

Réseaux et Sécurité, Réseaux, état de l'art

Les synthèses Orsys en formation réseau vous présentent les derniers développements en matière d'architectures et de solutions : l'Internet du futur, les réseaux mobiles et sans-fil, le haut débit, le câblage, la voix et le multimédia sur IP, la qualité de service, les méthodes d'audit, de supervision et de sécurisation.

Séminaires

- [Réseaux, synthèse technique....](#) (p2)
- [Réseaux et Internet du futur....](#) (p5)
- [IP, technologies et services....](#) (p7)
- [Internet des objets, synthèse et perspectives....](#) (p9)
- [Sécurité VPN, sans-fil et mobilité....](#) (p12)
- [Sécurité réseaux/Internet, synthèse....](#) (p14)
- [Câblage informatique et nouveaux réseaux....](#) (p16)
- [Réseau de distribution en fibre optique, synthèse....](#) (p17)
- [Audit et analyse des réseaux....](#) (p18)
- [Réseaux, solutions d'administration....](#) (p20)
- [La QoS dans les réseaux IP, MPLS et Ethernet....](#) (p21)
- [Introduction aux télécommunications....](#) (p22)
- [Réseaux sans fil - Wi-Fi....](#) (p24)
- [Téléphonie sur IP, architectures et solutions....](#) (p28)

Stages Pratiques

- [La convergence des systèmes....](#) (p10)
- [Architecture Wi-Fi....](#) (p26)
- [Introduction aux réseaux mobiles....](#) (p30)
- [Evolution des réseaux mobiles....](#) (p31)
- [Réseaux mobiles, GSM, GPRS et EDGE....](#) (p32)
- [Réseaux mobiles, solutions 3G - UMTS....](#) (p33)
- [Réseaux mobiles, évolution de l'UMTS, 3G+, IMS....](#) (p35)
- [Réseaux mobiles, LTE/4G....](#) (p36)

Participants

Ce séminaire est destiné à tous ceux qui ont à développer des applications réparties et à mettre en oeuvre des réseaux locaux ou étendus. Il constituera aussi une aide précieuse pour tous ceux qui travaillent déjà dans le domaine des réseaux et qui souhaitent avoir une vue synthétique et précise.

Pré-requis

Aucune connaissance particulière.

Prix 2012 : 2430€ HT

Eligible DIF

Dates des sessions

Paris

5 juin 2012, 18 sep. 2012
27 nov. 2012

Réseaux, synthèse technique

OBJECTIFS

Ce séminaire vous apportera des connaissances solides, précises et synthétiques dans le domaine des réseaux. Il fait le point sur les derniers développements en matière d'architecture de réseaux, leurs évolutions vers les hauts débits et le sans-fil, les méthodes de gestion et de sécurisation. Il analyse notamment les conséquences de l'apparition de nouvelles applications, notamment Internet, sur l'architecture des systèmes de communication de l'entreprise.

[1\) Les grandes solutions](#)

[2\) Les architectures de réseaux](#)

[3\) Le réseau d'accès](#)

[4\) Réseaux de mobiles et réseaux sans fil](#)

[5\) Les réseaux d'entreprise](#)

[6\) Les réseaux d'opérateurs](#)

[7\) Les environnements IP](#)

[8\) Multimédia, voix et image sur IP](#)

[9\) Gestion, sécurité](#)

[10\) Les choix stratégiques pour le futur](#)

Intervernants

Serge FDIDA

Professeur à l'université Pierre et Marie Curie, il dirige le thème Réseau et Performances du laboratoire LIP6-CNRS. Il anime depuis plusieurs années des travaux sur les réseaux haute vitesse multimédia et l'Internet du futur. Il est conseiller scientifique et animateur de plusieurs projets et manifestations scientifiques au niveau national et international. Il est également le directeur du laboratoire commun recherche-industrie " Euronetlab ".

Eric HORLAIT

Professeur à l'université Pierre et Marie Curie, il dirige le laboratoire LIP6. Ses principaux centres d'intérêt sont le contrôle et la gestion politique des réseaux, la mise en place de systèmes à hauts débits, la conception d'applications multimédias coopératives distribuées, l'évolution de l'Internet et des autoroutes de l'information. Il assure depuis maintenant plus de dix ans la responsabilité de nombreux projets industriels et académiques. Il est cofondateur de la société QosMOS, spécialisée dans la mise en place de solutions de contrôle des réseaux IP.

1) Les grandes solutions

- Informatique, télécom et câblo-opérateur.
- Les réseaux d'accès et les réseaux de coeur.
- La convergence vers le tout IP.

2) Les architectures de réseaux

Les architectures de niveau physique

- SONET et SDH. Techniques WDM et du DWDM.

Les architectures de niveau trame

- La montée d'ethernet. Architecture ATM. Exploitation. QoS. Trame PPP. Commutation. Label switching.

Les architectures de niveau paquet

- Les architectures IP. Les routeurs et les fonctions de niveau 3. Les contrôles et la signalisation IP.

Les architectures de niveau trame/paquet

- Label Switching. Norme MPLS. Les extensions GMPLS.

3) Le réseau d'accès

La boucle locale résidentielle

- Vers le haut débit. La boucle locale optique. EPON.
- Les solutions câblo-opérateurs. Le xDSL.
- La boucle locale ou radio. WiFi et WiMax. La 3G.

La boucle locale des entreprises

- Evolutions. Coût de connexion. Fibre optique.
- La parole (VoDSL) et la télévision (TVoDSL).
- Les nouvelles générations de Box d'accès.

4) Réseaux de mobiles et réseaux sans fil

Les réseaux de mobiles

- Typologies : WPAN, WLAN, WMAN, WRAN. Hot-spot, handover, roaming. Le GPRS. EDGE. La 3G : UMTS, W-CDMA et dérivées HSDPA, HSUPA. La 4G.

Technologies des réseaux sans fil

- L'IEEE 802.15 et les WPAN. Bluetooth, ZigBee et UWB.
- Les nouveaux produits.

- L'IEEE 802.11 (a/b/e/g/n). QoS. Sécurité.
- L'IEEE 802.16 et les produits WiMAX, les attentes.
- L'IEEE 802.22 et futurs produits Wi-RAN.
- La radio cognitive. L'Internet ambiant. L'IP mobile.

5) Les réseaux d'entreprise

Technologie des réseaux locaux

- Architecture : réseaux capillaires et coeur de réseau.
- Câblage. Les supports et les topologies.

Normalisation et évolutions des réseaux locaux

- Historique des techniques d'accès : ISO 8802.3 (CSMA/CD), ISO 8802.5 (jeton sur boucle).
- La normalisation. IEE 802 et ISO. Les couches physiques, MAC, et LLC. Les principaux protocoles.

Les réseaux locaux Ethernet

- De l'Ethernet 10Base5 au 10GigEther.
- Les protocoles de la famille 802, la QoS.
- Evolutions d'Ethernet : réseaux d'opérateurs (802.17), boucle locale, SAN...
- Ingénierie de trafic d'un réseau Ethernet.

Les interconnexions

- Commutateur de niveaux 3, 4 et de contenu.
- Commutation vs routage. Spanning tree. Routage IP intra et inter-domaine. commutation de labels.
- Les réseaux Overlays, CDN et P2P.

Les réseaux privés virtuels

- Filtrage de l'information. La sécurité et la gestion.
- Les environnements VPN-IP- IPsec et VPN-IP-MPLS.

6) Les réseaux d'opérateurs

- Fonctionnalités : QoS, contrôle, gestion. Signalisation.
- La facture télécom et postes à contrôler.
- L'Intégration Voix/Données/Vidéo. l'interconnexion.
- VPN. L'explosion de l'Internet.
- VPN IP, VPN IPSEC, Virtual Private LAN Service.
- Le relais de trames et l'ATM : solutions.
- Intégration Voix/données. Support QoS et multimédia.
- Architecture MPLS. QoS. MPLS-DiffServ ; les VPN-MPLS. Comparaison avec une architecture IP native.
- La technologie policy-based networking. Les politiques, le policy repository, le PDP et les PEP. Le protocole COPS, les SLA, les PIB.

7) Les environnements IP

- Principes fondateurs : L'interconnexion. TCP/IP et UDP/IP.
- Adressage public et privé. Le NAT. Le DNS. Les annuaires.
- Protocole IPv4, IPv6. ICMP. Transport : TCP, ODP, RTP.
- QoS Diff-Serv, Int-Serv, RSVP. Le protocole RSVP.
- Multicast IP. Situation, normalisation, utilisation.
- La gestion de réseaux IP. L'approche SNMP.
- Intranet : structure QoS, VPN IP, Sécurité.
- Les applicatifs : FTP, messagerie, Web, ToIP, vidéo...

8) Multimédia, voix et image sur IP

- Gestion de la voix : du codage au transport. QoS. Réserve de ressources, adaptation des applications (RTP/RTCP), services différenciés (Diff-Serv).
- Vidéo sur IP, vidéo à la demande (VoD) et télévision sur IP (IPTV). Codage, compression, performance.
- Peer-to-Peer, réseaux CDN et "Overlays".

9) Gestion, sécurité

La gestion dans les réseaux

- Le modèle proposé par l'ISO.
- SNMP : fonctionnalités, proxies, MIB. Versions 2 et 3.
- La configuration automatique (RARP, DHCP).
- Mesures de performance et Shaping. Positionnement.

La sécurité

- Problèmes. Attaques : Virus, Worms, DDOS. Solutions : firewall, authentification (MD5, RSA), cryptage (DES, IDEA), signature électronique...
- Les annuaires pour la sécurité. Le modèle LDAP.
- Le modèle IPSEC. Les services, la mise en oeuvre.

10) Les choix stratégiques pour le futur

- L'Internet du futur. Evolution de la boucle locale. Les mobiles et leurs évolutions. Réseaux sociaux et de personnes. Réseaux intelligents. Réseaux " autonomic ". Virtualisation de réseaux.

Séminaire de 3 jour(s)
Réf : RNG

Participants

Ce séminaire s'adresse aux responsables réseaux, responsables études, ingénieurs système qui ont à conduire l'évolution de leurs réseaux.

Pré-requis

Connaissances de base dans le domaine des réseaux.

Prix 2012 : 2430€ HT

Eligible DIF

Dates des sessions

Paris

12 juin 2012, 25 sep. 2012
4 déc. 2012

Réseaux et Internet du futur

OBJECTIFS

Ce séminaire vous présentera un état des avancées les plus récentes dans le domaine des réseaux et des télécommunications, les technologies émergentes et leur intégration dans les environnements actuels. Les différentes solutions seront explicitées sous l'angle technologique et économique. Ce séminaire s'adresse aux architectes et ingénieurs de réseaux ainsi qu'aux responsables informatiques qui disposent déjà de très solides connaissances dans le domaine des réseaux.

1) Internet et la nouvelle génération

2) La mobilité dans les réseaux

3) Prospective pour l'Internet mobile

4) Evolution des technologies d'acheminement dans les réseaux

5) La maîtrise de la qualité de service (QoS)

6) Les technologies des réseaux

d'acheminement et leurs évolutions

7) Boucle locale

8) Les réseaux sans fil

9) La voix sur IP

10) La sécurité

11) Prospective pour l'Internet du futur

1) Internet et la nouvelle génération

- La société de l'Internet. Standardisation.
- Les fonctions essentielles d'IP : adressage, routage (BGP, RIP, OSPF) ... Problèmes et solutions apportées.
- Réseaux privés/réseaux publics : NAT/PAT. L'IPv6.
- Le transport dans TCP/IP : UDP, TCP.

2) La mobilité dans les réseaux

- La première génération des réseaux mobiles.
- GSM et ses révolutions. Le mode paquet dans GSM : GPRS/EDGE. Routage dans les réseaux GPRS.
- 3G : UMTS, CDMA2000 : architecture, débits, applications. Evolutions de la 3G (3G+) : HSDPA, HSUPA, HSOPA, MIMO.
- Futures générations : débits, caractéristiques (LTE et UMB).
- La mobilité intertechnologies : Handover vertical et radio cognitive.
- Le rôle d'IP mobile dans une architecture hétérogène.

3) Prospective pour l'Internet mobile

- La mobilité, UMTS, 4G et routeurs radio.
- Distribution de contenus. Signalisation. Contrôle.
- Qualité de service sur réseau fixe et mobile.

4) Evolution des technologies d'acheminement dans les réseaux

- Commutation : très haut débit, label et contenus.
- Routage par contenu et routage XML.
- Les overlays, distributions de contenus et P2P.
- Les architectures orientées services.

5) La maîtrise de la qualité de service (QoS)

- Invariants de la QoS : de la conception aux algorithmes.
- Ingénierie du trafic. Calcul de bornes de bout en bout.
- Contrôle d'admission. Ordonnement.
- Gestion de files d'attente : RED, RIO.
- Projection des résultats dans diverses technologies.
- La classification applicative. La solution RTP/RTCP.

6) Les technologies des réseaux d'acheminement et leurs évolutions

L'ATM, le mythe du réseau universel

- L'ATM dans les réseaux des ISP et des opérateurs.
- Catégories de service et contrôle de flux.

Ethernet pour tout faire !

- Du 10 Mbit/s au 10 Gbit/s.
- Du réseau local au réseau grande distance. Le 802.17. Ethernet First Mile pour l'accès Fibre.

IP nouvelle génération

- IPv4 et IPv6. Les avantages d'IPv6 pour le haut débit et le multimédia. La QoS dans un réseau IP.
- Le routage IP multicast. Les modèles INTSERV et DIFFSERV. La signalisation et RSVP.
- Les classes de service : EF, AF et BE.
- DIFFSERV et MPLS. DIFFSERV et INTSERV.

MPLS et la nouvelle génération Internet Télécom

- Commutation de label. Origines et motivations.
- Protocoles LDP, CR-LDP, RSVP-TE. Génération G-MPLS.
- Comparaison MPLS et IP natif. Déploiements et acteurs.

7) Boucle locale

- Les solutions fibres optiques (FTTC, FTTH).
- Les solutions câble coaxial. Modems câbles.
- Les solutions paires torsadées métalliques. Modems ADSL. Débits. Autres options xDSL. DSLAM.
- L'intégration : le triple-play et le quadruple-play.
- Le réseau de domicile : l'utilisation du Wi-Fi et du CPL (Courant Porteur en Ligne). Architectures.

8) Les réseaux sans fil

Les WPAN

- Nouvelle génération et normes IEEE 802.15.
- UWB (Ultra Wide band) et les très hauts débits.
- Bluetooth 3.0, produits WUSB et WINET. ZigBee.

Les WLAN

- L'environnement Wi-Fi avec les IEEE 802.11a/b/g/n.
- Handovers, qualité de service et sécurité.
- Fast handover et mesh networks.

Les WMAN

- Réseaux métropolitains et IEEE 802.16. WDSL. ADSL Mobile et IEEE 802.16e. WiMAX.

Les WRAN

- Les communications sans fil régionales dans les bandes vidéo de télévision et l'IEEE 802.22. Les antennes intelligentes et la radio cognitive.

L'intégration des solutions Wi-xx

- L'intégration des réseaux sans fil avec l'IEEE 802.21.
- La compétition avec la 4G.

9) La voix sur IP

Convergence

- Transmission voix sur IP, ToIP et VoIP.
- Le passage au tout IP pour la téléphonie.
- Standardisation. Industriels impliqués.

H323 : transposition de la téléphonie classique

- Architecture et mise en place d'une signalisation compatible avec celle de la téléphonie classique.

L'approche SIP ou la définition de services ouverts

- Un système de signalisation ouverte pour construire des services. Produits. Consortium SIP Forum. Intégration dans les systèmes de téléphonie mobile 3G.
- Architectures comparées de SIP et H323.

MGCP et les Gatekeeper

- Interconnexion d'équipements de ToIP et de téléphonie classique. Intégration de services hétérogènes.

10) La sécurité

- Le modèle de sécurité de l'Internet est-il encore viable ? Authentification, RADIUS et IEEE 802.1x. Chiffrement et signature électronique.
- La classification des flux à des fins de sécurité.
- La nouvelle génération de firewall. Les cartes à puces.
- La distribution de certificats (PKI).

11) Prospective pour l'Internet du futur

- Réseaux autonomic. Pilotage de réseaux. Intelligence dans les réseaux. Virtualisation. Le Post-IP.

Séminaire de 3 jour(s)
Réf : IPS

Participants

Ce séminaire s'adresse aux responsables réseaux, responsables études, ingénieurs système qui ont à développer et à mettre en place des systèmes d'information et de communications.

Pré-requis

Connaissances de base dans le domaine des réseaux.

Prix 2012 : 2430€ HT

Eligible DIF

Dates des sessions

Paris

13 juin 2012, 25 sep. 2012
4 déc. 2012

IP, technologies et services

OBJECTIFS

Une présentation complète des technologies IP, des concepts fondamentaux et des évolutions majeures. Ce séminaire analyse des aspects aussi essentiels que la gestion de la qualité de service, les réseaux sans fil et la mobilité, la sécurité, les technologies haut débit, les interfaces avec les autres architectures et la migration vers IPv6.

1) Les technologies IP

2) IPv4... comment passer à IPv6 ?

3) Le routage

4) Les réseaux sans fil, IP et la mobilité

5) La technologie MPLS

6) La qualité de service dans les réseaux IP

7) La téléphonie sur IP

8) Gestion de réseaux, administration

9) La sécurité

1) Les technologies IP

- L'interconnexion de réseaux.
- Les protocoles de base.
- Internet et les réseaux d'opérateurs.
- Le multicast IP.
- Des exemples d'applications du monde IP.
- Le multimédia et les hauts débits.

2) IPv4... comment passer à IPv6 ?

- Limites de IPv4.
- IPv6, les fondements techniques. La mobilité.
- De IPv4 à IPv6. Stratégies de migration.

3) Le routage

- Structure du routage.
- Protocoles de routage.

4) Les réseaux sans fil, IP et la mobilité

- Impact du sans fil sur IP.
- Le Wi-Fi et le Wimax.
- IP dans les réseaux GPRS/UMTS. IP pour réseaux PLMN.
- IP, UMTS et WLAN.

5) La technologie MPLS

- Principes de la commutation de labels. Les solutions. Terminologie et architecture MPLS. Distribution de labels, LDP, CR-LDP, RSVP-TE, OSPF-TE, MBGP...
- L'ingénierie de trafic. L'apport de MPLS.

6) La qualité de service dans les réseaux IP

- Les bases.
- Le modèle INTSERV.
- Le modèle DIFFSERV.
- Le niveau applicatif.

7) La téléphonie sur IP

- Architecture H323.
- Architecture SIP.
- Transport de la voix et de la vidéo sur IP, RTP.

8) Gestion de réseaux, administration

- Configuration et administration.
- Gestion, approche SNMP.

9) La sécurité

- Les concepts et considérations. Les réseaux de vigilance : FIRST, CERT.
- Quelques solutions. La mise en place d'une protection d'accès : firewall (pare-feu). La sécurité applicative. Les solutions de détection d'intrusion.
- Le modèle IPSec. La standardisation. Les modes transport et tunnel. Les produits compatibles IP Sec.
- Les réseaux privés virtuels IP. L'architecture. La mise en œuvre. Offre des opérateurs. Les solutions VPN IPSec.

- La sécurité des réseaux sans fil. WEP, WPA. Filtrage d'adresses.

Séminaire de 2 jour(s)
Réf : IDO

Participants

Ce séminaire s'adresse aux responsables réseaux, responsables études, décideurs et entrepreneurs dans le domaine du futur service de l'Internet.

Pré-requis

Connaissances de base sur les réseaux (TCP/IP).

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

4 oct. 2012, 6 déc. 2012

Internet des objets, synthèse et perspectives

OBJECTIFS

Ce séminaire est un état de l'art du domaine émergent de l'Internet des objets qui permet de proposer de nouveaux services dans de nombreux secteurs comme l'aide à la personne, la surveillance, la traçabilité, l'automatisation des chaînes de production, etc. A l'issue, vous aurez acquis les connaissances essentielles à la mise en oeuvre de tels services.

1) Introduction, technologies d'objets et de communication

3) Internet du Futur

2) Mise en réseau dans l'Internet des Objets

Démonstration

Durant le séminaire, une démonstration illustrera un exemple pratique d'application à base de RFID. Mise en place du kit " Touch a Tag " pour concevoir une application simple avec déclenchement d'un service, basée sur la lecture RFID.

1) Introduction, technologies d'objets et de communication

- L'Internet des objets. Le modèle, les principes.
- Limites du modèle IP et éléments de sécurité, qualité de service et mobilité.
- La convergence IP : du fixe vers le Mobile, IMS et l'approche orientée Service.
- Nouvelles fonctionnalités de l'Internet des objets. Identification. Capture. Inférence et décision. Déclenchement à distance. Autres.
- Concept de terminal et d'objet. Architecture Microcontrôleur : Microchip, Systèmes numériques. Objet RFID et capteur. Terminal mono-interface, multi-interface/multimode.
- Technologie de communication, l'Internet des objets.
- Technologie CPL (Courant porteur en ligne), réseaux sans fil : Wifi, Bluetooth, ZigBee, HomeRF, RFID, NFC..
- Communications mobiles : GPRS, EDGE, 3G, HSPA, vers LTE.
- Communications radio de courte portée : UWB, NFC.
- Interaction entre les technologies hétérogènes.
- Panorama des autres technologies de l'Internet des objets : Nanotechnologie. Robotique. Autres.
- Technologies d'interconnexion : par passerelle, de bout en bout.
- Domaines d'application et nouveaux services : surveillance et monitoring (écologie, aide à la personne). Automatisation de processus : autour de la personne (à domicile, au bureau, en déplacement), entreprise, industrie (automatisation des chaînes de production), santé (automatisation de dossiers de malades).

2) Mise en réseau dans l'Internet des Objets

- Modèle IP et la consommation d'énergie.
- Architecture nano-IP et architecture 6LowPan.
- Routage : ROLL. Compression IP. Techniques de Nommage et identification d'objets. Object Name Service (ONS).
- Architecture d'accès aux services de l'Internet des Objets.
- Contraintes réseau : passage à l'échelle du routage, passage à l'échelle de l'identification et l'adressage, mobilité transparente au réseau. Etude de cas : traçabilité d'objets RFID à travers le réseau IP.
- Géolocalisation en intérieur et en extérieur. Tracking d'objets. Traçabilité.
- Exemple de services réseaux de l'Internet des objets. Paiement bancaire en mobile et NFC. Système de surveillance. Touch a Tag. Location based services.
- Exemple de plateforme réseaux : Senslab, Winlab.
- Pour aller plus loin. Sécurité et Vie privée dans l'Internet des Objets. La gouvernance de l'Internet. Interopérabilité et standardisation.

3) Internet du Futur

- Limitation du modèle IP. Consommation énergie. Manque d'adaptation.
- Nouveaux besoins. Nouveaux services.
- Nouvelles approches : approche intercouche, de communication autonome " Autonomic communication ", de Virtualisation réseau, de " Cloud Computing ", etc.
- Gouvernance IP. Introduction. Définitions et principes.
- Projets industriels et de recherche en cours : FIND/GENI, Planetlab/Onelab, Orbit/Winlab, FIT/FITING, autres...

Stage pratique de 1 jour(s)
Réf : CDS

Participants

Responsables réseaux,
responsables études,
responsables SI, chefs de
projets, architectes réseaux,
ingénieurs systèmes et
réseaux.

Pré-requis

Bonnes connaissances dans
le domaine des réseaux.

Prix 2012 : 890€ HT

Eligible DIF

Dates des sessions

Paris

11 juin 2012, 17 sep. 2012
19 nov. 2012

Lyon

19 sep. 2012

La convergence des systèmes

OBJECTIFS

Cette formation vous présentera les stratégies de la convergence des réseaux fixes et des réseaux mobiles. Vous verrez également les apports des communications optiques et filaires en termes de convergence ainsi que les interactions entre réseaux existants et évolutions futures.

1) La convergence et l'intégration dans Internet

2) La convergence fixe mobile

3) La convergence des réseaux coeur

4) La convergence des réseaux d'accès

5) La convergence du réseau de domicile

1) La convergence et l'intégration dans Internet

- La convergence IP : les enjeux et les difficultés.
- La convergence fixe mobile et celle des terminaux.
- Les convergences en matière de réseaux IP.
- Les réseaux en jeux : réseau coeur, réseaux d'accès, réseaux de domicile.

2) La convergence fixe mobile

L'IMS

- L'architecture de l'IMS. Le groupe de travail TISPAN.
- Les offres des opérateurs en matière d'IMS.

L'introduction d'IP dans la gestion de la mobilité

- La solution IP mobile : avantages et inconvénients.
- IP cellulaire et la micromobilité.
- Comparaison avec la mobilité des réseaux cellulaires.

La convergence interne aux réseaux de mobiles

- L'UMA (Unlicensed Mobile Access).
- Les intégrations fixe-mobile.
- L'intégration dans les réseaux 4G.

3) La convergence des réseaux coeur

Les technologies de convergence

- Les réseaux MPLS et GMPLS.
- Les solutions pour la convergence.
- Le Metro Ethernet Forum (MEF).

Les techniques optiques

- Les réseaux optiques.
- GMPLS et l'intégration de l'optique.
- Les signalisations IP.
- Les contrôles OSPF-TE, RSVP-TE.

Le NGN (Next Generation Network)

- Le protocole de base : SIP (Session Initiation Protocol).
- La convergence vers le tout Ethernet-IP.

4) La convergence des réseaux d'accès

Les réseaux d'accès terrestre

- Les solutions xDSL : le passage au tout Ethernet.
- Les solutions optiques : les différents types de câblage.
- Les PON ; APON, EPON et GPON.

Les réseaux d'accès sans fil

- Les solutions IEEE et Wi-Fi.
- Le WDSL et WiMAX.
- Les solutions Femto cell.

Les réseaux d'accès pour les mobiles

- Les solutions 2G, 3G et 4G.
- Le réseau d'accès aux Node B et E-Node B.

5) La convergence du réseau de domicile

Les solutions multiplay

- Le triple play et la convergence IP.
- Le quadruple play et la convergence de la mobilité.

- Les Internet-box.

Les normes pour la convergence

- Le standard DLNA (Digital Living Network Alliance).
- UPnP (Universal Plug & Play).

Le réseau de domicile

- Le réseau de domicile : CPL ? Wi-Fi.
- L'intégration du fixe et du mobile.

Perspectives et conclusion

- La place de la TNT. Le rôle de la virtualisation.

Séminaire de 2 jour(s)
Réf : VPN

Participants

DSI, RSSI, Responsables sécurité, chefs de projets, consultants, administrateurs, cadres utilisateurs de portables, Smartphones ou d'un accès VPN.

Pré-requis

Des connaissances de base sur l'informatique sont nécessaires.

Prix 2012 : 1690€ HT

Eligible DIF

Dates des sessions

Paris

21 28 juin 2012, 11 oct. 2012
13 déc. 2012

Sécurité VPN, sans-fil et mobilité, synthèse

OBJECTIFS

Aujourd'hui, le réseau Internet, les technologies de communication sans fil (Wi-fi, Bluetooth) et les terminaux mobiles (notebook, Smartphone) facilitent grandement l'accès aux applications de l'entreprise. Mais qu'en est-il réellement de la sécurité de ces accès ? Ce séminaire dresse le panorama complet des menaces et vulnérabilités et apporte des solutions concrètes pour s'en prémunir.

1) Menaces et vulnérabilités

2) Les attaques sur l'utilisateur

3) Les attaques sur les postes clients

4) Sécurité des réseaux privés virtuels (VPN)

5) Sécurité des réseaux sans-fil

6) Sécurité des Smartphones

Exemple

Approche théorique et pratique avec démonstration, avantages et inconvénients des solutions, retours d'expérience.

1) Menaces et vulnérabilités

- Evolution de la cybercriminalité en France.
- Statistiques et évolution des attaques.
- Evaluation des risques dans un contexte de mobilité.

2) Les attaques sur l'utilisateur

Attaques ciblées sur l'utilisateur

- Les techniques d'attaques orientées utilisateur.
- Les techniques de Social engineering.
- Codes malveillants et réseaux sociaux.
- Les dangers spécifiques du Web 2.0.
- Attaque sur les mots de passe.
- Attaque "Man in the Middle".

3) Les attaques sur les postes clients

- Risques spécifiques des postes clients (ver, virus...).
- Le navigateur le plus sûr.
- Rootkit navigateur et poste utilisateur.
- Quelle est l'efficacité réelle des logiciels antivirus ?
- Les risques associés aux périphériques amovibles.
- Le rôle du firewall personnel.
- Sécurité des clés USB.
- Les postes clients et la virtualisation.
- Les principales lacunes sécuritaires des OS clients.
- Amélioration de la sécurité dans Windows.

4) Sécurité des réseaux privés virtuels (VPN)

Les techniques de tunneling

- Accès distants via Internet : panorama de l'offre.
- Les protocoles PPT, LTP, L2F pour les VPN.
- Le standard IPsec et les protocoles AH, ESP, IKE.
- Les solutions de VPN pour les accès 3G.
- Quelles solutions pour Blackberry, iPhone... ?
- VPN SSL : la technologie et ses limites.
- Le panorama de l'offre VPN SSL. Critères de choix.
- IPsec ou VPN SSL : quel choix pour le poste nomade ?
- Le VPN avec DirectAccess sous Windows 7.

5) Sécurité des réseaux sans-fil

- La sécurité des Access Point (SSID, filtrage MAC...)
- Pourquoi le WEP est dangereux ? Qu'apportent WPA, WPA2 et la norme 802.11i ?
- L'authentification dans les réseaux Wi-fi d'entreprise.
- Technologies VPN (IPsec) pour les réseaux Wi-fi.
- Comment est assurée la sécurité d'un hotspot Wi-fi ?
- Les techniques d'attaques sur WPA et WPA2.
- Les fausses bornes (Rogue AP).
- Attaques spécifiques sur Bluetooth.
- Les principales attaques : Bluebug, BlueSmack, BlueStack...

6) Sécurité des Smartphones

- La sécurité sur les mobiles (Edge, 3G, 3G+...).
- Les risques spécifiques des Smartphones.
- Failles de sécurité : le palmarès par plateforme.
- Virus et code malveillants : quel est le risque réel ?
- Protéger ses données en cas de perte ou de vol.

Démonstration

Mise en oeuvre d'un accès Wi-fi fortement sécurisé avec IPsec et EAP-TLS. Attaque de type " Man in the Middle " sur une application Web en HTTPS via un Smartphone (sslsnif et sslstrip). Accès au SI en VPN SSL avec authentification forte. Protection des données par le chiffrement (EFS, Bitlocker et Bitlocker to go).

Séminaire de 3 jour(s)
Réf : SRI

Participants

Responsables sécurité, développeurs, concepteurs, chefs de projets intégrant des contraintes de sécurité, responsables ou administrateurs réseau, informatique, système.

Pré-requis

Bonnes connaissances des réseaux et des systèmes.

Prix 2012 : 2430€ HT

Eligible DIF

Dates des sessions

Paris

4 19 juin 2012, 25 sep. 2012
27 nov. 2012

Rennes

11 juin 2012

Sécurité réseaux/Internet, synthèse

OBJECTIFS

Ce séminaire vous montrera comment répondre aux impératifs de sécurité des communications de l'entreprise et intégrer la sécurité dans l'architecture d'un système d'information. Il comprend une analyse détaillée des menaces et des moyens d'intrusion ainsi que des techniques spécifiques de sécurité, solutions et produits. A l'issue de ce séminaire, vous disposerez des éléments techniques pour comprendre les technologies qui protègent votre système d'information et sécurisent son ouverture aux réseaux extérieurs Internet, Extranet et VPN.

1) Introduction : qui fait quoi et comment ?

2) Outils et méthodes d'intrusion par TCP-IP

3) Sécurité des postes clients

4) Sécurité du sans-fil (Wi-fi et Bluetooth)

5) Technologie firewall/proxy

6) Techniques cryptographiques

7) Sécurité pour l'Intranet/Extranet

8) Réseaux Privés Virtuels (VPN)

9) Sécurité des applications

10) Gestion et supervision active de la sécurité

Intervernants

Pascal GOUACHE

Consultant, chef de projet, spécialisé dans la sécurité des réseaux et des systèmes d'information. Il dirige des projets de sécurité active et de qualité de service pour des grandes entreprises mettant en oeuvre des technologies de type firewall réseau et applicatif, proxy, authentification, PKI, haute disponibilité et VPN. Il est spécialisé dans la protection, la disponibilité et l'amélioration des performances des services en ligne.

Boris MOTYLEWSKI

Fondateur et directeur technique de la société ExperLAN (Sécurité des réseaux IP) devenue aujourd'hui Thales Security Solutions. Fondateur de la société Axiliance, il conçoit le firewall RealSentry et dirige la R&D de 2001 à 2005. Avec plus de 10 ans d'expertise dans la sécurité, Boris Motylewski est un des meilleurs experts français en sécurité informatique.

1) Introduction : qui fait quoi et comment ?

- Concepts : risque, menaces, vulnérabilité...
- Evolution de la cybercriminalité.
- Nouveaux usages (Web 2.0, virtualisation, Cloud Computing...) et risques associés.
- Nouvelles techniques d'attaque et contre-mesures.

2) Outils et méthodes d'intrusion par TCP-IP

- Les attaques par le stack IP.
- Les attaques applicatives (DNS, HTTP, SMTP, etc.).
- Utilisation d'un code mobile malveillant.
- Comprendre les techniques des hackers.
- Les sites (CERT, Security focus/bugtraq, CVE...).

3) Sécurité des postes clients

- Les menaces : backdoor, virus, spyware, rootkit...
- Le rôle du firewall personnel et ses limites.
- Les logiciels anti-virus/anti-spyware : comparatif.
- Linux et Open Office vs Windows et MS Office ?
- Les attaques par les documents PDF.
- Comment sécuriser les périphériques amovibles.
- Contrôle de conformité de Cisco NAC, MS NAP.
- La sécurité intégrée dans Windows 7 (AppLocker, BitLocker, UAC, DirectAccess...).

4) Sécurité du sans-fil (Wi-fi et Bluetooth)

- Technologies de réseaux sans fil (standards 802.11).
- Attaques spécifiques (Wardriving, failles WEP et EAP).
- Sécurité des bornes (SSID, Filtrage MAC).
- Vulnérabilités WEP. Faiblesse de l'algorithme RC4.
- Le standard de sécurité IEEE 802.11i (WPA et WPA2).
- Authentification des utilisateurs (EAP, certificats, token...).
- Les différentes méthodes Cisco LEAP, EAP-TLS, PEAP...
- Attaque sur les hotspots Wi-fi (Rogue AP).
- Attaques spécifiques sur Bluetooth (Bluebug...)
- Comment se protéger efficacement contre les attaques ?
- Audit et surveillance du réseau. Outils d'audit.

5) Technologie firewall/proxy

- Serveurs proxy, reverse proxy, masquage d'adresse.

- Filtrage. Firewall et proxy : quelle complémentarité ?
- Principe des firewalls, périmètre fonctionnel.
- La mise en place de solutions DMZ.
- Sécurité liée à l'adressage.
- Evolution de l'offre Firewall (appliance, VPN, IPS, UTM...).
- Notion de " dé-périmétrisation " du forum Jericho.
- Utilisation des firewalls dans la protection des environnements virtuels.

6) Techniques cryptographiques

- Terminologie, principaux algorithmes. Législation et contraintes d'utilisation en France et dans le monde.
- Algorithmes à clé publique : Diffie Hellman, RSA...
- Scellement et signature électronique : MD5, MAC...
- Mots de passe, token, carte à puce, certificats ou biométrie ?
- Authentification forte : logiciels (S/key), cartes à puces, caulettes d'authentification.
- Sécurisation des clés de chiffrement (PFS, TPM...).
- Evaluation des systèmes d'authentification : Radius, Tacacs+, Kerberos, X509.
- Compléter l'authentification par l'intégrité et la confidentialité de vos données.

7) Sécurité pour l'Intranet/Extranet

- Les architectures à clés publiques.
- Les attaques sur SSL/TLS (sslstrip, sslnif...).
- Un serveur de certificat interne ou public ? En France ou aux USA ? A quel prix ? Comment obtenir des certificats ? Comment les faire gérer ?
- Les risques liés aux certificats X509. L'apport des certificats X509 EV.
- Annuaire LDAP et sécurité.
- Architectures "3A" (authentification, autorisation, audit) : SSO, Kerberos, OSF/DCE et ECMA Tacacs.

8) Réseaux Privés Virtuels (VPN)

- Analyse du besoin, conception et déploiement.
- La création d'un VPN site à site via Internet.
- IPSec. Les modes AH et ESP, IKE et la gestion des clés.
- Les produits compatibles IPSec, l'interopérabilité.
- Surmonter les problèmes entre IPSec et NAT.
- Les VPN SSL (quel intérêt par rapport à IPSec ?).
- Les produits VPN SSL, l'enjeu de la portabilité.
- Le VPN avec DirectAccess sous Windows 7.
- Les offres VPN Opérateurs. VPN IPSec ou VPN MPLS ?

9) Sécurité des applications

- Les principales techniques d'attaque des applications (buffer overflow, XSS, SQL Injection, vol de session...).
- Le processus SDL (Security Development Lifecycle).
- Utilisation de la technique de " fuzzing ".
- Les outils de revue de code orientés sécurité.
- Le Firewall applicatif (WAF).
- Solution WAF Open source avec Apache en reverse proxy et mod_security.
- Les critères d'évaluation d'un WAF selon le Web Application Security Consortium (WASC).
- Le hardening et la vérification d'intégrité temps réel.

10) Gestion et supervision active de la sécurité

- L'apport des normes ISO 27001 et ISO 27002.
- Les tableaux de bord Sécurité. La norme ISO 27004.
- Les missions du RSSI dans le suivi de la sécurité.
- Les audits de sécurité (techniques ou organisationnels).
- Les tests de vulnérabilité ou tests d'intrusion.
- Les outils Sondes IDS, Scanner VDS, Firewall IPS.
- Consigner les preuves et riposter efficacement.
- Mettre en place une solution de SIM.
- Se tenir informé des nouvelles vulnérabilités.
- Gérer les mises à niveaux.
- Savoir réagir en cas d'incidents.
- Les services indispensables : où les trouver.

Travaux pratiques

Intrusion dans un service Web en ligne. Mise en oeuvre d'un serveur HTTPS. Mise en oeuvre d'un tunnel de sécurité de type IPSec. Protection avancée d'un service Web ; détection des attaques et parades en temps réel. Mise en oeuvre d'un IPS.

Séminaire de 2 jour(s)
Réf : CAB

Participants

Ce séminaire s'adresse aux techniciens et ingénieurs responsables de la conception et mise en oeuvre d'un câblage informatique, mais aussi aux décideurs impliqués dans des projets d'infrastructures de réseaux physiques.

Pré-requis

Connaissances de base dans la technique du câblage informatique.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

15 mai 2012, 27 sep. 2012
29 nov. 2012

Câblages informatiques et nouveaux réseaux

OBJECTIFS

Le câblage informatique est un poste crucial dans l'entreprise, par son coût et son amortissement sur plus de 10 ans. Ce séminaire revisite les techniques cuivre et optique avec illustrations par analyse de CCTP typiques, manipulations avec scanner cuivre, échantillons de connectique actuelle. Il propose également un panorama des technologies récentes qui complètent le câblage traditionnel, parmi lesquelles le CPL et le Wimax.

1) Dernières évolutions des réseaux cuivre et optique, apports des nouvelles technologies

2) Caractérisation, architecture, normes et performances des réseaux

3) Déploiements intérieurs et extérieurs, locaux, campus et métropolitains

4) Description des extensions possibles des LAN par les courants porteurs

Démonstration

Analyses détaillées de plusieurs CCTP de câblage, étude d'un exemple de réponse. Démonstration de scanner DTX1800 cat6 et cat6A. Un échantillonnage de connectiques résumera l'évolution de 25 ans du câblage.

1) Dernières évolutions des réseaux cuivre et optique, apports des nouvelles technologies

- Panorama de l'évolution des techniques et des performances sur un quart de siècle.
- Description des différents médias de transmission disponibles actuellement : cuivre, fibres optiques (silice et plastique), courants porteurs et évolution du sans fil version Wimax.

2) Caractérisation, architecture, normes et performances des réseaux

- Supports cuivre paires torsadées : caractérisation et classification : catégories 5, 5E, 6, 6A, 7. Connectiques cat6 de-embedded. Cat6A re-embedded. Câbles UTP, FTP, STP.
- Evolution des tests paires torsadées : NEXT, atténuation, delay skew, return loss, alien crosstalk
- Fibres optiques silice : multimodes et monomodes. Classifications OM1, OM2, OM3, OM4. OS1.
- Injecteurs LED, lasers, VCSEL. Câbles optiques actifs, cassettes MPO/MTP. Fibres plastiques.
- Mutation apportée par OFDM dans les hauts débits en milieux difficiles (sans fil, CPL, ADSL...).
- Courants porteurs : norme IEEE P1901, maturité et point de départ pour la diffusion de masse.
- Wimax : 802.16a,d,e du fixe au mobile, quel avenir pour le sans fil à portée métropolitaine.
- Normes pour l'ensemble des médias de transmission (US, européennes, françaises).

3) Déploiements intérieurs et extérieurs, locaux, campus et métropolitains

- Les fibres optiques en intérieur et en extérieur (réseaux de Campus, réseaux opérateurs).
- Déploiement de courants porteurs (DLAN Audio Video, dépôts de caméra, d'écran d'affichage).
- Exemples et limites de réalisation de réseaux Wimax par des collectivités territoriales.
- L'avenir incertain du Wimax contrarié par le 3G et 4G et l'hostilité aux micro-ondes.

4) Description des extensions possibles des LAN par les courants porteurs

- Promesses et limitations des courants porteurs. Cibles préférentielles : Hotels, colloques, hôpitaux, musés, grandes surfaces (musiques et écran déportés) comme extensions de LAN. Complément et non alternative aux LAN cuivre et optique.

Séminaire de 2 jour(s)
Réf : FOP

Participants

DSI et responsables télécoms, bailleurs, responsables de collectivités, etc.

Pré-requis

Connaissances de base des problématiques de câblage et des réseaux de distribution informatiques/téléphoniques ou d'interconnexion de sites distants.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

14 juin 2012, 11 oct. 2012
13 déc. 2012

Réseau de distribution en fibre optique, synthèse

OBJECTIFS

Ce séminaire vous propose une synthèse des solutions fibres optiques. Vous verrez comment réaliser un aménagement numérique efficient de bâtiments publics, privés, de grands ensembles tertiaires, commerciaux, de centres urbains... et comment y sont traités les flux d'informations et les services.

- [1\) Fibre optique, fonctionnement et composants](#)
- [2\) Réseaux fibres optiques](#)
- [3\) Usages de la fibre optique dans le bâtiment](#)
- [4\) Usages de la fibre pour les liaisons intersites](#)

1) Fibre optique, fonctionnement et composants

- Découverte des notions élémentaires de la fibre optique.
- Principes et fonctionnement des fibres optiques.
- Les décibels. Les fibres utilisées en Télécom et LAN. Les différents types de connecteurs, cordons et câbles.
- Facteurs de perte sur les liaisons fibres optiques. Les causes de l'affaiblissement.
- Les trois types de dispersion (Modale, PMD, DC).
- Les éléments passifs constitutifs de l'infrastructure du réseau.
- Les bonnes pratiques de mise en oeuvre d'un réseau fibre.
- La définition d'un cahier des charges et les outils d'analyse.

2) Réseaux fibres optiques

- Les déploiements du FTTx - FFTh (Fiber To The home).
- Les notions clés. Le vocabulaire.
- Le cadre législatif, la loi LME. Les obligations concernant l'équipement en fibre optique des bâtiments.
- Choix du média fibre optique dans un réseau d'entreprise LAN.
- Les avantages techniques.
- Les avantages économiques.
- Utilisation de la fibre optique dans les réseaux d'interconnexion de sites distants.
- Les paramètres clés dans le cadre de cette dernière utilisation.

3) Usages de la fibre optique dans le bâtiment

- Une nouvelle architecture réseau.
- Création de nouveaux services et de nouveaux usages.
- Un constat : une montée des besoins.
- Convergence sur une même infrastructure.
- Rappel sur les équipements actifs.
- L'arrivée de solutions dédiées.
- Comment traiter les flux d'informations et les services.
- Etude de cas : enjeux, solutions, résultats. Différents exemples de bâtiments seront ici analysés.

4) Usages de la fibre pour les liaisons intersites

- Comment optimiser son architecture réseau.
- Mutualiser ses services sur fibre optique - WDM.
- Introduction aux critères de qualité de service (QoS).
- Présentation du standard Y1564 concernant la qualité de service.
- Problème de sécurité du réseau optique.
- Etude de cas : enjeux, solutions, résultats.

Travaux pratiques

Séminaire de 2 jour(s)
Réf : AUR

Participants

Ce cours s'adresse aux architectes de réseaux, aux chefs de projets, aux responsables de systèmes d'information, aux ingénieurs réseaux.

Pré-requis

Connaissances de base dans le domaine des réseaux.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

7 juin 2012, 4 oct. 2012
6 déc. 2012

Audit et analyse des réseaux

OBJECTIFS

Le trafic sur les réseaux de données est composé de nombreuses applications dont les volumes sont en général inversement proportionnels à l'importance qu'ils revêtent pour l'entreprise. Ce cours se propose de donner les clés, techniques et pratiques, de l'analyse des réseaux. Les différents types d'outils disponibles aujourd'hui seront présentés et analysés. Des exemples concrets illustreront comment, à travers une méthodologie précise, un système de communication multi-applications peut être contrôlé efficacement pour apporter aux applications le niveau de service indispensable.

1) Le contexte technique

2) La gestion du trafic

3) Sécurité

4) La méthodologie

5) La qualité de service

6) Les outils d'audit et de Qos

1) Le contexte technique

Les architectures de réseaux

- Rappels sur les architectures de protocoles.
- Le réseau d'entreprise, les réseaux virtuels, les techniques de VPN.
- Le réseau longue distance, les services des ISP.
- Les réseaux d'accès : xDSL, WiFi, WiMax.

Les paramètres clés du réseau

- Notion d'échantillonnage, problématiques de la mesure.
- Les débits, valeurs moyennes, rafales.
- Le nombre de paquets par seconde (PPS).
- La distribution de la taille des paquets.
- Le volume des données, les taux de perte.
- Les temps de réponse (RTT) au niveau réseau, au niveau des applications.

L'analyse des goulets d'étranglement

- Le terminal.
- Le réseau d'accès.
- Le cœur de réseaux.
- La performance des équipements (pps, statefull context...).
- Les serveurs.

Métriologie active vs métriologie passive

- Que peut-on mesurer avec des éléments passifs ?
- Qu'apportent les mesures actives ?
- La limite des méthodes de collecte.
- Le passage à l'échelle.

Métriologie : l'impact des couches du modèle en couches

- Les approches purement réseau (niveau 2-3-4*).
- Les approches applicatives (niveau 7) : la classification applicative.
- L'impact applicatif sur le réseau.

L'état de la normalisation

- Les groupes de l'IETF : IPSAMP, IPPM, IPFIX...
- Pourquoi tant d'efforts différents.
- Les approches SNMP.
- Les sondes RMON.

La notion de ticket

- Garder une trace des échanges.
- La sécurité et ses obligations légales.
- Le cas de la téléphonie sur IP et de la messagerie.
- La réglementation française.

Les pistes de recherche

- Packet pair.
- Corrélations statistiques.

2) La gestion du trafic

Les outils

- Les méthodes de contrôle d'admission.
- RED, WFQ, leaky bucket, token bucket, etc.
- Impact des technologies sur les comportements.

Capacity planning

- Prévoir les évolutions.
- Garantir les performances.
- Contrôler les engagements de service.

Des outils pour la gestion de parcs informatiques

- Analyse des systèmes d'exploitation.
- Analyse des applications.
- Découverte de topologies.

3) Sécurité

- Les principes de sécurité liés au trafic : les firewalls.
- Les approches Statefull et Stateless.
- Les limites des systèmes actuels.
- La détection d'intrusion : un audit en temps réel.
- La conformité du trafic aux règles du firewall.

4) La méthodologie

- Les étapes importantes.
- Pourquoi une méthodologie ?
- L'audit permanent.

5) La qualité de service

- Notions de SLA.
- QoS vs CoS.
- Le modèle de bout en bout.

6) Les outils d'audit et de Qos

Audits ponctuels

- Pour quoi faire ? Exemple.
- La qualification d'un réseau pour des usages.

Audits structurels

- Le réseau est un système qui doit être géré et contrôlé.
- Les performances et l'impact financier.

Analyseurs, systèmes de gestion, Traffic Shapers, un état du marché

- Acterna/Sniffer Pro.
- Ethereal/TCPDUMP.
- RMON.
- MRTG.
- Infovista/Concord/Qualaby.
- Qosmos.
- Qosmetrix.
- NetFlow v5, v7, v8, v9.
- Ntop.
- Packeteer.
- Ipanéma.
- Streamcore.

Bilan et comparaison synthétique

Séminaire de 2 jour(s)
Réf : RSA

Participants

Ce séminaire s'adresse aux responsables réseaux, responsables études, architectes, ingénieurs et administrateurs systèmes et réseaux ayant à déterminer et à participer à la mise en place des solutions de supervision et d'administration des réseaux de leur organisation.

Pré-requis

Connaissances de base dans le domaine des réseaux.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

14 juin 2012, 6 sep. 2012
8 nov. 2012

Réseaux, solutions d'administration

OBJECTIFS

Ce séminaire propose une synthèse des solutions pour l'administration des systèmes et réseaux d'entreprise. Il présente l'administration des équipements réseaux, serveurs et postes de travail, les protocoles, les outils du marché ainsi que les évolutions à prendre en compte pour la gestion de la sécurité et des performances.

- 1) L'évolution de l'administration réseau/système** **3) Exemples d'outils disponibles**
2) Evolution des outils d'administration

1) L'évolution de l'administration réseau/système

- Les domaines " classiques " d'administration : configuration, erreurs, tarification, performances, sécurité.
- Importance croissante de la gestion de la sécurité et des performances : " IP everywhere ", applications " temps réel " (VoIP...).
- Administration des équipements réseaux. Routeurs, switches, pare-feu. Configurations, statistiques.
- Administration des postes de travail. Aspects statiques : applications, matériels, systèmes d'exploitation. Aspects dynamiques : utilisateurs, processus, disques, mémoire.

2) Evolution des outils d'administration

- Modèle de fonctionnement Agent/Superviseur.
- Les premiers protocoles : SGMP : Simple Gateway Monitoring Protocol (TCP/IP). CMIS : Common Management Information Service (OSI).
- Le protocole SNMP (Simple Network Management Protocol) version 1. Messages SNMP. Alarmes SNMP.
- Les MIB (Management Information Bases). Représentation des données de gestion : SMI (Structure of Management Information), ASN.1 (Abstract Syntax Notation 1). MIB normalisées et MIB propriétaires.
- Evolutions de SNMP. Problèmes de sécurité. Modification du modèle de supervision. Versions 2c et 3. Les nouvelles MIB.
- Les efforts de l'industrie. DMTF : Distributed Management Task Force. Extension des possibilités. Intégration de différentes techniques.
- WBEM (Web Based Enterprise Management).
- ACPI (Advanced Configuration and Power Interface). (Hewlett-Packard/Intel/Microsoft/Phoenix/Toshiba).
- WMI (Windows Management Instrumentation) de Microsoft.

3) Exemples d'outils disponibles

- Outils gratuits et applications propriétaires.
- Capacités d'observation et/ou de modification. Les environnements surveillés (Linux, Windows, et autres).
- Techniques de surveillance. SNMP. Services réseaux. Paramètres et services " internes ".
- Démonstration de Big Brother (Quest Software).
- Démonstration avec Nagios (Open source).

Séminaire de 2 jour(s)
Réf : OOS

Participants

Ingénieur, architecte et chef de projet réseau. Tout décideur informatique, notamment les responsables technique/infrastructure.

Pré-requis

Connaissances de base en réseau informatique.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

15 mai 2012, 6 sep. 2012
29 nov. 2012

La QoS dans les réseaux IP, MPLS et Ethernet

OBJECTIFS

Ce cours vous apportera des connaissances complètes et synthétiques sur la Qualité de Service (QoS) : comment fournir un service conforme à des exigences en matière de temps de réponse et de bande passante. Il montre l'interaction de la QoS avec les protocoles les plus utilisés dans le monde des réseaux informatiques.

- 1) [Concepts de base](#)
- 2) [La QoS et le protocole IP](#)

- 3) [La QoS et le MPLS](#)
- 4) [La QoS et Ethernet](#)

1) Concepts de base

- Le fonctionnement du réseau.
- La caractérisation de la Qualité de Service (QoS) IP.
- Les mécanismes qui permettent de la garantir.
- Les protocoles de transport.
- Mise en oeuvre de la QoS.

2) La QoS et le protocole IP

- Le modèle DiffServ.
- Le classement du service.
- Les informations à stocker dans le paquet IP.
- Le champ TOS (Type Of Service).
- Le traitement différencié.
- Le contrôle et le marquage des équipements réseaux.
- Le modèle IntServ.
- Comment faire de la QoS sans " toucher " le protocole IP ?
- Le protocole RSVP.
- Réserver la bande passante dynamiquement.
- La facturation différenciée par le récepteur.
- La redondance des passerelles.
- Les protocoles HSRP et VRRP.
- La reconfiguration des équipements.
- Le mécanisme Graceful Restart.
- Le principe de redémarrage de la carte de contrôle.

Etude de cas

Exemples de configuration.

3) La QoS et le MPLS

- Le support de Diffserv par MPLS.
- Contrôler et réguler la distribution du trafic.
- Implémenter le Trafic Engineering.
- Les protocoles RSVP-TE et OSPF-TE.
- La mise en oeuvre conjointe de la QoS et du TE, le Diffserv-Aware TE.
- La garantie de reroutage en moins de 50 ms.
- Le mécanisme Fast ReRoute.
- Mise en oeuvre du Fast ReRoute.
- Le Graceful Restart et MPLS.

Etude de cas

Exemples de configuration.

4) La QoS et Ethernet

- La gestion des priorités et le mappage avec DiffServ.
- Le protocole Subnetwork Bandwidth Manager (SBM).
- Comment réserver les ressources avec SBM.
- Le Spanning Tree et la QoS.
- Reconfigurer le réseau avec les protocoles STP et RSTP.

Exercice

Exemples de configuration.

Séminaire de 2 jour(s)
Réf : IAT

Participants

Ce cours s'adresse à tous les métiers de l'entreprise susceptibles de participer de près ou de loin à l'évolution de la filière téléphonique, que ce soit du personnel technique ou des métiers directement liés à l'activité de l'entreprise. Ce cours peut fournir un excellent pré-requis pour les cours de Téléphonie sur IP.

Pré-requis

Aucune connaissance particulière.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

14 juin 2012, 27 sep. 2012
29 nov. 2012

Introduction aux télécommunications RTC/RNIS # PABX / IPBX # ToIP # Convergence fixe/mobile

OBJECTIFS

Cette formation présente les principes des télécommunications d'entreprise et du vocabulaire associé. Elle décrit les normes utilisées en téléphonie, les principes d'architecture, les équipements, les services et les applications disponibles, et montre comment structurer et organiser un réseau de téléphonie d'entreprise.

1) Réseaux téléphoniques d'opérateurs fixes

2) Téléphonie d'entreprise : du PABX à l'IP Centrex

3) La signalisation

4) Services et applications de la téléphonie

5) La téléphonie sur IP

6) Téléphonie sans fil et téléphonie mobile

7) Les services de communications avancés

1) Réseaux téléphoniques d'opérateurs fixes

- De la voix à la téléphonie.
- Le traitement du signal (analogique et numérique).
- Historique des réseaux téléphoniques RTC, RNIS.
- Organisation des réseaux opérateurs.
- Les accès opérateurs numériques (MIC).
- Les signalisations D (Q931), SS7.
- Les services évolués et le réseau intelligent.
- Evolution des Télécoms.

2) Téléphonie d'entreprise : du PABX à l'IP Centrex

- Architecture et composants.
- Le traitement des appels (call handling).
- Le routage et la commutation.
- Evolution de l'architecture des réseaux d'entreprise, convergence voix/données (PABX, PABX-IP).
- Evolution vers la téléphonie sur IP (ToIP).
- Interconnexion de PABX (RPIS).

Les Call Centers

- Architecture et composants.
- Les étapes de traitement d'un appel client.
- Distribution et gestion de file d'attente.
- CTI et les standards CSTA.

3) La signalisation

- Rôle et objectifs. Types de signalisation. Les standards et la convergence vers l'IP.
- Les protocoles multimédias H323, SIP, RTP, MGCP. Les codecs multimédias (G7xx, AMR, H263, MPEG 4).
- Architecture et dynamique des flux.

4) Services et applications de la téléphonie

- Les services de base (double appel, multiligne).
- Les services d'accueil (prédécroché, groupement...).
- Messagerie vocale et messagerie unifiée.
- Synthèse vocale et technologie " text to speech ".
- Standard automatique et serveur vocal interactif.
- Les applications de gestion.

5) La téléphonie sur IP

- Besoins des réseaux data et réseau de téléphonie.
- Les nouveaux services.
- Les scénarios d'entreprise.

6) Téléphonie sans fil et téléphonie mobile

- Les réseaux mobiles GSM, EDGE et UMTS.
- La mobilité sur IP (Wifi / 802.11x, Wimax).
- La convergence fixe-mobile (UMA).

7) Les services de communications avancés

- Personal Information Management.
- Services voix/vidéo temps réel via le web (API XML, Voice XML).
- Nouveaux services (présence, messagerie instantanée, visiophonie...).

- Perspectives d'évolution IMS (IP Multimedia Subsystem) : tendances et opportunités.
- Nouveaux usages et conduite du changement.

Séminaire de 3 jour(s)
Réf : RSW

Participants

Ce séminaire s'adresse aux informaticiens et aux ingénieurs réseaux souhaitant se spécialiser dans les réseaux cellulaires, aux responsables réseaux mobiles et responsables études désireux d'acquérir des connaissances plus approfondies sur le sujet.

Pré-requis

Bonnes connaissances dans le domaine des réseaux d'entreprise.

Prix 2012 : 2430€ HT

Eligible DIF

Dates des sessions

Paris

19 juin 2012, 2 oct. 2012
11 déc. 2012

Réseaux sans fil, Wi-Fi

OBJECTIFS

Le monde des réseaux sans fil s'enrichit rapidement de nouvelles normes et de nouveaux standards. Ces réseaux permettent de connecter entre eux les équipements de l'entreprise de type voix, données, images. Ils sont également à la base des " hot spots " des opérateurs. Les réseaux IEEE 802.11 (Wi-Fi et toutes les déclinaisons), Bluetooth, UWB, Zigbee, IEEE 802.16, WiMAX, WRAN, etc., seront étudiés en détail dans ce séminaire ainsi que les applications qui peuvent y être associées. Compte tenu des spécificités et de l'importance de la sécurité, la dernière journée de ce séminaire lui sera entièrement consacrée.

1) Principes des réseaux sans fil

2) Bluetooth, UWB, ZigBee et IEEE 802.15

3) Wi-Fi – IEEE 802.11

4) Les réseaux mesh et les réseaux ad hoc

5) Les normes IEEE 802.16 et WiMAX

6) Les autres solutions

7) Les protocoles et les applications des réseaux sans fil

8) La mobilité dans les réseaux sans fil

9) L'Internet ambiant

10) 3G vs WLAN

11) Sécurité WiFi

12) Interconnexion des LAN et des WLAN

1) Principes des réseaux sans fil

Introduction aux réseaux sans fil

- Comparaison avec le fixe. Les diverses générations.

Les WPAN, WLAN, WMAN, WRAN

- Les caractéristiques et les performances attendues.
- Les handovers et l'intégration des solutions.

L'intégration des réseaux sans fil dans l'entreprise

- Débits nécessaires. Applications disponibles. Environnement domotique, de bureaux, et d'entreprise.

Les " hot spots " des opérateurs

- Les avantages des technologies Wi-Fi.
- Les problèmes durs posés par Wi-Fi aux opérateurs.

Les handovers

- Le problème de la mobilité. Les différents types.
- L'intégration avec les mobiles.

2) Bluetooth, UWB, ZigBee et IEEE 802.15

- Les normes IEEE 802.15 et les technologies UWB, Zigbee et Bluetooth. Le soutien des industriels.
- La technologie IEEE 802.15.1 et Bluetooth.
- IEEE 802.15.3. La technologie à très haut débit UWB.
- Le consortium Wimedia et WUSB.
- IEEE 802.15.4 et les produits ZigBee.
- Les technologies de réseaux personnels.

3) Wi-Fi – IEEE 802.11

Wi-Fi (IEEE 802.11b/g)

- Les raisons de son succès. Les particularités.
- Equipements Wi-Fi : cartes et points d'accès.
- Couche MAC : CSMA/CA. Bandes de fréquences.
- Intégration Ethernet. Débits et performances.
- La technique d'accès au support physique.
- La qualité de service et l'IEEE 802.11e.
- La parole téléphonique et les flux " stream ".
- Les commutateurs et les contrôleurs Wi-Fi.
- L'ingénierie et la gestion des réseaux Wi-Fi.
- L'avenir de la norme IEEE 802.11b avec l'IEEE 802.11n et l'introduction des techniques MIMO.

Mise en place d'un réseau Wi-Fi

- Contraintes. Equipements. Coût. Configuration.

4) Les réseaux mesh et les réseaux ad hoc

- Définition d'un réseau mesh et d'un réseau ad hoc.
- Routage dans les réseaux mesh. Protocoles de routage : proactifs (OLSR, DSDV) et réactifs (AODV, DSR). Sécurité et QoS dans les réseaux ad hoc.

5) Les normes IEEE 802.16 et WiMAX

- Définition : boucle locale radio (BLR) et accès WDSL (Wireless DSL). Concurrence avec les solutions fixes.
- Les techniques et les fréquences disponibles.
- WiMAX. Performances attendues. Normalisation IEEE 802.16. WiMAX mobile. Comparaison à la 3G/4G.

6) Les autres solutions

- La génération de réseaux sans fil régionaux WRAN. L'intégration des canaux de télévision et l'IEEE 802.22. La radio cognitive. La télévision interactive.
- L'intégration des réseaux sans fil dans un réseau unique. IEEE 802.21 et le handover vertical. La continuité de service et l'Internet hertzien.

7) Les protocoles et les applications des réseaux sans fil

- L'environnement IP. Les problèmes du slow start.
- Les technologies MIMO et l'augmentation des débits.
- Les réseaux de domicile : UPnP et DLNA.
- Les applications : parole, vidéo, production, P2P...

8) La mobilité dans les réseaux sans fil

- IP Mobile et la gestion de la mobilité inter domaines
- Les réseaux cellulaires : GSM, GPRS, EDGE
- Les réseaux 3G (UMTS) et 3G+ (HSDPA et HSUPA)
- La méthode d'accès OFDMA et les réseaux HSOPA
- La future génération : LTE et UMB.
- Les handovers horizontaux, diagonaux et verticaux.

9) L'Internet ambiant

- Les développements. Les villes Internet.
- L'intégration dans la nouvelle génération IP.
- Réseaux de capteurs. Poussières électroniques.

10) 3G vs WLAN

- L'opposition 3GPP/3GPP2 et Wi-xx. La concurrence avec l'UMTS. La quatrième génération de mobiles (4G) et l'intégration. UMA et IMS.

11) Sécurité WiFi

Faiblesses intrinsèques des réseaux sans fil

- Est-il possible de se protéger d'un déni de service ? Comment contrôler la zone d'émission ? Etc.
- Le rôle du SSID en matière de sécurité.
- Attaques : Man in the middle, ARP Spoofing.
- Les faiblesses des solutions d'authentification.

Fonctions élémentaires : SSID et MAC Filtering

- Intérêt et limites. Le rôle et les risques de la " beacon frame " et de la " SSID Probe Request ".
- Illustration d'attaques : SSID Brute Force...

Wired Equivalent Privacy – WEP

- Fonctionnement. Echange des clefs. Authentification et chiffrement. Attaques connues, démonstrations.

WiFi Protected Access – WPA

- Fonctionnement. Avantages de WPA sur WEP.
- Extensible Authentication Protocol – EAP.
- Temporal Key Integrity Protocol – TKIP.
- Message Integrity Check – MIC.
- WPA v2 et norme 802.11i.

12) Interconnexion des LAN et des WLAN

- Contrôle de la zone de couverture. Segmentation du réseau. Firewall et zones démilitarisées. Protection du poste client. Utilisateurs nomades, VPN et réseaux sans fil.

Stage pratique de 1 jour(s)
Réf : AWF

Participants

Informaticiens et ingénieurs réseaux souhaitant se spécialiser dans les réseaux mobiles à haut débit. Il s'adresse également aux responsables réseaux mobiles et responsables études désireux d'acquérir des connaissances approfondies sur le sujet.

Pré-requis

De bonnes connaissances dans le domaine des réseaux, de l'informatique ou des télécoms.

Prix 2012 : 890€ HT

Eligible DIF

Dates des sessions

Paris

10 sep. 2012, 12 nov. 2012

Architecture Wi-Fi - WiMAX

Architectures, services, normes, choix techniques

OBJECTIFS

Ce cours examine les différentes solutions opérationnelles aujourd'hui en matière de Wi-Fi et de WiMAX. L'objectif de ces réseaux est d'introduire le monde IP dans les environnements sans fil pour former l'Internet sans fil ou Internet hertzien. Aujourd'hui ces réseaux sont capables de transporter des applications de tout type : téléphonie IP, transfert de données à très haut débit, vidéo, télévision, multimédia, etc. Ce cours propose une vision de l'ensemble des éléments nécessaires à la réalisation d'un environnement sans fil d'entreprise utilisant à la fois le Wi-Fi et le WiMAX.

1) Introduction aux réseaux IEEE

2) Les réseaux Wi-Fi

3) Les réseaux WiMAX

4) Conclusions et perspectives

1) Introduction aux réseaux IEEE

Introduction aux catégories de réseaux sans fil

- Les WWAN (Wireless WAN);
- Les principales normes IEEE (802.11 et 802.16).
- internet haut débit par Wi-Fi et WiMAX.

2) Les réseaux Wi-Fi

Les différents réseaux Wi-Fi

- Wi-Fi et ses options à 11, 54, 190 Mbit/s.
- Les changements intercellulaires et le handover : IEEE 802.11f.
- Les faiblesses en matière de sécurité et les solutions de base.
- Les commutateurs, les contrôleurs, les ponts et les produits Wi-Fi.
- La réglementation.
- Mise en fonctionnement de la carte, programmation des différentes fonctionnalités gérées par la carte.

Les performances d'un réseau Wi-Fi

- Distance et puissance.
- Installation dans un bâtiment et sur un campus.
- Le choix des fréquences à utiliser.

La sécurité dans les réseaux Wi-Fi

- Les niveaux de sécurité dans les équipements Wi-Fi commercialisés.
- Les trois générations de sécurité : WEP, WPA et WPA2.
- Mise en place d'un contrôle par liste d'accès (Adresse MAC) et d'une sécurité WEP, WPA et WPA2.

Les applications sous Wi-Fi

- Les applications de données.
- La téléphonie Wi-Fi d'entreprise (ToIP over Wi-Fi).
- La téléconférence, la vidéo et la télésurveillance sur Wi-Fi. Les applications professionnelles.

3) Les réseaux WiMAX

Les différents réseaux WiMAX

- Le réseau WiMAX fixe et l'ADSL hertzien : le WDSL.
- Les débits possibles pour le client.
- La boucle locale radio.
- Le WiMAX mobile) et l'ADSL mobile.
- Les opérateurs WiMAX fixe et mobile.

La technologie WiMAX

- L'OFDM ; les fréquences et les portées.
- La technique d'accès.
- Les classes de service du WiMAX fixe et du WiMAX mobile.
- Les applications de parole et de vidéo au travers du WiMAX.
- Les différences avec les technologies 3G et 4G.

La sécurité dans les réseaux Wi-Fi

- Les niveaux de sécurité dans les équipements WiMAX commercialisés.
- L'authentification de l'utilisateur.

L'installation d'un réseau WiMAX

- Installation en ville et dans les zones rurales.
- Les fréquences disponibles et les possibles fréquences futures.
- Exemple d'installation d'un réseau WiMAX dans une zone rurale.

Les applications sous WiMAX

- Les applications de données.
- La téléphonie WiMAX d'entreprise (ToIP over WiMAX et IPTV).
- Les applications professionnelles.

4) Conclusions et perspectives

- Les évolutions et révolutions possibles.

Séminaire de 2 jour(s)
Réf : VIP

Participants

Responsables réseaux, responsables études, responsables SI, chefs de projets, architectes réseaux, ingénieurs systèmes et réseaux. Tous ceux devant participer à la définition, à la mise en place de solutions de téléphonie et de multimédia sur IP.

Pré-requis

Connaissances de base en réseaux.

Prix 2012 : 1775€ HT

Eligible DIF

Dates des sessions

Paris

21 juin 2012, 13 sep. 2012
15 nov. 2012

Téléphonie sur IP architectures et solutions

OBJECTIFS

Ce séminaire propose une synthèse des solutions de téléphonie sur IP. Il présente les concepts fondateurs et les finalités. Il décrit l'essentiel des protocoles sous-jacents et traite les problématiques de migration, de performance et de sécurité. Les différentes solutions possibles sont analysées et illustrées au moyen d'études de cas réels.

[1\) Rappels réseaux et télécoms](#)

[2\) La téléphonie sur IP](#)

[3\) L'essentiel des protocoles \(H323, SIP, ...\)](#)

[4\) Migrer vers la téléphonie sur IP](#)

[5\) Intégration et administration](#)

[6\) Performance et QoS des réseaux ToIP](#)

[7\) La sécurité](#)

[8\) L'avenir](#)

1) Rappels réseaux et télécoms

- Le RTC : le Réseau Téléphonique Commuté.
- Le service téléphonique d'entreprise. Son architecture. Ses éléments actifs (PABX, Terminaux). Les services disponibles. Ses contraintes et limitations.
- L'architecture Internet, les réseaux TCP/IP.
- Le réseau de données d'entreprise. Son architecture.

2) La téléphonie sur IP

- Définition et concepts. Le vocabulaire de la ToIP.
- Les réseaux d'entreprise et leurs évolutions : Voix et Données, convergence vers un seul réseau.
- Pourquoi migrer vers la ToIP ? Comment intégrer la ToIP au système d'information de l'entreprise ? Comment interopérer avec les réseaux téléphoniques classiques ?
- Les fonctionnalités utilisateur apportées par la ToIP.
- Le marché et ses acteurs.

3) L'essentiel des protocoles (H323, SIP, ...)

- Rôle et intérêt de chacun des protocoles.

Présentation et architecture H323

- Principes et définitions.
- Composants H323 : gatekeeper, MCU, gateway...
- Communication H323 : RAS, H225, H245...
- Exemples d'architectures d'entreprises.

Présentation et architecture SIP

- Principes et définitions.
- Composants SIP : proxy, registrar, redirection, location...
- Communication SIP : enregistrement, localisation, appel, mobilité...
- Exemples d'architectures d'entreprises.

Les autres protocoles VoIP

- MGCP, MEGACO, H248...
- Le protocole IAX, le protocole Open Source d'Asterisk.

4) Migrer vers la téléphonie sur IP

Les clés du choix pour la ToIP

- Les motivations des entreprises pour le passage à la ToIP sont : le coût : les plus (les communications, la maintenance), les moins (le matériel, les compétences)...
- Les nouveaux services : améliorer la productivité des collaborateurs (VisioConf, Mobilité...etc.).
- L'évolutivité du réseau et de ses applications.
- L'image de l'entreprise.

Scénarii d'entreprises et solutions du marché

- Plusieurs solutions, pour différentes entreprises :
- L'interconnexion PABX-PABX.
- La migration vers le PABX IP : exemples de solutions constructeurs, ses avantages et ses contraintes.
- Les solutions de type IP Centrex : exemples de solutions opérateurs, ses avantages et ses contraintes.
- Peer-to-peer : le modèle Skype et Wengo.
- Satisfaction et maturité des solutions.

La gestion d'un projet ToIP

- Les étapes : analyse du besoin, audit des réseaux, comparaison des solutions disponibles, adaptation de la solution à l'entreprise, migration...
- Les clés de la réussite. Les freins.

Travaux pratiques

TPE, PME et Grands comptes. Fonctionnalités, analyse du coût, disponibilité, maintenance...

5) Intégration et administration

- Outils d'administration constructeurs. Sondes de mesure de la QoS.
- Intégration avec les bases de données utilisateurs : LDAP, SSO.
- Utilisation et mise à jour des équipements réseaux : DHCP, TFTP, DNS...
- Les terminaux de téléphonie mobiles (VoIP sur WiFi, DECT, terminaux bi-mode...).
- Les liens : xDSL, Ethernet, liaisons radio, dimensionnement.

6) Performance et QoS des réseaux ToIP

Pourquoi les réseaux de données n'apportent pas la fiabilité requise pour le transport de la voix ?

- La référence en matière de fiabilité : le RTC.
- Forces et faiblesses des réseaux de données en matière de qualité de service.
- Concepts de la QoS. Le délai, la gigue, la perte de paquets... Impacts de la QoS d'un réseau IP sur la ToIP.

Le transport de la voix

- Numérisation de la voix : utilisation des codecs.
- Pour compenser le manque de fiabilité des réseaux IP, utilisation de protocoles spécifiques : RTP et RTCP.
- Résumé des flux en jeu dans la ToIP. La signalisation (acheminement des appels). Le média (voix, vidéo...).

Apporter de la performance aux réseaux IP

- Renforcer la bande passante.
- Les outils de gestion de la QoS pour les réseaux IP (802.1P/Q, RSVP, DiffServ, MPLS...).
- Les référentiels de qualité en VoIP : E-model, PESQ, PAMS, PSQM.

7) La sécurité

- Problématique du passage aux solutions ToIP. De quoi doit-on se protéger, de qui, pourquoi peut-on être attaqué ?
- Les menaces connues. La confidentialité : protéger les flux media et les données de type signalisation. L'intégrité : contrôler et empêcher les modifications des données. La disponibilité et le déni de service. L'usurpation d'identité. La fraude. Le spam. La réglementation : les obligations légales de sécurité et les freins au développement technologique.
- La problématique des services d'urgence.

8) L'avenir

- Les évolutions des opérateurs : convergence fixe/mobile et abandon du modèle RTC pour la VoIP.
- Les technologies de la convergence : WiMax, MPLS...
- Les nouveaux services et usages multimédias.
- IMS, IP Multimedia Subsystem, le réseau multimédia de demain.

Stage pratique de 1 jour(s)
Réf : ICO

Participants

Toute personne souhaitant être initiée au contexte des systèmes de communication.

Pré-requis

Aucun

Prix 2012 : 890€ HT

Eligible DIF

Dates des sessions

Paris

18 juin 2012, 1 oct. 2012
3 déc. 2012

Introduction à la communication cellulaire

OBJECTIFS

Cette formation offre un aperçu de l'histoire des réseaux cellulaires, de leurs services ainsi qu'un survol technique des technologies. Il permettra d'acquérir le vocabulaire nécessaire pour comprendre et discuter avec les professionnels du domaine.

1) La naissance de l'architecture cellulaire

2) Interface radio

3) Les générations de réseaux cellulaires

4) Evolution du marché cellulaire

5) La mobilité dans les réseaux IP

1) La naissance de l'architecture cellulaire

2) Interface radio

- Multiplexage fréquentiel, temporel, par code.
- Contrôle de puissance.
- Planification et réutilisation de fréquence.

3) Les générations de réseaux cellulaires

- Radiocom 2000 et les autres technologies.
- GSM et ses évolutions (GPRS, EDGE).
- 3G et ses évolutions vers le très haut débit.
- LTE/4G et le WIMAX.

4) Evolution du marché cellulaire

- Le GSM : une success story.
- L'héritage du succès de GSM.
- L'échec de la concurrence.

5) La mobilité dans les réseaux IP

- IP mobile.
- IP cellulaire.
- Les réseaux ad hoc.

Exercice

Exercices sur le calcul de débit en GSM, GPRS, EDGE et UMTS. Exercices sur la mobilité IP.

Stage pratique de 2 jour(s)
Réf : ERC

Participants

Ingénieurs réseaux souhaitant se spécialiser dans les réseaux mobiles à haut débit. Responsables réseaux mobiles et responsables études.

Pré-requis

Bonnes connaissances dans le domaine des réseaux, de l'informatique ou des télécoms.

Prix 2012 : 1730€ HT

Eligible DIF

Dates des sessions

Paris

7 juin 2012, 27 sep. 2012
29 nov. 2012

Evolution des réseaux cellulaires

OBJECTIFS

Le but de ce séminaire est d'offrir une vue générale des réseaux cellulaires et de leurs concurrents. Il couvre les méthodes d'accès et de transferts de données, la structure des réseaux mobiles, le sans-fil et le passage à l'Internet mobile. A l'issue, le public aura les connaissances nécessaires pour décider d'une politique de réseaux mobiles.

1) Généralités

2) Base des systèmes cellulaires

3) Structure générale des réseaux mobiles

4) Les réseaux sans fil et le passage à la mobilité

5) L'évolution vers l'Internet mobile

1) Généralités

- Introduction.
- Historique : service mobile, transmission radio.
- Réseaux fixes vs. Réseaux mobiles.
- Les fréquences et le spectre hertzien.
- Propagation et directivité.
- Les cellules : tailles, obstacle, performance.
- Les quatre générations de réseaux mobiles.
- Réseaux analogiques : les radio-mobiles (1 G),
- Réseaux circuit numérique : le GSM (2 G),
- Réseaux paquet numérique : l'UMTS (3 G).
- Réseaux multimédias : le LTE (4G).

2) Base des systèmes cellulaires

- Réseaux mobiles : ondes et propagation.
- Méthodes d'accès FDMA.
- Méthodes d'accès TDMA.
- Méthodes d'accès CDMA.
- La solution du futur : l'OFDMA.
- Méthodes de transfert des données.
- La compatibilité à l'Internet et à la norme IP.

3) Structure générale des réseaux mobiles

- Liaison radio.
- GSM, GPRS, EDGE, UMTS, HSDPA.
- L'itinérance.
- Les handovers.

4) Les réseaux sans fil et le passage à la mobilité

- Les réseaux cellulaires IEEE.
- Le Wi-Fi et le WiMAX.
- L'Internet sans fil.
- Les handovers horizontaux et verticaux.

5) L'évolution vers l'Internet mobile

- Architecture des réseaux tout-IP.
- Mobilité IP.
- Les réseaux ad hoc.
- Les réseaux mesh.

Stage pratique de 2 jour(s)
Réf : GGE

Participants

Ingénieurs réseaux souhaitant se spécialiser dans les réseaux mobiles. Responsables réseaux mobiles et responsables études.

Pré-requis

Bonnes connaissances dans le domaine des réseaux, de l'informatique ou des télécoms.

Prix 2012 : 1730€ HT

Eligible DIF

Dates des sessions

Paris

11 oct. 2012, 13 déc. 2012

Aix

21 juin 2012, 6 sep. 2012
8 nov. 2012

Bordeaux

13 sep. 2012, 22 nov. 2012

Bruxelles

13 sep. 2012, 22 nov. 2012

Genève

13 sep. 2012, 22 nov. 2012

Lille

13 sep. 2012, 22 nov. 2012

Luxembourg

13 sep. 2012, 22 nov. 2012

Lyon

21 juin 2012, 6 sep. 2012
8 nov. 2012

Nantes

14 juin 2012, 13 sep. 2012
15 nov. 2012

Rennes

14 juin 2012, 13 sep. 2012
15 nov. 2012

Sophia-antipolis

6 sep. 2012, 8 nov. 2012

Strasbourg

13 sep. 2012, 22 nov. 2012

Toulouse

13 sep. 2012, 22 nov. 2012

Réseaux mobiles, GSM, GPRS et EDGE

OBJECTIFS

Ce séminaire vous présente les techniques qui ont introduit la mobilité dans notre quotidien : GSM, GPRS, et EDGE. Il détaille la norme GSM et son évolution vers le mode paquet et le haut débit. Il examine également les enjeux induits par les nouvelles applications fonctionnant sur les réseaux mobiles. A l'issue, vous aurez tous les éléments nécessaires pour faire le point sur les systèmes existants et les évolutions en cours.

1) Le système GSM

2) Le système GPRS

3) Le système EDGE

1) Le système GSM

- Son essor à travers le monde.
- Ses avantages et ses défauts.
- L'architecture du GSM.
- Les différents éléments composant le GSM : MS, BTS, BSC, MSC, HLR, VLR, etc.
- Les interfaces reliant ces éléments entre eux.
- Etude détaillée de l'interface Um, soit l'interface radio.
- Définition du canal physique dans GSM. Ses différents débits.
- La capacité maximale du réseau d'accès dans GSM.
- Les canaux logiques.
- Comment GSM utilise-t-il son canal physique pour la signalisation et pour l'information utile ?
- Les structures des multi-trames. Le multiplexage.
- Les messages. Les protocoles existant entre le terminal et le réseau pour établir une communication.
- Etude du transfert intercellulaire (handover) et de l'établissement d'appel.
- L'authentification et le chiffrement dans le GSM.
- Les concurrents de GSM.
- Quels sont les systèmes américains ? L'IS136 et l'IS95. En quoi se distinguent-ils de GSM ?
- Aperçu des innovations apportées par l'IS95 : soft handoff et transmission discontinue.

2) Le système GPRS

- GSM et le mode paquet.
- A quel type de trafic en mode paquet le GPRS est-il adapté ?
- Etude du trafic www.
- L'architecture GPRS.
- Les éléments du mode paquet et la passerelle vers l'Internet : GGSN et GGSN.
- Exemple de routage GPRS.
- L'allocation des ressources radio par GPRS.
- Allocations statique et dynamique.
- La multi-trame GPRS.
- Les classes de service.
- Les canaux logiques de GPRS.
- La cohabitation avec GSM.
- La gestion des terminaux : actifs et oisifs.

3) Le système EDGE

- Le haut débit.
- Comment peut-on améliorer le débit de GSM ?
- La modulation 8-PSK.
- Les débits EDGE.
- L'adaptation du lien.

Stage pratique de 3 jour(s)
Réf : GUM

Participants

Ingénieurs réseaux souhaitant se spécialiser dans les réseaux mobiles à haut débit. Responsables réseaux mobiles et responsables études.

Pré-requis

Bonnes connaissances dans le domaine des réseaux, de l'informatique ou des télécoms.

Prix 2012 : 2340€ HT

Eligible DIF

Dates des sessions

Paris

1 oct. 2012, 3 déc. 2012

Lyon

27 juin 2012

Réseaux mobiles, solutions 3G - UMTS

OBJECTIFS

Après une évolution de notre société avec l'utilisation de GSM, le monde des télécommunications a voulu se tourner définitivement vers le haut débit. La 3G (UMTS) en était la première version dans les réseaux mobiles. Le mode paquet est venu d'une évolution du GPRS et d'EDGE où les débits pouvaient avoisiner la centaine de Kbit/s dans le meilleur des cas, vers l'UMTS avec des débits de l'ordre de quelques centaines de Kbit/s. Ce cours vous apportera les connaissances nécessaires à une bonne compréhension des réseaux UMTS après avoir fait un rappel des réseaux GSM/GPRS/EDGE.

- 1) Architecture cellulaire
- 2) Réseaux GSM/GPRS/EDGE
- 3) Le CDMA

- 4) La 3ème génération
- 5) Illustration : comprendre le CDMA

1) Architecture cellulaire

- Concepts et rappels.
- Les quatre générations de réseaux mobiles.
- Radio-mobile, GSM, UMTS, LTE.
- Méthodes d'accès et de transfert des données.
- Structure générale d'un réseau mobile.

2) Réseaux GSM/GPRS/EDGE

- Rappel des principes et des concepts maintenus par la 3G.
- Architecture du GSM.
- Les éléments composant le GSM.
- Les messages et protocoles du GSM.
- Architecture et composants GPRS.
- EDGE. Le haut débit.

3) Le CDMA

- Présentation de CDMA (Code Division Multiple Access).
- Codage des transmissions.
- L'orthogonalité entre les ressources et les difficultés rencontrées pour la maintenir.
- Codes orthogonaux et séquences pseudo-aléatoires.
- Synchronisation des canaux de communication en CDMA.
- Allocation des codes aux utilisateurs dans une cellule et sur l'envoi de l'information en mode CDMA.

4) La 3ème génération

- UMTS et IMT2000.
- Introduction aux réseaux universels de troisième génération.
- Le programme IMT2000.
- La concurrence mondiale dans la troisième génération.
- Le système UMTS.
- Les services proposés par l'UMTS.
- Les débits variables.
- Les différents modes de multiplexage sur l'interface radio.
- Les fréquences allouées pour l'UMTS.
- Zoom sur la disponibilité de cette bande de fréquences au plan mondial.
- La transition de la deuxième à la troisième génération.
- L'architecture de l'UMTS.
- Le module utilisateur : UE.
- Le réseau d'accès : UTRAN.
- Le réseau coeur : CN.
- L'interface radio Uu.
- Les modes FDD/W-CDMA et TDD/TD-CDMA. Une comparaison entre les deux modes.
- Le W-CDMA.
- Les canaux physiques.
- Les canaux logiques et le mapping avec les canaux physiques.
- La méthode d'allocation de codes aux terminaux. Le concurrent américain : cdma2000.
- HDR (High Data Service). Le service paquet du cdma2000 et une interconnexion efficace avec l'Internet et le protocole IP.

5) Illustration : comprendre le CDMA

- Le contrôle de puissance : boucle ouverte et boucle fermée.
- Comment générer des codes orthogonaux.
- Illustrer le problème de la synchronisation et la perte d'orthogonalité.
- Les séquences pseudo-aléatoires et la correction de la désynchronisation.

- Voir un exemple complet de la chaîne de transmission CDMA (codage et scrambling).

Stage pratique de 2 jour(s)
Réf : EUM

Participants

Ingénieurs réseaux souhaitant se spécialiser dans les réseaux mobiles.
Responsables réseaux mobiles et responsables études.

Pré-requis

Bonnes connaissances dans le domaine des réseaux, de l'informatique ou des télécoms.

Prix 2012 : 1730€ HT

Eligible DIF

Dates des sessions

Paris

31 mai 2012, 4 oct. 2012
6 déc. 2012

Réseaux mobiles, solutions 3G+ évolution de l'UMTS

OBJECTIFS

Les optimisations appelées 3G+ (HSPA, MBMS, LTE) ont dopé les débits de l'UMTS et contribué à son succès commercial. A l'issue de ce stage, vous aurez acquis toutes les connaissances nécessaires à la maîtrise des réseaux 3G et de leur optimisation.

1) La technologie 3G et son fonctionnement

2) Optimisations pour la 3G+

3) L'environnement IMS et la signalisation associée SIP

4) Les systèmes 3G+

1) La technologie 3G et son fonctionnement

- UMTS et IMT2000.
- Le système UMTS.
- Les services proposés par l'UMTS.
- L'architecture de l'UMTS.
- Les composants de l'UMTS.
- Connexion aux réseaux fixes.
- Interface radio : WCDMA, CDMA 2000.
- Les problèmes de performance.

2) Optimisations pour la 3G+

- Définition de l'optimisation algorithmique.
- Les intervalles de transmissions à 2ms.
- Le canal partagé.
- Les procédures d'ordonnancement intelligent.
- La modulation et le codage adaptatif (de la QPSK à la 16 QAM).
- La transmission hybride (H- ARQ).
- Les interfaces MIMO (Multiple Input Multiple Output).
- Les débits.
- Illustration sur le boosting du débit de la 3G.
- Illustration sur la chaîne de transmission 3G et optimisation pour améliorer les performances.

3) L'environnement IMS et la signalisation associée SIP

- Migration vers des réseaux tout IP.
- Standardisation de l'IMS.
- Architecture de l'IMS.
- Les protocoles utilisés dans l'IMS.
- La signalisation dans l'IMS : protocole SIP.
- Mécanismes de signalisation et des flux voix.
- Les composants SIP : UAC/UAS, agent, proxy server, redirect server, registrar server, gateways.
- Les messages SIP.
- Le routage SIP.
- Le futur de SIP.

4) Les systèmes 3G+

- Systèmes HSPA (HSDPA/HSUPA).
- Systèmes pour le multicast et le broadcast (MBMS, BCMCS, DVB).
- Systèmes OFDM (LTE).
- Positionnement de Wimax par rapport au LTE.
- Positionnement du sous-système IMS.
- Pérennité de la 3G+ face à l'arrivée de la 4G.

Stage pratique de 2 jour(s)
Réf : ITE

Participants

Informaticiens et ingénieurs réseaux souhaitant se spécialiser dans les réseaux mobiles à haut débit. Il s'adresse également aux responsables réseaux mobiles et responsables études désireux d'acquérir des connaissances approfondies sur le sujet.

Pré-requis

De bonnes connaissances dans le domaine des réseaux, de l'informatique ou des télécoms.

Prix 2012 : 1730€ HT

Eligible DIF

Dates des sessions

Paris

31 mai 2012, 20 sep. 2012
22 nov. 2012

Lyon

25 juin 2012

La génération LTE # 4G

Architectures, services, normes, choix techniques

OBJECTIFS

Cette formation vous permettra d'examiner les différentes solutions : se repérer dans l'évolution des technologies vers la 4G, les solutions pré-4G, ses solutions techniques, son avenir économique, les services 4G et son inclusion dans le " full IP ".

1) Architecture de la nouvelle génération

2) Les réseaux pré-4G

3) Les réseaux de mobiles 4G

4) La convergence et l'intégration dans Internet

5) Perspectives et conclusion

1) Architecture de la nouvelle génération

Introduction aux technologies de la 4G

- Les techniques OFDMA et SOFDMA de la 4G.
- Avantages et inconvénients par rapport à la 3G et le CDMA.
- Les antennes intelligentes.
- La radio cognitive.
- Les plans de fréquences.
- La diversité, le MIMO, le H-ARQ, FPS, AMC.

L'architecture des réseaux 4G

- Quelle architecture pour quelle application dans la 4G ?
- Le tout IP : les avantages et les inconvénients.
- La convergence fixe mobile : l'IMS (IP Multimedia Subsystem).
- Le coût de cette architecture.
- L'architecture du E-Node B.
- Les performances de cette nouvelle génération.

Le réseau coeur et le réseau d'accès

- Le réseau coeur et l'omniprésence du monde IP.
- La gestion de la mobilité.
- GMPLS dans le réseau coeur et le réseau d'accès.
- Le rôle du NGN (Next Generation Network).

2) Les réseaux pré-4G

Le réseau WiMAX

- Les réseaux WiMAX fixes et mobiles.
- Le WDSL et les performances à en attendre.
- L'IEEE 802.16e, les classes de service.
- Les opérateurs WiMAX fixe et les grandes opérations autour du WiMAX mobile.
- Le WiMAX phase 2.

Les normes des futures générations IEEE de type 4G

- La norme d'interconnexion des différents réseaux Wi-xx : l'IEEE 802.21 et le plan d'information.
- IEEE 802.22 et les réseaux régionaux pour la télévision interactive.
- Le dividende numérique : la vision américaine et la vision de l'ARCEP.
- Les nouvelles générations du Wi-Fi et leur impact sur la 4G.

3) Les réseaux de mobiles 4G

La quatrième génération (4G), HSOPA et LTE

- Les révolutions de la 4G : radio cognitive, antennes intelligentes, etc., les très hauts débits : plus de 100 Mbit/s en crête.
- La 4G avec le LTE (Long Term Evolution) et l'UMB (Ultra Mobile Broadband).
- Les premiers opérateurs 4G.
- Les terminaux 4G.
- Le WWI (World Wireless Initiative).
- Les tests du LSTI (LTE/SAE Trial Initiative).

La technologie 4G

Les terminaux

- L'E-UTRAN (Evolved UTRAN).
- L'EPC (Evolved Packet Core).
- Les interfaces S1 à S12.
- L'utilisation du spectre et la technique d'accès.
- L'approche multi-technologies.
- Les technologies Pico cell.

- L'impact de la 4G dans les réseaux de domicile.

Les services de la 4G

- Les services audio vidéo.
- Les services P2P et plus généralement T2T.
- Les nouveaux services Web et la sécurité.

4) La convergence et l'intégration dans Internet

La convergence fixe mobile

- L'IMS (IP Multimedia Subsystem) : la convergence IP # Télécom.
- L'architecture de l'IMS. Le groupe de travail TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking).
- L'intégration dans la 4G.

L'introduction d'IP dans la gestion de la mobilité

- La solution IP mobile : avantages et inconvénients. Les versions IPv4 et IPv6.
- IP mobile : définitions et problématique.
- IP cellulaire et la micromobilité.
- Comparaison avec la mobilité des réseaux cellulaires.
- Quelle solution pour la quatrième génération : Home Agent et Foreign Agent ou HLR/VLR ?
- L'optimisation de la route ; les smooth handovers.

Les réseaux ad hoc et MANET pour la 4G

- Les architectures de réseaux ad hoc.
- L'optimisation de l'utilisation du spectre.
- L'impact du monde IP sur les réseaux ad hoc.
- Les protocoles standardisés OLSR et AODV.

5) Perspectives et conclusion

- La place de la TNT (télévision numérique terrestre) dans la 4G.
- Les réseaux 4G et le #Full IP#.
- Les nouvelles architectures autonomiques pour le contrôle de la 4G.
- La virtualisation des équipements 4G.
- Les évolutions comme LTE-Advanced.

Exercice

Calcul du débit d'un réseau WiMAX. Implémentation d'un réseau WiMAX.