

Architecture de Réseaux

Aina Alain Patrick
AfNOG V
Dakar, 17-21 mai 2004
aalain@trstech.net

La loi de Ferguson en Architecture Réseau

Africa Network Operator's Group

“No amount of magic knobs will save a sloppily designed network”

Paul Ferguson—Consultant,
Cisco Systems

Conception Réseau et Architecture

Africa Network Operator's Group

- ...cela peut être critique
- ...cela peut contribuer au succès du réseau
- ... cela peut contribuer à sa faillite

Qu'est ce qu'un réseau bien architecturé

Africa Network Operator's Group

Principaux facteurs à prendre en considération :

- Infrastructure physique
- Topologie/protocole hiérarchique
- Redondance
- Agrégation d'adresses (IGP et BGP)
- Dimensionnement
- Implémentation de politique (cœur/périphérie)
- Management/maintenance/exploitation
- Coût

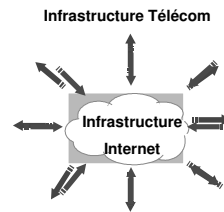
Vieux Monde contre Nouveau monde



Africa Network Operator's Group

En dépit du changement de relation Client-Fournisseur, les bases de la construction d'un réseau n'ont pas changées

Il y a des leçons apprises en 100 ans d'expérience que les ISPs peuvent apprendre des Opérateurs Télécom et les Opérateurs peuvent apprendre de l'expérience de croissance de +100% par an acquise par les ISPs



Outils conceptuels pour réseaux ISP qui affectent la topologie



Comment y arrive-t-on ?



Africa Network Operator's Group

“In the Internet area, reliability is becoming something you have to build, not something you buy. That's hard work, and it requires intelligence, skills and budget. Reliability is not part of the basic package.”

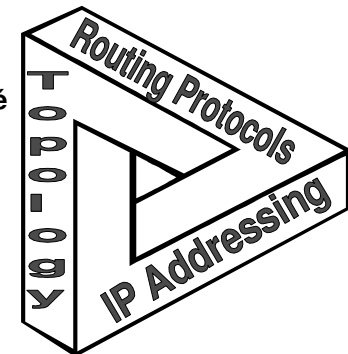
Joel Snyder – Network World Test Alliance 1/ 10/00
“Reliability: Something you build, not buy”

Concepts de base de scalabilité pour ISP



Africa Network Operator's Group

- Design Modulaire et Structuré
- Design Fonctionnel
- Design par tiers/hierarchique



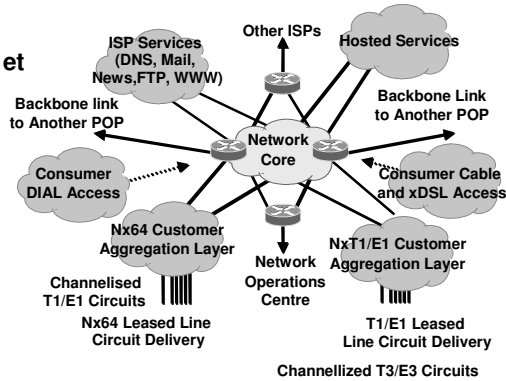
Design modulaire et structuré



Africa Network Operator's Group

Organiser le réseau en modules séparés et and répliquables

Coeur
POP
Hosting services
ISP Services
Support/NOC



Design Fonctionnel



Africa Network Operator's Group

- Une boîte ne peut pas tout faire—(même si des gens ont cherché à le faire)
- Chaque router/switch dans le réseau a une fonction bien définie
- Les différentes boîtes interagissent ensemble
- Les équipements sont sélectionnés et fonctionnellement placés dans le réseau en fonction de leurs points forts

Design modulaire et structuré



Africa Network Operator's Group

• La modularité rend un réseau plus dimensionnable

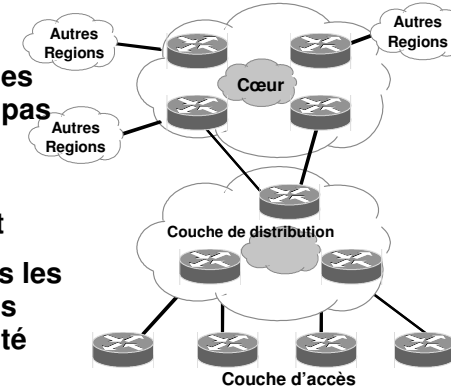
1. Design de petite unité de réseau qui sont branchées les unes aux autres
2. Chaque module est construit pour une fonction spécifique
3. Upgrader consiste à redimensionner un seul module, pas le réseau

Design reseau par tiers et hiérarchique



Africa Network Operator's Group

- Plat—les topologies maillées ne scale pas
- La hiérarchie est utilisée pour le dimensionnement
- Bon concept, mais les contours sont plus flous dans la réalité



Différentes Etapes

Africa Network Operator's Group

Définition des objectifs

Fonctionnalités

Disponibilité

Fiabilité

Flexibilité

Coût

Type de media

Africa Network Operator's Group

Média pour Les LAN

Ethernet

Ethernet commuté

Fast Ethernet

Gigabit Ethernet

Token Ring

FDDI

etc.

Différentes Etapes (2)

Africa Network Operator's Group

2- Choix de l'architecture modulaire et hierarchise

Noyau fédérateur

La Distribution

Accès

3- Le choix des médias

Type de media (2)

Africa Network Operator's Group

Média pour Les WAN

Modem Analogique

RNIS (BRI et PRI)

Les liaisons Spécialisées(LS)

Frame Relay

etc...

Traffic

Africa Network Operator's Group

Deux éléments sont à retenir dans le choix du media

La Fonction première de chaque composant réseau

Le type et la quantité de trafic espéré

Plusieurs règles concernant le ratio traffic local/traffic distant

Les règles de 80/20, 70/30, 90/10

Penser garder la max de traffic local

Les couches supérieures doivent gérer le trafic généré par les couches inférieures

Hubs, Switch et routeurs

Africa Network Operator's Group

Hubs

Répéteur multiport

Niveau 1

Disponible pour Ethernet, token Ring, FDDI

Manageable ou non

Constitue un domaine de collision et de broadcast

Bien connu, mais de moins en moins utilisé

Topologies Physiques

Africa Network Operator's Group

Plusieurs topologies pour la conception des réseaux

Point à Point

Maille

Anneau

Bus

Etoile

Hybride

Hubs, Switch et routeurs(2)

Africa Network Operator's Group

Switch ou routeur

Deux tendances

1- Les partisans des Ponts et Switch

Les routeurs sont chers

Les routeurs sont difficiles à configurer et à gérer

Les ponts et Switch sont plus rapides

2- Les partisans des routeurs

Les switch n'offrent pas un bon contrôle des réseaux(MAC)

Les Ponts et switch ne permettent pas aux réseaux de grandir (broadcast)

Hubs, Switch et routeurs(3)

Africa Network Operator's Group

Les deux tendances ont raison, mais pour des raisons d'extension des réseaux, les partisans des routeurs l'emportent.

Les routeurs ont un degré plus élevé de synthèse des données à cause des adresses assignées selon les topologies

Ils déplacent la décision de savoir si un routeur est nécessaire au niveau de l'émetteur au lieu de nécessiter que le routeur écoute tout le trafic sur tous les segments

Avantage d'un backbone de niveau 3



Africa Network Operator's Group

Control du trafic multicast et broadcast

Partage de charge

Pas de liens bloqués

Convergence rapide EIGRP/OSPF

Meilleure scalabilité globale

Adjacences de routeurs diminuées

Alors, Switch ou routeur

Africa Network Operator's Group

Les Switch ne sont tout de même pas à banir.

Les Switch offrent plus de "throughput" et une latence plus faible et sont faciles à configurer et sont moins chers

Les Switch servent à réduire les domaines de collision et augmentent ainsi la bande passante. Sont une solution pour les réseaux à accès partagé surchargés.

Et la redondance ?

Africa Network Operator's Group

"Le technicien de surface a tiré la prise..."

Pourquoi avait-il accès près de l'équipement?

Pourquoi ne s'en est-on aperçu qu'après?

Pourquoi cela a-t-il pris 6 semaines ?

Pourquoi l'alimentation n'était-elle pas sécurisée ?

Pourquoi le réseau n'était-il pas redondant?



pannes

Africa Network Operator's Group

Dernier élément important dans la conception

Assure la fiabilité et la disponibilité du réseau

Un moyen sûr d'augmenter le budget

Entre les deux extrémités, il faut un intermédiaire

Pas de redondance, pas de surcôt

Pleine redondance, budget doublé

Où a-t-on besoin de redondance ?

Identifier les points faibles et les sources possibles de pannes

Evaluer l'impact et la probabilité des pannes (Soyez réalistes)

Multiple niveaux de redondance



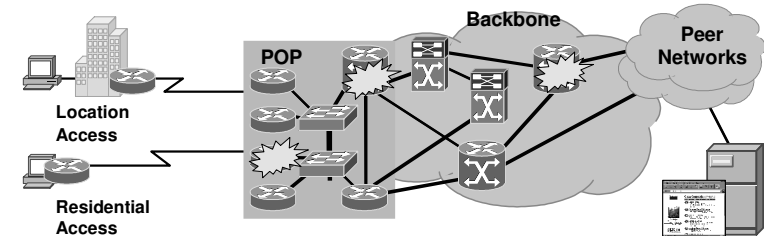
Africa Network Operator's Group

Objectifs

Impacter le moins possible le client final

Minimiser l'impact des fautes dans n'importe quelle partie du réseau

Le réseau doit résister à des fautes de niveau 2, 3, 4 et à des crash routeurs



pannes(2)

Africa Network Operator's Group

Une solution raisonnable peut consister en :

Faire une pleine redondance pour les points qui en ont vraiment besoin (Disponibilité 100% obligatoire)

Secourir les autres dans des délais raisonnables par des équipements en spare

Et les liaisons ?

Mêmes solutions que ci-dessus

En cas de pleine redondance, il faut décider :

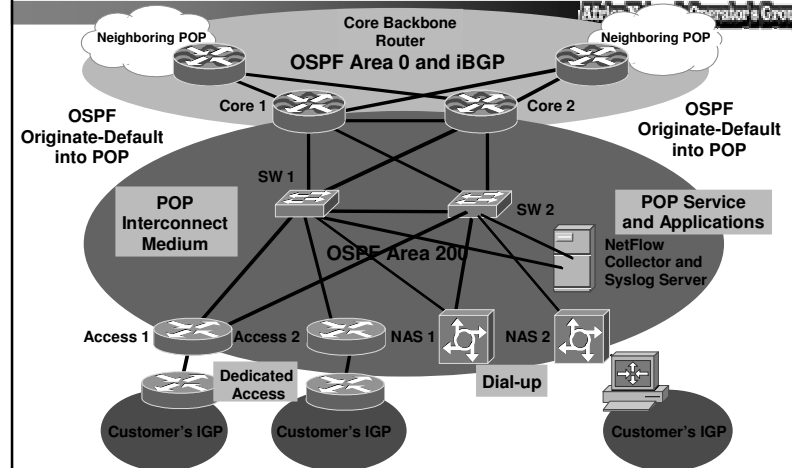
Une principale, Une backup

partage de traffic

Multiple niveaux de redondance



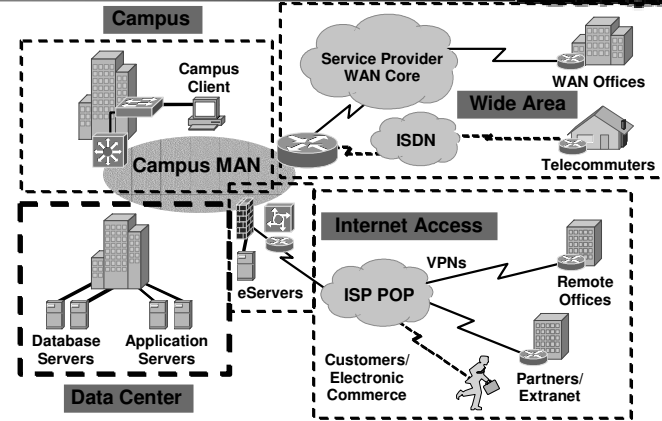
Africa Network Operator's Group



Conception et Technologies



Disponibilité du Data Center



LES BASES : Machines et

Environnement



Africa Network Operator's Group

Courant sécurisé

Refroidissement sécurisé

1:1 or N:1 redondance de cartes

Redondance de processeurs

Redondance de fond de panier

Contrôle de l'environnement

Câblage

Une mauvaise architecture



Africa Network Operator's Group

Un maillon faible

Un domaine de collision

Un domaine de sécurité

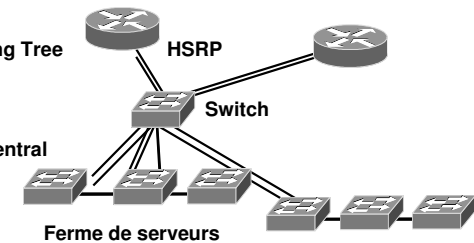
Convergence du Spanning Tree

Pas de traceroute

Pas de backup

Performance du switch central

Où est le firewall ?



Réseau d'entreprise

Une autre ...



Africa Network Operator's Group

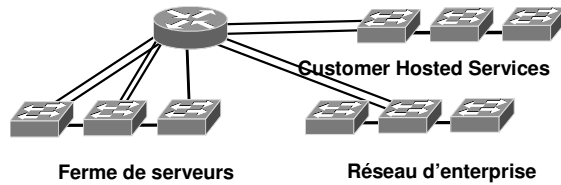
Simple à construire

La résilience est le problème du fabricant

Plus cher

Aucun routeur n'est résilient aux fautes logicielles

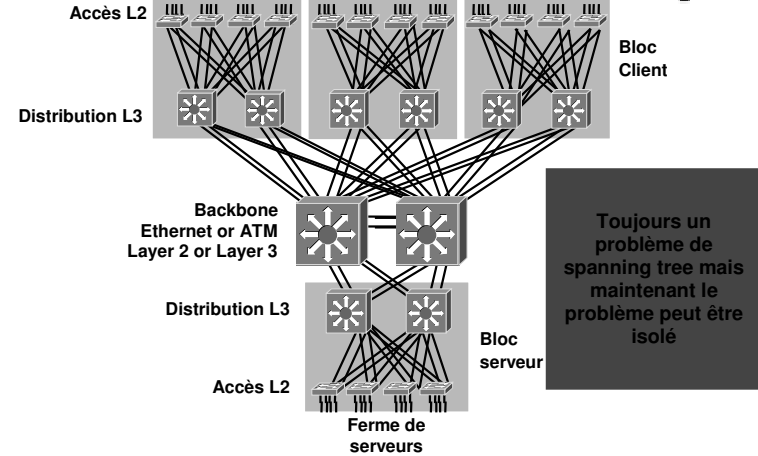
Vous avez toujours besoin d'un plus gros routeur



Un meilleur cœur de réseau



Africa Network Operator's Group

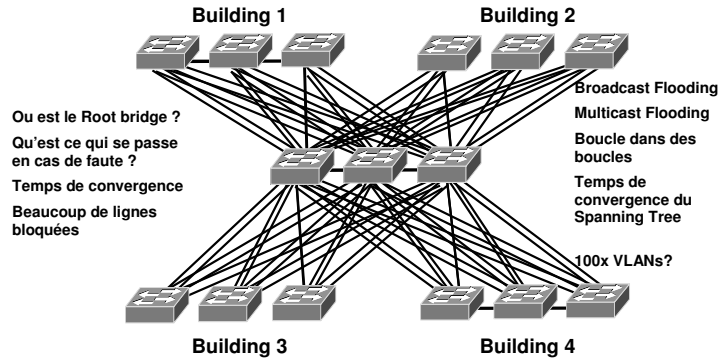


Encore pire



Africa Network Operator's Group

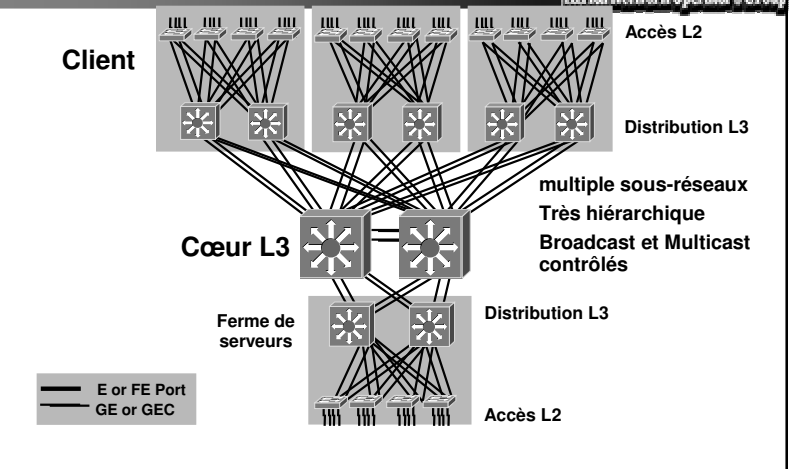
Éviter les réseaux niveau 2 Très maillé, Non-Déterministe

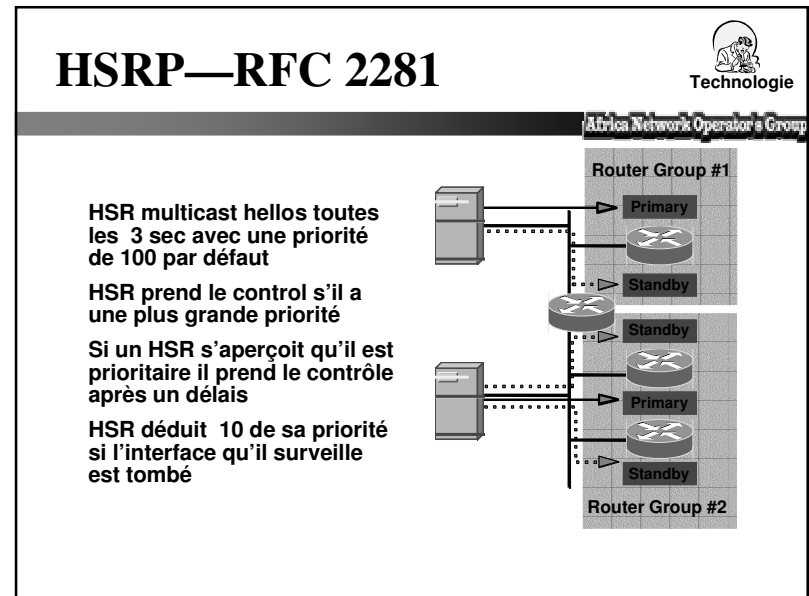
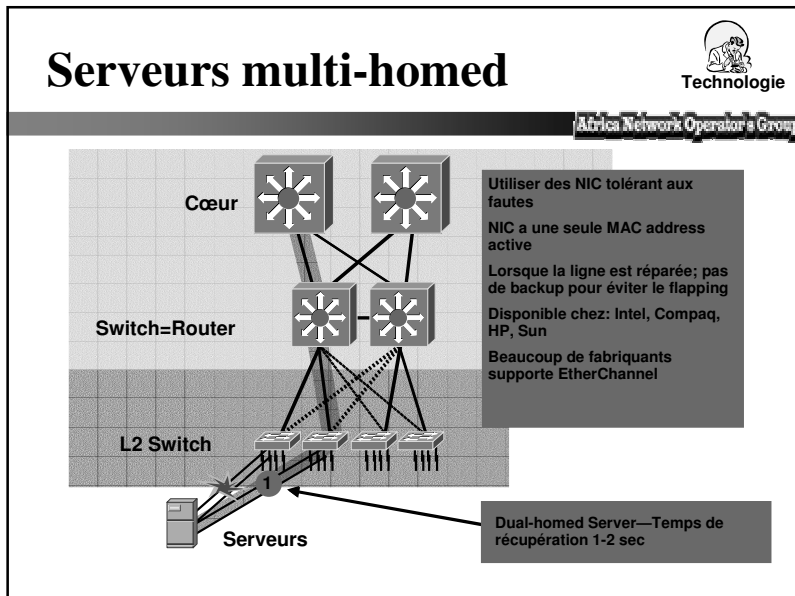
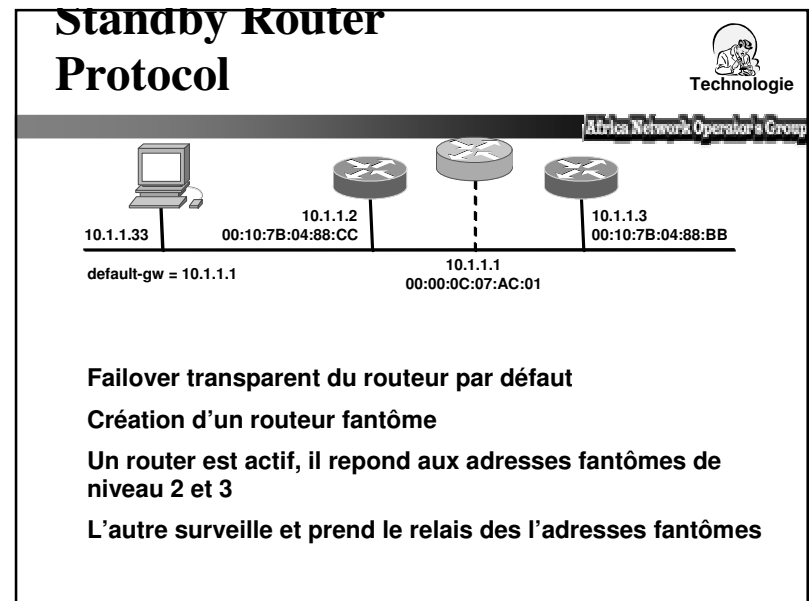
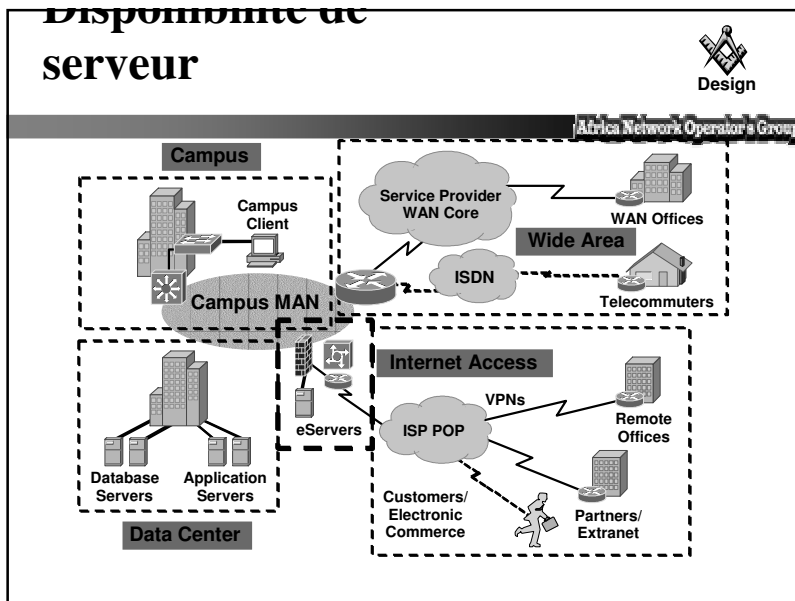


La meilleur architecture



Africa Network Operator's Group





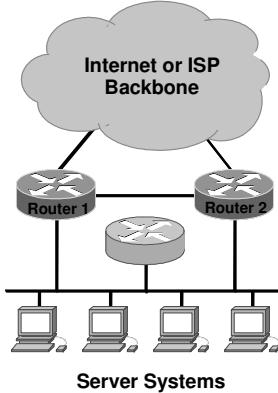
HSRP



Africa Network Operator's Group

```
Router1:
interface ethernet 0/0
bandwidth 128
ip address 169.223.10.1 255.255.255.0
standby 10 ip 169.223.10.254
```

```
Router2:
interface ethernet 0/0
bandwidth 1500
ip address 169.223.10.2 255.255.255.0
standby 10 priority 150 pre-empt delay 10
standby 10 ip 169.223.10.254
standby 10 track serial 0 60
```



Diversité de circuit



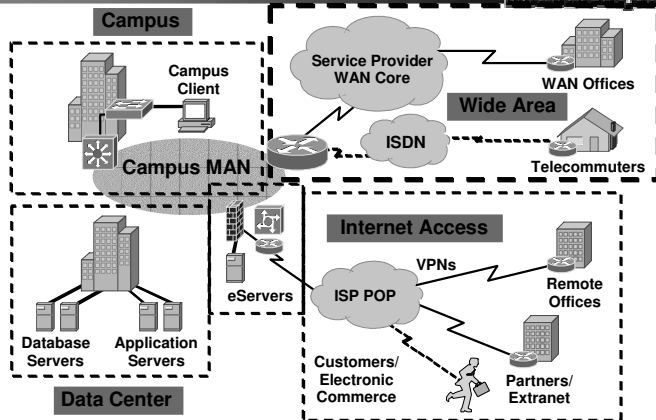
Africa Network Operator's Group

- Avoir plusieurs PVCs à travers le même port physique ne sert à rien
- Un port a plus de chance d'être défectueux qu'un seul PVC
- Utiliser des ports séparés; si possible sur des routeurs différents
- Essayez de demander à votre ISP de terminer vos lignes de backup sur des équipements différents

Disponibilité WAN



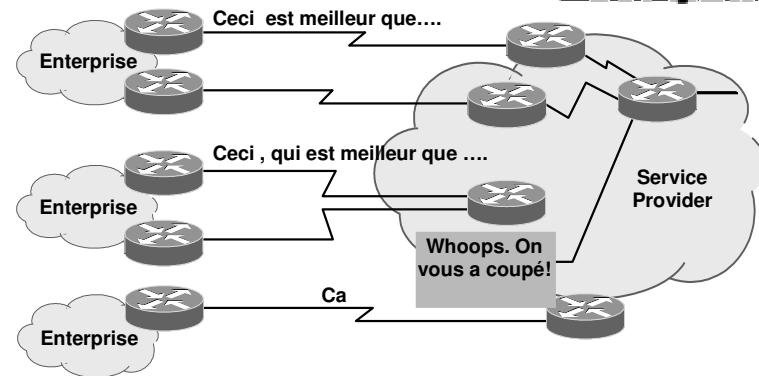
Africa Network Operator's Group



Diversité de circuit



Africa Network Operator's Group



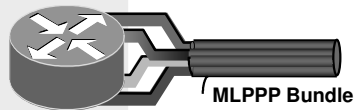
Utilisons MLPPP



Africa Network Operator's Group

```
interface Multilink1
ip address 172.16.11.1 255.255.255.0
ppp multilink
multilink-group 1
!
interface Serial1/0
no ip address
encapsulation ppp
ppp multilink
multilink-group 1
!
interface Serial1/1
no ip address
encapsulation ppp
ppp multilink
multilink-group 1
```

Employé avec une diversité de circuit; Multi-link PPP, fournit la redondance des lignes. Cela augmente votre bande passante



Partage de charge



Africa Network Operator's Group

- Il y a partage de charge lorsqu'un routeur a 2 (ou plus) chemins pour atteindre la même destination
- EIGRP permet le partage inégale de charge
- Le partage de charge peut être par paquet ou par destination
- Le partage de charge est une technique puissante car il permet un chemin alternatif si un routeur a une déficience

Partage de charge



Africa Network Operator's Group

- OSPF fait le partage de charge de manière égale par défaut
- EIGRP fait le partage de charge de manière égale par défaut, et peut être configuré pour partager la charge de manière inégale

```
router eigrp 111
network 10.1.1.0
variance 2
```

- Unequal-cost load-sharing n'est pas recommandé car il crée des problèmes de timing et de retransmissions

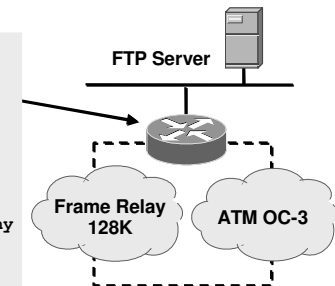
Policy-based Routing



Africa Network Operator's Group

Si vous avez des liens de coût différent et vous ne voulez pas utiliser unequal-cost load sharing, vous pouvez utiliser PBR pour envoyer le trafic basse priorité vers le lien le plus lent

```
! Policy map that directs FTP-Data
! out the Frame Relay port. Could
! use set ip next-hop instead
route-map FTP_POLICY permit 10
match ip address 6
set interface Serial1.1
!
! Identify FTP-Data traffic
access-list 6 permit tcp any eq 20 any
!
! Policy maps are applied against
! inbound interfaces
interface ethernet 0
ip policy route-map FTP_POLICY
```



Facteurs déterminant la convergence du protocole



Africa Network Operator's Group

- Taille du réseau
- Limitations du nombre de saut
- Arrangements des voisinages (cœur, bordure)
- Vitesse de la détection du changement
- Propagation des changements
- Design réseau : hiérarchie, summarization, redondance

Convergence



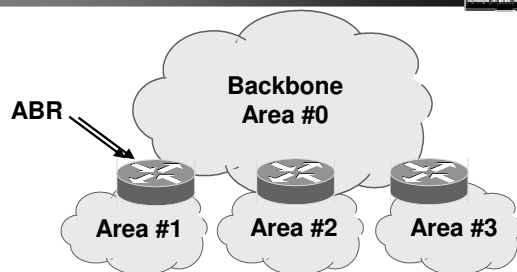
Africa Network Operator's Group

- Le temps de convergence du protocole de routage affecte la disponibilité de votre WAN
- Examiner si le design niveau 2 affecte l'efficacité au niveau 3

OSPF — Structure Hiérarchique



Africa Network Operator's Group

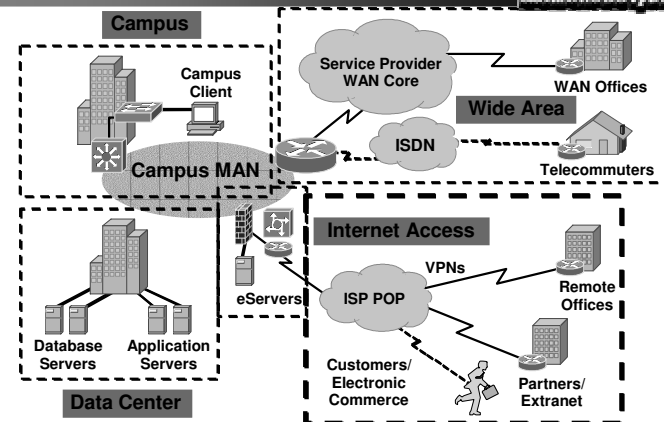


- La topologie d'une aire est invisible or de l'aire
LSA flooding reste dans l'aire
Le calcul SPF se passe indépendamment dans chaque aire

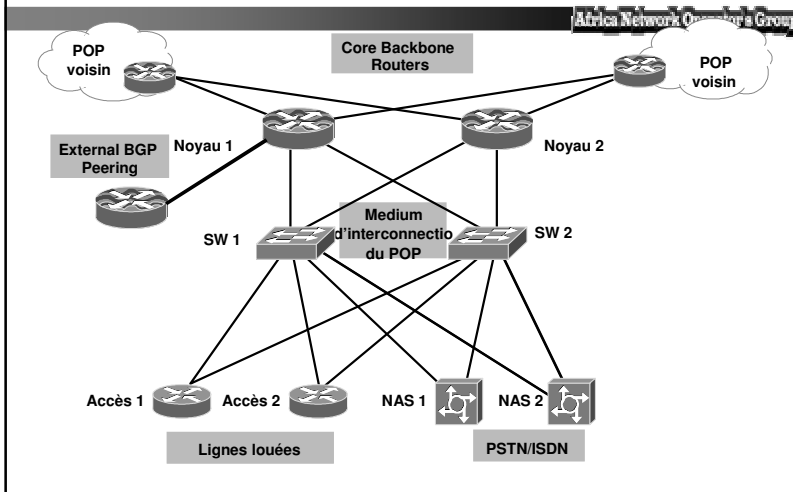
Disponibilité Internet



Africa Network Operator's Group



Design de Point de Presence (POP)



réseaux

Routeur : Logiciel ou matériel ?

Logiciel

Des PC sous Unix ou Win NT ou 2000 avec ou sans logiciel de routage gated, zebra etc.....

Moins chers,

Les PC peuvent servir à autres choses

Pas flexible,

Problèmes avec les OS et les autres services

Choix des équipements



Choix des équipements réseaux(2)

Matériel

Des équipements spécialisés avec processeur, mémoires (morte,vive), Interfaces et logiciels

Plus optimisé

Plus flexible

Chers

Critères de choix

Africa Network Operator's Group

Fonctionnalités

Interopérabilité

Fiabilité

Facilité de maintenance

Assistance du vendeur

Performance

Un routeur calcule des routes

Un routeur transfère des paquets entre Interfaces

Donc doit être bien dimensionné pour sa mission

Perception

Africa Network Operator's Group

Grand=meilleur



... Allant à 200 km/h

Critères de choix(2)

Africa Network Operator's Group

Deux éléments difficiles à mesurer entrent en compte

Le débit

Quantité de données que le routeur peut transférer dans un intervalle de temps.

Mesuré en paquets par second (PPS)

Généralement avec des paquets de 64 octets (le minimum)

La latence

Temps qu'un paquet passe à l'intérieur d'un routeur(en ms)

Caractéristiques des Media

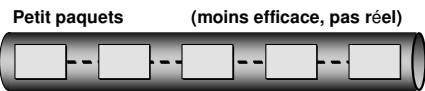
Africa Network Operator's Group

	IFG	Minimum Valid Frame	Maximum Valid Frame	Bandwidth
Ethernet	96 bits	64 Bytes	1,518 Bytes	10 Mbps
Fast Ethernet	96 bits	64 Bytes	1,518 Bytes	100 Mbps
FDDI	0	34 Bytes	4,500 Bytes	100 Mbps
Token Ring	4 bit	32 Bytes	16K Bytes	16 Mbps
BRI	0	24 Bytes	1500 Bytes	128 Kbps
PRI	0	24 Bytes	1500 Bytes	1.472 Mbps
T1	0	14 Bytes	4500 Bytes	1.5 Mbps
ATM	0	30 Bytes (AAL5)	16K Bytes (AAL5)	155 Mbps

Valeurs Théoriques

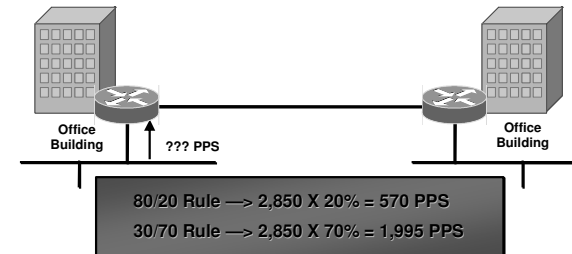
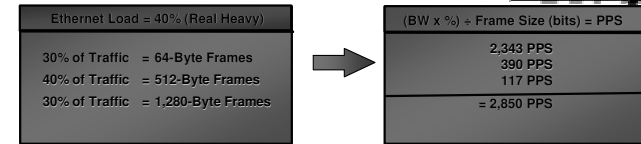
Africa Network Operator's Group

Bande passante ÷ taille des paquets = Performance Théorique



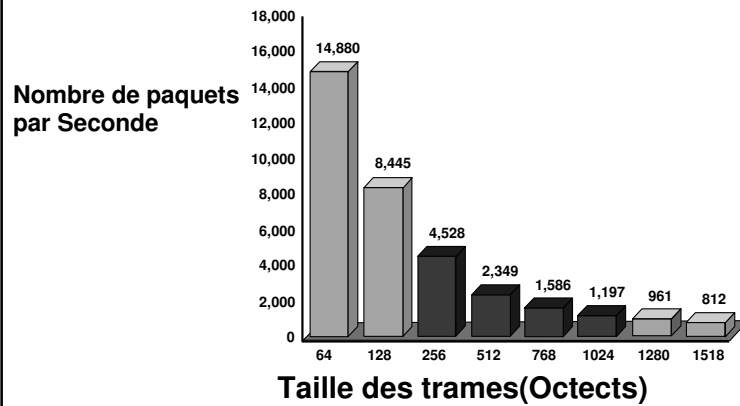
Analyse du trafic réel

Africa Network Operator's Group



Maximum Théorique PPS pour Ethernet

Africa Network Operator's Group



Critères de choix(3)

Africa Network Operator's Group

Max PPS théoriques pour certaines interfaces

Media	Bande passante	Taille minimum de paquet	Max PPS
Ethernet	10 Mbps	64 octets	14 880
Token Ring	16 Mbps	64 octets	24 691
FDDI	100 Mbps	64 octets	152 439
T1	1,544 Mbps	64 octets	3 300

Pour un routeur avec deux Ethernet et deux T1, Le max de paquets que ce routeur doit gérer est la somme des paquets sur toutes les interfaces divisée par 2:
 $(2 \times 14800 + 2 \times 3300) / 2 = 18100$ pps

Dans la pratique, il faut considérer 40% de ce trafic soit 7240 pps

Bonnes pratiques(1)



Africa Network Operator's Group

Utiliser les VLANs

Faites de l'agrégation de bande passante si nécessaire
Utiliser l'interface loopback

Son état ne change jamais

Offre un accès plus stable et sécurisé aux routeurs

Sert à déterminer le router-ID etc.....

Utiliser l'option description des interfaces

Aide à identifier et comprendre

N'oublier pas la commande bandwidth

Est utilisé par des IGP

La QoS(1)



Africa Network Operator's Group

Quelle application a besoin de QoS ? Comprendre les caractéristiques de l'application

1- Application sensible au délai et aux pertes(voix et video)

Utiliser du LLQ(low latency queuing) et priority queue

2- Application gourmande en bande passante (ftp et http)

Utiliser WRED, policing, traffic shaping, or class-based weighted fair queuing (CBWFQ) pour garantir la bande passante.

3- Les applications TCP

Utiliser WRED si les pertes de paquets causent retransmissions.

Si le trafic est UDP et ne retransmet pas, ne pas utiliser WRED.

Utiliser "Policing" si vous avez besoin de limiter la bande passante allouée à l'application.

Bonnes pratiques(2)



Africa Network Operator's Group

Eviter l'utilisation du "redistribute connected ou static"

au pire des cas utiliser les avec des route-map

Faites porter les préfixes de l'infrastructure par IGP

les loopbacks et les liens p-to-p entre les routeurs

Eviter d'injecter individuellement les préfixes d'accès dans IGP

ADSL,RTC,RNIS etc....

Faites porter les préfixes externes par BGP ou du statique

Clients et Internet

La QoS(2)



Africa Network Operator's Group

Créer les classes de services selon les critères Créer les politiques pour marquer les paquets Marquer les paquets en entrée Travailler de l'extrémité(edge) vers le noyau(core)



Créer les politiques pour traiter le trafic Faites des tests au labo avant le réel

Se connecter à Internet



Africa Network Operator's Group

Router vers Internet n'est pas significativement différent de router vers un autre WAN

S'assurer de la diversité des circuits

Utiliser HSRP et «track interface » pour les liens redondants

Optimiser le routage avec du partage de charge



Questions ?

24

Pour résumer

Africa Network Operator's Group

- Implémenter des réseaux IP fiable requière une combinaison d'un bon processus, d'un bon design et d'une bonne technologie
- Le procédure est le plus important

