation des messages vocaux dans Cisco Unity Connection
- Configurer le système de récupération d'urgence

Contenu :

1. Présentation de la Solution Cisco de Communications Unifiées

- Composants des architectures de Communications Unifiées Cisco
- Les réseaux voix traditionnels et convergés
- Le transport de la Voix et la signalisation
- Paramètres et mécanismes de QoS

2. Interfaces administrateurs et utilisateurs

- Interfaces graphiques et ligne de Commandes pour l'administration de CUCM
- Définir les privilèges d'accès au CUCM
- Interfaces d'administration pour d'autres composants (CUCME,CUE,CUCX,CUPS)
- Interfaces utilisateurs de ces mêmes composants

3. Diagrammes des flux et architectures avec Cisco CUCM et CUCM Express

- Configuration de Dial-peer pots et VoIP sur CUCME pour établir des call legs
- Paramétrage de la discrimination dans CUCM et CUCME
- Éléments pour router les appels avec CUCM
- Groupements de postes
- Notion de Region,Location et CAC avec CUCM

4. Administration des terminaux et utilisateurs

- Paramétrage pour l'enregistrement d'un phone IP sur CUCM et CUCME
- Administration des comptes utilisateurs et des terminaux

5. Activation de fonctionnalités utilisateurs

- Fonctions téléphoniques sur CUCM et CUCME
- Extension et Unified Mobility

6. Mise en œuvre de Cisco Unity Connection et Cisco Unified Presence

- Caractéristiques et configuration nécessaires des boîtes vocales des utilisateurs
- Options pour le paramétrage des boîtes vocales des utilisateurs dans CUCX
- Architectures et gestion des utilisateurs avec Cisco Unified Presence

7. Maintenance des solutions Cisco de Communications Unifiées

- Dépanner les problèmes d'enregistrement des phones et de QoS
- Générer des rapports avec le Cisco Unified Reporting , CDR Analysis and Reporting, Cisco Unified Real-Time Monitoring Tool
- Surveillance de la messagerie vocale dans Cisco Unity Connection
- Système de récupération d'urgence (Disaster Recovery System)

Cursus Téléphonie IP & Communication Unifiée



CVOICE: Cisco Voice Over IP V8.0

Cette formation apporte les connaissances nécessaires sur la passerelle Voix, les caractéristiques sessions d'appels VoIP, les plans de numérotation et leurs mises en œuvre ainsi que la mise en œuvre des téléphones IP dans un environnement Cisco Unified Communications Manager Express. Les mécanismes QoS relatifs à la Voix nécessaires dans les réseaux Cisco Unified Communication sont aussi abordés dans ce cours.

Durée: 5 jours

Pré-requis:

Avoir suivi les formations Cisco ICND1, ICND2 et ICOMM ou posséder les connaissances équivalentes.

Objectifs :

A l'issue de ce stage, les stagiaires seront capables de :

- Expliquer ce qu'est une passerelle Voix, comment elle travaille et décrire son utilisation, ses composants et ses fonctionnalités
- Décrire les caractéristiques et les éléments de configuration des sessions d'appels VoIP
- Décrire comment mettre en œuvre les téléphones IP à l'aide de Cisco Unified Communications Manager Express
- Décrire les composants d'un plan de numérotation et expliquer comment mettre en œuvre un plan de numérotation sur une passerelle voix Cisco Unified
- Expliquer ce que sont les gatekeepers et Cisco Unified Border Element (CUBE), comment ils travaillent, et quelles fonctionnalités ils supportent
- Décrire pourquoi la QoS est nécessaire, quelles fonctions sont améliorées et comment elle peut être mise en œuvre dans le réseau Cisco Unified Communications

Contenu :

1. Introduction à la Voix sur IP dans un environnement Cisco

- Comprendre les réseaux Cisco Unified Communications et le rôle des passerelles
- Examiner le routage d'appels et les sessions d'appels
- Configurer les ports Voix
- Comprendre les fonctionnalités DSP, les Codecs et les Codes complexes

2. Session d'appels VoIP

- Examiner les caractéristiques des sessions d'appels VoIP et la transmission Media VoIP
- Expliquer le protocole de signalisation H.323
- Expliquer le protocole de signalisation SIP
- Expliquer le protocole de signalisation MGCP
- Décrire les besoins nécessaires pour les sessions d'appels
- Configurer les sessions d'appels VoIP

3. Mise en oeuvre de Cisco Unified Communications Manager Express Endpoints

- Introduction à Cisco Unified Communications Manager Express
- Examiner les besoins de Cisco Unified Communications Express Endpoint
- Configurer les endpoints de Cisco unified Communications Manager Express

4. Mise en oeuvre du plan de numérotation

- Introduction au plan de numérotation
- Comprendre le plan de numérotation
- Décrire la manipulation de digits
- Configurer la sélection de route
- Configurer les privilèges d'appels

5. Gatekeepers et mise en oeuvre de Cisco Unified Border Element

- Comprendre les Gatekeepers
- Examiner Cisco Unified Border Element

6. Qualité de service

- Introduction à QoS
- Comprendre les mécanismes et modèles QoS
- Expliquer la classification, le marquage et les mécanismes de liens efficaces
- Gérer la congestion et les limites
- Comprendre Cisco AutoQoS

Cursus Téléphonie IP & Communication Unifiée



CIPT 1: Implementing Cisco Unified Communication Manager PART 1 V 8.0

Cette formation prépare les participants à la mise en œuvre de la **solution Cisco Unified Communications Manager (CUCM)** dans un environnement mono site. Elle est orientée sur la version 8 du Cisco Unified Communications Manager , plus précisément sur le routage d'appels et les composants de signalisation pour la solution Cisco Unified Communications.

Durée: 5 jours

Pré-requis: Avoir suivi la formation Cisco CVOICE V8 ou posséder les connaissances équivalentes.

Objectifs :

A l'issue de la formation, les stagiaires seront capables de :

- Décrire la solution Cisco CUCM incluant les fonctions, l'architecture, le déploiement, les options de redondance, l'installation et la mise à jour
- Effectuer la configuration initiale de Cisco CUCM et la gestion des utilisateurs
- Configurer Cisco CUCM pour supporter les appels on-cluster
- Mettre en oeuvre l'accès PSTN dans CUCM et construire le plan de numérotation dans le déploiement d'un MONO site CUCM
- Mettre en oeuvre les ressources Media CUCM
- Mettre en oeuvre les fonctionnalités et applications de Cisco CUCM

Contenu :

1. Introduction à Cisco CUCM

- Comprendre la solution Cisco Unified Communication Manager
- Comprendre le déploiement de Cisco Unified Communications Manager et les options de redondance

2. Administration de Cisco CUCM

- Gestion des services et configuration initiale de Cisco Unified Communications Manager
- Gestion des comptes utilisateurs dans Cisco Unified Communications Manager

3. Appels On-net mono site

- Présentation des terminaux dans CUCM
- Mettre en oeuvre des téléphones IP

4. Appels off-net mono site

- Mettre en oeuvre les passerelles PSTN dans CUCM
- Configurer les composants du routage d'appels dans CUCM
- Utiliser les partitions et CSSs pour mettre en oeuvre les privilèges d'appels pour les appels off-net
- Mettre en oeuvre la manipulation des digits dans CUCM
- Mettre en oeuvre la sélection des passerelles et les fonctionnalités d'accès PSTN
- Mettre en oeuvre la fonction Call coverage dans CUCM

5. Ressources Media

- Mettre en oeuvre les ressources Media dans CUCM

6. Mise en oeuvre des fonctionnalités et applications

- Configurer les services des téléphones IP Cisco
- Configurer la fonction de présence native dans CUCM
- Configurer Cisco Unified Mobility

Cursus Téléphonie IP & Communication Unifiée



CIPT 2: Implementing Cisco Unified Communication Manager PART 2 V 8.0

Cette formation permettra aux stagiaires de **mettre en oeuvre la solution Cisco Unified Communications (CUCM) dans un environnement multi-sites**. Elle couvre également des sujets tels que le routage d'appels globalisé, SAF (Cisco Service Advertisement Framework) et CCD (Call Control Discovery), TEHO (Tail-end hop-off), SRST (Cisco Unified Survivable Remote Site Telephony) et les fonctionnalités de mobilité telles que Cisco Device Mobility et Cisco Extension Mobility

Durée: 5 jours

Pré-requis: Avoir suivi la formation Cisco CIPT1V8 ou posséder les connaissances équivalentes

Objectifs :

A l'issue de ce stage, les stagiaires seront capables de:

- Décrire les problèmes et les solutions aux problèmes de déploiement multi-sites.
- Décrire et configurer les éléments requis pour le plan de numérotation
- Mettre en oeuvre la résilience du processus d'appels dans les sites distants à l'aide de Cisco unieif SRST, MGCP fallback et Cisco Unified Communications Manager Express en mode SRST
- Mettre en oeuvre la gestion de la bande passante et du CAC pour prévenir une surallocation sur le WAN IP
- Mettre en oeuvre Device Mobility et Cisco Extension Mobility
- Décrire et mettre en oeuvre les déploiements CCD

Contenu :

1. Mise en oeuvre du déploiement multi-site

- Identifier les problèmes de déploiement multi-site
- Apporter les solutions pour un déploiement multi-sites
- Mettre en oeuvre les connexions multi-site
- Mettre en oeuvre le plan de numérotation pour les déploiements internationaux multi-site

2. Mise en oeuvre de la redondance du process d'appels centralisé

- Examiner les options de redondance des sites distants
- Mettre en oeuvre du SRST et de MGCP Fallback
- Mettre en oeuvre CUCM Express dans le mode SRST

3. Gestion de la bande passante et contrôle d'admission des appels

- Gestion de la bande passante
- Mettre en oeuvre du CAC

4. Fonctionnalités et applications pour les déploiements multi-sites

- Mettre en oeuvre Device Mobility
- Mettre en oeuvre Cisco Extension Mobility

5. Découverte du contrôle d'appels

- Mettre en oeuvre SAF et CCD

Cursus Téléphonie IP & Communication Unifiée



TVOICE: Troubleshooting Cisco Unified Communications Systems V8.0

Cette formation permettra aux participants de diagnostiquer et de résoudre les problèmes sur le système **Cisco Unified Communications Manager CUCM v8** ainsi que sur les passerelles Cisco VoIP.

Durée: 5 jours

Pré-requis: Avoir suivi les formations Cisco CVOICEv8, CIPT1v8 et CIPT2v8 ou posséder les connaissances équivalentes.

Objectifs : A l'issue de ce stage, les stagiaires seront capables de:

- Appréhender une méthodologie de dépannage
- Utiliser les outils et rapports permettant d'isoler les problèmes
- Utiliser les outils de dépannage et de surveillance tels que RTMT
- Dépanner les problèmes courants des passerelles et des terminaux téléphoniques
- Dépanner les problèmes de réplication des bases de données dans les clusters CUCM
- Dépanner l'intégration avec les serveurs LDAP
- Diagnostiquer et résoudre les problèmes d'appels
- Examiner les problèmes au sein d'un cluster («on-premise single-site calling»)
- Examiner les problèmes entre clusters («on-net multisite calling»)
- Identifier les problèmes d'accès PSTN («off-net calling»)
- Dépanner SAF et CCD
- Diagnostiquer et résoudre les problèmes liés à Extension, Device et Unified Mobility
- Identifier les problèmes de «Presence» native à CUCM
- Dépanner les problèmes de MOH, MTP, conférences et transcodeurs
- Diagnostiquer et résoudre les problèmes des agents RSVP pour la QoS
- Dépanner la qualité des transmissions Voix et Video
- Dépanner un plan de numérotation globalisé E.164

Contenu :

1. Introductions au dépannage des solutions de communications unifiées cisco

- Identifier les différents éléments d'un déploiement d'une solution ToIP CUCM
- Comprendre la méthodologie Cisco de dépannage
- Décrire les principaux outils de dépannage et de surveillance de CUCM et de l'IOS

2. Dépannage Cisco CUCM

- Problèmes d'enregistrements des terminaux
- Problèmes liés aux passerelles MGCP, H323 et SIP
- Problèmes de disponibilité CUCM
- Problèmes de réplication de bases de données
- Problèmes d'intégration LDAP

3. Dépannage des problèmes d'appels

- Examiner les principales causes de problèmes lors de l'établissement des appels
- Rappeler le fonctionnement du plan de numérotation CUCM et résoudre les principales problématiques
- Problèmes d'appels dans un cluster
- Problèmes d'appels entre clusters
- Problèmes d'appels lors des accès PSTN

4. Dépannage des problèmes SAF et CCD

- Décrire les éléments du service SAF et CCD et savoir les dépanner

5. Dépannage des fonctionnalités CUCM et des problèmes d'applications

- Problèmes avec Device Mobility
- Problèmes avec Extension Mobility
- Problèmes liés à Unified Mobility (Mobility Connect et Mobility Voice Access)
- Problèmes avec la «Presence», native au CUCM

6. Dépannage des problèmes de qualité de la VoIP (QoS) et des Media Resources

- Problèmes MOH
- Problèmes MTP
- Problèmes sur les conférences
- Problèmes de transcodeurs
- Problèmes avec les agents RSVP
- Problèmes de qualité de la VoIP

Cursus Téléphonie IP & Communication Unifiée



CAPPS: Integartion Cisco Unified Communications Applications V8.0

Cette formation permettra aux participants de comprendre les différents modes d'intégration de Cisco Unified Presence, de Cisco Unity Express et de Cisco Unity Connection, appuyés par des exemples de déploiements et des mécanismes de dépannage

Durée: 5 jours

Pré-requis:

- Avoir déjà travaillé sur des réseaux de convergence Voix/données.
- Posséder des connaissances basiques de l'IOS des Gateways Cisco.

Objectifs : A l'issue de ce stage, les stagiaires seront capables de:

- Décrire les différents modes d'intégration et les conditions nécessaires
- Mettre en oeuvre Cisco Unity Connection lors du déploiement de Cisco Unified Communications Manager
- Décrire comment mettre en oeuvre Cisco Unity Express lors du déploiement de Cisco Unified Communications Manager Express
- Mettre en oeuvre la messagerie vocale à l'aide de VPIM
- Mettre en oeuvre Cisco Unified Presence et Cisco Unified Personal Communicator

Contenu :

1. Introduction à la messagerie vocale

- Vue d'ensemble de l'intégration de la messagerie vocale
- Besoins nécessaire pour l'intégration de la messagerie vocale

2. Cisco Unity Connection dans l'environnement Cisco Unified Communications Manager

- Intégration avec Cisco Unified Communications Manager
- Configurer le système Cisco Unity Connection
- Utiliser les partitions pour Cisco Unity Connection et Search Space

- Mettre en oeuvre Cisco Unity Connection Call Management
 - Configurer les utilisateurs de Cisco Unity Connection
 - Superviser et dépanner Cisco Unity Connection
- 3. Mise en oeuvre de Cisco Unity Express dans l'environnement Cisco Unified Communications Manager Express**
- Comprendre Cisco Unity Express
 - Intégration de Cisco Unity Express avec Cisco Unified Communications Manager Express
 - Configurer le système Cisco Unity Express
 - Configurer les utilisateurs de Cisco Unity Express
 - Comprendre Cisco Unity Express AutoAttendant
 - Dépanner Cisco Unity Express
- 4. Voice Profile pour développer la messagerie sous Internet**
- Comprendre VPIM
 - Mettre en oeuvre VPIM sous Cisco Unity Connection
 - Mettre en oeuvre VPIM sous Cisco Unity Express
- 5. Mise en oeuvre de Cisco Unified Presence**
- Comprendre Cisco Unified Presence
 - Comprendre les composants et les flux de communication de Cisco Unified Presence
 - Intégrer Cisco Unified Presence
 - Configurer les fonctionnalités de Cisco Unified Presence et mettre en oeuvre Cisco Unified Personal Communicator
 - Outils de vérification et de dépannage des composants de Cisco Unified Presence

Cursus Réseaux Sans Fil



IUWNE: Implementing Unified Wireless Networking Essentials V1.0

Ce cours est conçu pour aider les stagiaires à préparer la certification CCNA Wireless. Il donnera aux stagiaires les informations nécessaires pour concevoir, installer, configurer, surveiller et mener les tâches basiques de dépannage sur les WLANs en entreprise.

Durée: 5 jours

Pré-requis: Avoir suivi les cours ICND1 et ICND2 ou posséder les connaissances équivalentes

Objectifs :

- Décrire les fondamentaux des technologies sans fils
- Installer et configurer les contrôleurs WLAN dans un réseau unifié sans fils
- Installer le client et configurer des profils clients sans fils
- Configurer la sécurité sans fils
- Gérer le réseau avec l'outil Cisco Wireless System Navigator (WCS)
- Utiliser le contrôleur et le WCS pour dépanner un réseau sans fils

Contenu :

1. Fondamentaux sans fils

- Présenter les réseaux sans fils et les topologies
- Présenter les principes en Radio Fréquence
- Examiner les antennes
- Comprendre les techniques de bases à étalement de spectre
- Examiner les standards, organismes de réglementation et certification
- Examiner la structure et les technologies physiques sans fils 802.11 et leurs impacts sur les Vlans
- Structure de la journée

2. Installation de base Cisco WLAN

- Comprendre l'architecture de base d'un réseau Cisco sans fils
- Configurer un contrôleur
- Découvrir et associer un Point d'Accès à un contrôleur
- Examiner les modes de fonctionnement des différents Point d'Accès
- Mode itinérant
- Gérer le réseau à partir du contrôleur
- Configurer et migrer les Access-points Stand alone
- Comprendre l'architecture sans fils de Cisco (Cisco Mobility Express Wireless Architecture)

3. Clients sans fils

- Utiliser les outils de configuration par défaut
- Décrire l'outil client (Cisco Secure Service Client)

4. Comprendre le programme d'extension Cisco (CCX) Sécurité WLAN

- Vue d'ensemble de la sécurité des WLANs
- Sécurité IEEE 802.11
- Centraliser la sécurité des WLANs
- Décrire les méthodes d' authentifications EAP
- Gérer les authentifications et le cryptage avec le WPA et WPA 2
- Configurer la sécurité sans fils sur les contrôleurs et les clients

5. Administration WCS

- Présenter l'outil WCS
- Installer le WCS
- Administrer le WCS
- Travailler avec les contrôleurs à partir du WCS
- Travailler avec les cartes clientes
- Assurer la surveillance avec le WCS

6. Maintenance et dépannage

- Assurer le dépannage du système
- Conception et besoins en évaluation de site
- Dépannage

Cursus Réseaux Sans Fil



CUWSS: Conducting Cisco Unified Wireless Site Survey V1.0

Dans cette formation, les stagiaires pourront se préparer pour la Certification CCNP Wireless, et avoir une bonne compréhension sur la manière de procéder à une étude de site. Ils pourront explorer les topologies des réseaux sans-fils voix et données, les services de localisation, les outils de planification de Cisco WCS, le Cisco Spectrum Expert et AirMagnet Survey Pro, ainsi que les méthodologies et la gestion de projet

Durée: 5 jours

Pré-requis: Posséder la certification CCNA Wireless

Objectifs : A l'issue de la formation, les stagiaires seront capables de :

- Préparer, planifier, concevoir, mettre en œuvre et optimiser un WLAN
- Analyser les besoins techniques en signal radio pour les applications sans fils
- Elaborer un projet pour la data, la voix et le service de localisation.
- Réaliser une étude de site couche 1 avec le Cisco Spectrum Expert pour identifier les interférences
- Réaliser une étude de site couche 2 pour les équipements 802.11n (Greenfield Survey)
- Réaliser un audit d'un site WLAN déjà installé
- Compléter un rapport d'audit de site

Contenu :

1. Etude de site

- Besoins nécessaires pour les différentes industries verticales
- Déterminer les besoins pour les applications RF
- Besoins clients
- Problèmes réguliers
- Besoins en sécurité et d'esthétisme
- Besoins logistiques

2. Planifier l'évaluation du site

- Sélectionner un modèle de données
- Caractéristiques de déploiement
- Outils nécessaires pour compléter un audit de site
- Documents d'étude de site

3. Effectuer l'évaluation de site

- Produire une étude de site prédictive
- Effectuer une étude de site sur la couche 1
- Effectuer une étude de site pour les données sur la couche 2
- Effectuer une étude de site pour les applications vocales sur la couche 2
- Effectuer l'étude de site pour les clients 802.11

4. AP, Contrôleur et Licence

- Besoins d'infrastructure pour les WLAN
- Equipements et licences pour WLAN

5. Déploiement

- Vérifier la couverture RF

6. Présenter un rapport d'installation

Cursus Réseaux Sans Fil



IUWVN: Implementing Cisco Unified Wireless Voice Networks V1.0

Cette formation permettra aux participants d'intégrer les services VoWLAN dans le réseau WLAN et de mettre en œuvre la QoS et les applications à bande passante élevée dans le réseau sans fils

Durée: 5 jours

Pré-requis: Posséder la certification CCNA Wireless

Objectifs : A l'issue de la formation, les participants seront capables de :

- Mettre en œuvre la QoS pour les applications sans fils
- Architecture traditionnelle et VoIP
- Concevoir un réseau sans fils pour assurer le support de la Voix
- Mettre en œuvre la Voix sur l'infrastructure réseau LAN sans fils
- Mettre en œuvre le Multicast sur un réseau sans fils
- Configurer l'infrastructure sans fils pour la vidéo et les applications à haute bande passante

Contenu :

1. Mise en œuvre de la QoS pour les applications sans fils

- Besoins pour la QoS sans fils
- Schémas de déploiement de la QoS
- Configurer le WLC et le WCS pour la QoS
- Configurer l'infrastructure filaire pour la QoS
- Meilleures pratiques pour le déploiement de la QoS

2. Voix sur une architecture sans fils

- Evolution de l'architecture de la Voix
- Circuit d'appels VoWLAN
- Concevoir un réseau sans fils pour la Voix
- Vérifier la disponibilité de la Voix

3. Mise en œuvre de VoWLAN

- Besoins matériels et logiciels pour la VoIP
- Configurer un WLAN pour la Voix
- Configurer l'infrastructure des périphériques pour la Voix sur les réseaux sans fils
- Configurer la Voix sur les téléphones sans fils
- Dépanner les VoWLANs

4. Mise en œuvre du Multicast sur un réseau sans fils

- Concepts Multicast
- Implications du Multicast dans les réseaux sans fils
- Configurer le Multicast dans les réseaux sans fils
- Dépanner le Multicast dans les réseaux sans fils

5. Préparation du réseau sans fils pour la Vidéo et les applications à haute bande passante

- Mettre en œuvre la QoS pour les applications sensibles
- Avantages de 802.11n pour la vidéo
- Calculer les besoins en bande passante et configurer le réseau sans fils pour les applications vidéo

Cursus Réseaux Sans Fil



IUWMS: Implementing Cisco Unified Mobility Service V1.0

Cette formation permettra aux participants d'apprendre à intégrer les services de mobilité dans le réseau Wlan, de dépanner le réseau WLAN et d'en assurer la mise en œuvre

Durée: 5 jours

Pré-requis: Posséder la certification CCNA Wireless

Objectifs : A l'issue de la formation, les participants seront capables de :

- Concevoir une infrastructure WLAN pour les services de localisation
- Concevoir le réseau pour la haute disponibilité
- Mettre en œuvre du service de localisation Cisco
- Configurer des Template sur WCS pour le contrôleur et pour les Access-point
- Mettre en œuvre et gérer les réseaux maillés dans l'entreprise
- Installer le réseau sans fil à l'extérieur
- Améliorer la couche 2 pour les périphériques 802.11n
- Concevoir une évaluation et un audit d'un site sans-fil une fois installé
- Compléter un rapport d'étude de site

Contenu :

1. Conception d'une infrastructure WLAN mobile

- Utiliser les pratiques recommandées
- Implication des couches 2 et 3
- Concevoir une infrastructure de haute disponibilité
- Concevoir un SSID pour la mobilité

2. Mise en œuvre et gestion des services avancés avec le WCS et le navigateur WCS

- Configurer le contrôleur et les Access points
- Configurer le WCS pour WLC Auto-provisioning
- Mettre en œuvre du partitionnement WCS
- Planifier l'accès sans fils à l'aide du WCS
- Configurer les rapports
- Configurer les tâches administratives
- Connecter et dépanner les clients
- Rôles, caractéristiques et fonctionnement du navigateur WCS

3. Conception d'un réseau sans fils

- Besoins en déploiements
- Applications de RFID, Chokepoint et TDoA

4. Mise en œuvre des services Cisco

- Architecture et équipements des services de mobilité
- Configurer le Cisco 2700 Series et Cisco 3300 Series
- Intégrer et gérer le MSE et le location Appliance avec WCS
- Configurer et optimiser avec WCS, MSE et le Location Appliance
- Suivi des clients mobiles
- Configurer, générer, interpréter les notifications d'évènements
- Intégrer les applications tierces
- Maintenance du location Appliance et du MSE
- Dépanner le location Appliance

5. Mise en œuvre et gestion d'un réseau maillé interne

- Réseau maillé interne
- Mettre en œuvre un réseau maillé
- Configurer les fonctionnalités avancées du réseau maillé
- Configurer le WCS pour un réseau maillé interne
- Dépanner un réseau maillé interne

6. Mise en œuvre et gestion du réseau maillé externe

- Réseau sans fil extérieur
- Routage mobile
- Réseau maillé externe



IAUWS: Implementing Advance Cisco Unified Wireless Security V1.0

Cette formation permettra aux participants de sécuriser les réseaux, de mettre en œuvre les standards de la sécurité et de configurer les composants.

Durée: 5 jours

Pré-requis: Posséder la certification CCNA Wireless

Objectifs :

Organiser et réguler les stratégies de sécurité

- Segmenter l'entreprise et rechercher le trafic WLAN
- Configurer l'administration et la sécurité sur les contrôleurs WLAN
- Configurer l'administration et la sécurité sur les contrôleurs WLAN à l'aide de TACACS+
- Sécuriser les périphériques clients à l'aide de l'authentification EAP
- Configurer le Client «Cisco Secure Services»
- Concevoir et mettre en œuvre le GUEST Wlan sur les contrôleurs WLAN
- Configurer le contrôleur WLAN pour Cisco NAC
- Configurer le serveur local d'authentification sur les contrôleurs WLAN
- Configurer la protection des trames de management MFP (Management Frame Protection) sur les contrôleurs WLAN
- Mettre en œuvre des ACL (Access Control List) sur les contrôleurs WLAN
- Configurer la détection d'intrusion (IDS) sur les contrôleurs WLAN
- Configurer le contrôleur WLAN pour intégrer les applicatifs IPS et IDS

Contenu :

1. Stratégies de sécurité organisationnelles et réglementation

- Conformité réglementaire
- Trafic segmenté
- Configurer la sécurité administrative
- Gérer les contrôleurs WLAN et les alarmes sur le Cisco WCS
- Outils d'audit de sécurité

2. Sécuriser les périphériques clients

- Configurer l'authentification EAP
- L'impact de la sécurité sur les applications
- Configurer le Client «Cisco Secure Services»
- Dépanner la connectivité sans fils

3. Conception et mise en œuvre des services d'accès «GUEST»

- Architecture "GUEST Access"
- Configurer le WLAN pour supporter le «Guest access»
- Configurer les comptes d'accès clients
- Dépanner le «Guest access»

4. Conception et intégration d'un réseau sans fil intégrant le NAC

- Solution Cisco NAC Appliance
- Configurer le contrôleur pour le Cisco NAC Out-of-Band

5. Mise en œuvre des services de connectivité sécurisés sans fils

- Configurer l'authentification pour l'infrastructure WLAN
- Configurer de protection des trames de management
- Configurer les services de certificats
- Mettre en œuvre les listes de contrôles d'accès
- Configurer l'IBNS sur les contrôleurs
- Dépanner la connectivité sécurisée sans fils

6. Réduction de la sécurité interne et intégrée

- Réduire les vulnérabilités du sans fils
- Utiliser l'IDS sur les contrôleurs
- Solutions de la sécurité Cisco end-to-end
- Intégrer le Cisco WCS avec l'IPS sans fils

Cursus Data Center



DCNI-1: Data Center Network Infrastructure -1

Ce cours aborde principalement les catalysts Cisco séries 6500 et 4900, certains aspects de la technologie de Cisco blade, mais cela ne sera pas le focus principal. Les modules du switch Catalyst 6500 sont inclus, ils couvriront FWSM et NAM. Ce cours est un cours d'implémentation, mais les stagiaires acquerront une vue d'ensemble sur l'évolution des data centers et les dernières nouveautés technologiques, leur permettant de positionner correctement les plateformes Cisco pour l'accès, l'agrégation et les couches principales du data center. L'objectif de ce cours est de permettre aux stagiaires de construire un réseau data center fiable et intelligent, en utilisant les switches Catalysts 6500 et 4900

Durée: 5 jours

Pré-requis: Avoir suivi les cours BSCI, BCMSN, ONT et ISCW ou posséder les connaissances équivalentes.

Objectifs : A l'issue de ce stage les stagiaires seront capables de:

- Déployer la solution Cisco Data Center
- Incorporer les switches Catalyst 6500 et 4900
- Identifier et mettre en œuvre le flux du trafic
- Mettre en œuvre la configuration initiale de NAM
- Utiliser NAM pour surveiller le trafic réseau
- Savoir décrire et déployer les fonctionnalités de haute disponibilité dans le Data Center

Contenu :

1. Mise en œuvre des Catalyst 6500, 4900 et Blade
2. Décrire l'architecture Data Center pour les Catalysts 6500 et 4900
3. Décrire et positionner les Catalysts 6500 et 4900
4. Décrire les superviseurs des Catalysts 6500
5. Décrire le module switch et les options Power Supply
6. Mettre en œuvre VSS 1440

- 7.** Mettre en œuvre NetFlow, QoS et EEM
- 8.** Mettre en œuvre SPAN, RSPAN et ERSPAN
- 9.** Décrire la famille de switch Cisco Blade
- 10.** Mise en œuvre du Module Service Firewall pour une infrastructure réseau Data Center
- 11.** Mettre en œuvre Le flux du trafic
- 12.** la gestion des accès
- 13.** le routage
- 14.** le Failover
- 15.** Deep Inspection Packet
- 16.** Mise en œuvre de l'analyse réseau avec NAM
- 17.** Présenter Cisco NAM
- 18.** Mettre en œuvre la configuration initiale
- 19.** Maintenance de NAM
- 20.** Mettre en œuvre les fonctionnalités de haute disponibilité de Data Center
- 21.** Mettre en oeuvre «Stateful Switchover» et «Nonstop forwarding»

Cursus Data Center



DCNI-2: Data Center Network Infrastructure -2

Durant ce cours, les stagiaires apprendront comment implémenter une infrastructure réseau data center avec les plateformes Nexus 7000 et 5000. Ce cours abordera en détail Nexus 7000 et donnera une vue d'ensemble de Nexus 5000 et de Fibre Channel over Ethernet (FCoE).

L'architecture de la plateforme Nexus et son déploiement seront abordés, ce qui inclut Virtual Device Contexts, les caractéristiques de Layer 2 et Layer 3, QoS et la sécurité. Les caractéristiques de NX-OS seront abordées avec des labs sur un simulateur Nexus 7000

Durée: 5 jours

Pré-requis: Il est recommandé aux stagiaires d'avoir suivi les cours :

- Interconnecting Cisco Network Devices Part 1 (ICND1)
- Interconnecting Cisco Network Devices Part 2 (ICND2)
- Building Scalable Cisco Internetworks (BSCI)
- Building Cisco Multilayer Switched Networks (BCMSN)
- Implementing Secure Converged Wide Area Networks (ISCW)
- Implementing Cisco IOS Network Security(IINS)

Objectifs : A l'issue de ce stage les stagiaires seront capables de:

- Décrire les fonctionnalités clés du châssis Nexus 7010
- Décrire les fonctionnalités Supervisor Engine et le module Line Card
- Décrire les fonctionnalités clés de Nexus 7010 power supplies et le système de ventilation
- Décrire le process de gestion de la connectivité
- Décrire l'architecture de base de NX-OS
- Expliquer le process de récupération NX-OS
- Expliquer le superviseur de redondance NX-OS
- Expliquer comment les fonctions Nexus 5000 dans des environnements SAN et LAN
- Décrire le protocole Fibre Channel sur Ethernet (FCoE)

Contenu :

1. Déploiement de Nexus 7000

- Vue d'ensemble de Nexus 7000
- Contextes virtuels dans Cisco Nexus 7000
- Nexus 7000 et protocoles NX-OS de la couche2 et fonctionnalités
- Nexus 7000 et protocoles NX-OS de la couche3 et fonctionnalités
- Nexus 7000 Fabric Switching
- Nexus 7000/NX-OS Qualité de service
- Nexus 7000/NX-OS Sécurité
- Dépannage

2. Vue d'ensemble de Nexus 5000

3. Vue d'ensemble de Nexus 5000

- Mettre en œuvre le réseau FCoE avec les switchs Nexus 5000
- Comprendre Fibre Channel
- Comprendre le protocole FCoE

Cursus Data Center



DCNID: Designing Cisco Data Center Network Infrastructures

Ce cours d'Architecture permettra aux participants d'appréhender la conception des réseaux Data Center incluant les équipements Nexus 5000, Nexus 7000, Catalysts 6500 et 4900, les switches Ethernet Blade et les modules FWSM (Module Firewall Services), NAM (Network Monitoring Module), Application ACE (Acceleration Control Engine), IPS (Cisco Intrusion Prevention System), ASA (Cisco Adaptive Security Appliance), SFS (Cisco Server Fabric Switch) et ONS (Cisco Optical Networking).

Les participants utiliseront différentes caractéristiques allant d'une opération en continue, de la capacité de résistance du processus, aux services de sécurité intégrés, et à la virtualisation, afin en œuvre des améliorations au niveau de l'efficacité et de la gestion du réseau.

Durée: 5 jours

Pré-requis:

- Recommandé: la certification CCDA ou CCDP et/ou avoir suivi le cours DESGN.
- Avoir des connaissances dans l'architecture réseau Cisco, les commutateurs et routeurs

Objectifs : A l'issue de ce stage les stagiaires seront capables de:

- Créer le «core layer design» pour optimiser le flux des données
- Créer une couche agrégation
- Créer une couche d'accès
- Optimiser un Data Center pour la Haute Disponibilité
- Concevoir la mise en œuvre à l'aide des modules Catalyst 6500
- Concevoir une infrastructure de gestion pour la gestion centralisée des services

Contenu :

1. Objectifs du Data Center

- Besoins pour un environnement Data Center
- Orientation de la conception d'un Data Center
- Critères de conception

2. Switch Cisco Nexus 7010

- Architecture matérielle et logicielle
- Disponibilité continue des Cisco Nexus 7010
- Gérer les commutateurs réseau
- Vue d'ensemble de la sécurité
- Mettre en œuvre la qualité de service (QoS)
- Positionnement des Nexus 7010 dans un réseau Data Center

3. Vue d'ensemble du système Nexus 5000

- Introduction au FCoE (Fibre Channel over Ethernet)
- Introduction au système Nexus 5000
- Vue d'ensemble du système Nexus 5000

4. Conception d'un Data Center

- Evolution de l'architecture
- Vue d'ensemble de la conception Data Center
- Evolution du modèle Data Center

5. Conception de l'architecture applicative Data Center

- Architecture applicative
- Impact des boîtiers/modules ACE
- Redondance Intra Data Center
- Redondance Inter Data Center
- Présentation générale GSLB
- Injection de route (RHI)

6. Stratégie Data Center

- Architecture réseau
- Technologie des commutateurs virtuels
- Entrées/Sorties unifiées
- Ethernet pour Data Center (DCE)
- Estimation de capacités du Data Center

7. Conception du réseau Data Center

- Conception des niveaux 2 et 3 dans la couche d'accès
- Couche d'accès: diagnostic de la topologie en triangle
- Couche d'accès: diagnostic de la topologie en carré
- Conception sans boucle
- Conception minimale de niveau 2
- Nouvelles topologies de Data Center
- Conception classique avec VSS, VRF et VDC
- Conception du routage
- Topologie améliorée de niveau 2
- Extensions de niveau 2 pour Interconnexion

Pour plus d'informations:

<http://www.microtel-net.com>

<http://www.microtel-net.com/index.php/formation/>

www.cisco.com/go/certification

Itinéraire à prendre pour arriver à l'institut:

<http://www.microtel-net.com/index.php/contact/>

Ou Nous contacter par Email:

formation@microtel-net.com

MCours.com