# BIG-IP の物理構成と論理構成

BIG-IP
・物理構成
ワンアーム or ツーアーム
・特殊な論理構成
DSR(Direct Server Return/BIG-IP では nPath): あて先 MAC アドレス変換、node に Static ARP を設定

SNAT: x-forwarded-for にあるクライアント IP を使い、AP/Web がログにクライアントの IP を書き込む。

http://www.f5 networks.co.jp/pv_obj_cache/pv_obj_id_54382 D85 C9 C5239 C5 C53 A1 A8 A81673040 DC60400/filename/BIG-IP_TB_packet_flow.pdf
「BIG-IP のデプロイメントパターンとパケットフローについて」 pdf

参照
サーバ負荷分散入門 [ 大型本 ]
みやた ひろし ( 著 )

# ネットワーク機器の性能評価についての RFC

RFC 3511 ファイアウォール性能についての試測方法論 (Firewall)
RFC 2647 ファイアウォールパフォーマンス用語 (Firewall)
RFC 1242 ネットワーク相互接続デバイスのためのベンチマーキング用語 ( ルータ )
RFC 2544 ネットワーク相互接続装置のためのベンチマーク方法論 ( ルータ )
RFC 2285 LAN スイッチのためのベンチマーキング用語 ( スイッチ )
RFC 2889 LAN スイッチはベンチマーキング方法論 ( スイッチ )

# Fiddler (Web Debugging Proxy) Hack

Web アクセス専用のキャプチャツール
MS 専用 .Net 2.0 必須

実は Fiddler がすごすぎたので、機能まとめ紹介
http://blog.loadlimits.info/2009/09/%E5%AE%9F%E3%81%AFfiddler%E3%81%8C%E3%81%99%E3%81%94%E3%81%99%E3%81%8E%E3%81%9F%E3%81%AE%E3%81%A7%E3%80%81%E6%A9%9F%E8%83%BD%E3%81%BE%E3%81%A8%E3%82%81%E7%B4%B9%E4%BB%8B/

# C3550/3750 IOS イメージアップグレード (tar 形式 /archive コマンド )

IOS バージョン 確認
3550#sh ver

空き容量確認
3550#dir flash:

イメージだけ削除

# delete flash:c3550-i5q3l2-mz.121-9.EA1c.bin

イメージ ディレクトリと、その中のファイルをすべて削除するには、
# delete /force /recursive c3550-i5q3l2-mz.121-11.EA1

イメージのアップグレード
#archive download-sw ［ /leave-old-sw | /overwrite ｝ tftp://<tftp server ip>/<filename>
/leave-old-sw イメージを残す
/overwrite 上書きする。

ベリファイ
#verify c3550-i5q3l2-mz.121-13.EA1/c3550-i5q3l2-mz.121-13.EA1.bin

起動するイメージが変わっているかを確認
#sh boot

#conf t
(config#boot system flash:c3550-i5q3l2-mz.121-13.EA1/c3550-i5q3l2-mz.121-13.EA1.bin
# write mem
で変更する。

# reload

# sh ver
で確認

## VRF NAC アプライアンス

http://www.cisco.com/JP/support/public/mt/tac/106/1065385/nac-layer3-design-guide.shtml

## 無線 LAN セキュリティ

802.1x + でコンピュータ認証 (windows 独自実装 )
http://akiog.hmki.com/archives/2005/10/8021x_windows20.html

Windows で動作可能な無料の無線 LAN パケットキャプチャ「Omnipeek Personal」
http://gigazine.net/index.php?/news/comments/20071202_omnipeek_personal/

初心者管理者のための無線 LAN セキュリティ講座 【第 3 回】
http://enterprise.watch.impress.co.jp/cda/special/2005/01/20/3826.html

## Catalyst MAC アドレスから port 番号の特定方法

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00801c9199.shtml

## ドメイン用ツール

ネットブラウザ ++ というソフトを使用すれば、ネットワークに接続しているＰＣの IP アドレス・MAC アドレス・ＯＳのバージョン・コンピュータ名・PDC/BDC が調べられます。

私は「DomainView（フリーソフト)」を使用しております。

## SAN とストレージについて解説

2003 年
http://www.nic.ad.jp/ja/materials/iw/2003/proceedings/T27-1-1.pdf
2004 年
http://www.nic.ad.jp/ja/materials/iw/2004/proceedings/T20-1.pdf

## CCX (Wireless Cicso 対応 ) 解説

CCX
Cisco Compatible Extensions Client Devices
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html
http://www.cisco.com/web/partners/pr46 /pr147
/program_additional_information_new_release_features.html

## MIB 入手方法

特定のベンダー機器用の MIB ファイルを取得する必要がある場合、一般的な方法としてはインターネットを利用することが考えられます。ベンダーの公式 Web サイトから入手する方法が最善ですが、MIB ファイルを集約している Web サイトがいくつか存在します。
http://www.mibdepot.com/cgi-bin/downloads.cgi
http://www.oidview.com/mibs/detail.html
http://www.somix.com/software/mibs
http://www.hdopp.de/S-ManageWise-Body.html#mwmibs

## ICMP オプション

ICMP-info (ICMP type 15 code 0)
http://www.asahi-net.or.jp/~AA4T-NNGK/ipttut/output/icmpheaders.html

ICMP を使ったフィンガープリント (Xprobe)
http://itpro.nikkeibp.co.jp/members/ITPro/SEC_CHECK/20010921/1/

## Netscreen/SSG パスワード初期化方法

設定に行き詰ったら、初期化しましょう。
設定を色々いじると、設定のゴミが入ったり設定が複雑になります。潔くリセットしましょう。
心配なら、Config を保存しておけば、いつでも戻せますよ。

◆方法１　コマンドラインから
次の手順で行う。
「unset all」
確認メッセージがでるので、「y」
リセットする 「reset」
unset する前の設定を保存するか聞いてくるので、「no」
本当にリセットするか確認「y」

◆方法２　シリアル番号を入力
コンソールで接続し（Telnet は不可）、login と password にシリアル番号を入力する。

この機能は Asset Recovery という。この機能を停止させたいのであれば、以下のコマンドを入力する。
unset admin device-reset

◆方法３　ハード的に初期化する
この方法はちょっと難しいので、割愛。
何が難しいかというと、タイミングが難しい。

Juniper のサイトにて、SSG の設定の中に詳しい初期化が書かれてます。
ただし、9M ほどあるので注意してください。
http://www.juniper.co.jp/products_and_services/firewall_slash_ipsec_vpn/datasheets/fsssg5.pdf

**初期化方法 （シリアルナンバー） 】**

起動済みの NetScreen と管理端末をシリアルケーブルでコンソール接続します

ログイン名とパスワードに、機器のシリアル番号を入力します

質問メッセージには "y" を入力します

Lost Password Reset !!! You have initiated a command to reset the device to
factory defaults, clearing all current configuration and settings. Would you like to continue? y/[n] y
Reconfirm Lost Password Reset !! If you continue, the entire configuration of
the device will be erased. In addition, a permanent counter will be incremented
to signify that this device has been reset. This is your last chance to cancel
this command. If you proceed, the device will return to factory default configuration, which is: System IP: 192.168.1.1 ; username: netscreen, password: netscreen. Would you like to continue? y/[n] y
In reset ...

# Brocade SAN スイッチの設定

http://www.imasy.or.jp/~kommy/san/Zoning/Zoning.files/v3_document.htm
http://homepage1.nifty.com/~ayumi/article0003.html
http://homepage3.nifty.com/sony/sd/contents/san_cmd.htm
http://www-01.ibm.com/support/docview.wss?uid=std3430c6d82695fb0e949257408003c7902
http://hidamari.s45.xrea.com/lab/switch.html

http://support.express.nec.co.jp/care/user/N8406-019_020_8.pdf

http://www-01.ibm.com/support/docview.wss?uid=std358f4f513ab0f60424925729f000a3e87

http://www.brocadekorea.com/download/resource/53-0000231-03.pdf

## EAP バージョン 1.01 の証明書のガイド

PKI 証明書 (Windows CA での作成 ) のサンプル
http://www.cisco.com/JP/support/public/mt/tac/100/1004855/eap-v101-cert-guide.shtml#t10

## Catalyst で Uplink の障害検知、サーバとチーミングを使った連携

リンクステート トラッキングの設定
http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sw/cat29/2960cg5/chapter31/8603_04_31.shtml#60906

## HTTP 通信で、キャッシュのしかた

IE で自動プロキシ設定で Web アクセスできない。
EnableAutoProxyResultCache

HTTP 通信で、レスポンス 304、Etag、Last-Modified について
条件付き GET(Conditional GET)
http://as-is.net/blog/archives/000956.html

WinHTTP
http://www2.wbs.ne.jp/~kanegon/proxyconfig/readme.txt

## SMB 署名

CIFS 認証プロトコル仕様
http://www.monyo.com/technical/samba/translation/CIFS-Auth-Spec.ja.txt

MS-SMB の仕様書 セクション 3.1.5.1 Receiving Any Message
http://msdn.microsoft.com/en-us/library/cc246345(PROT.13).aspx

samba 3.0 での会話 (CIFS プロトコルのメーリングリスト )
http://archives.free.net.ph/message/20090210.151348.0cf779d5.ja.html
SMB 署名は AES256 のセッションキー (32byte) を使って署名を生成している。

SMB の署名は
SMB ヘッダ構造の予約領域に
UCHAR SecuritySignature[8](8 バイト ) に署名が記述される。

SMB 署名の計算は MD5 (MAC キー ) を使って
MAC( セッションキー、メッセージ本文 ) = SMB 署名 (8 バイト )

## CiscoWorks で SNMPv3（認証と暗号化）

CiscoView 6.1.7 以上が必要
http://www.cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html
上記の、User Guide for CiscoView 6.1.7 を参照。

6.1.7 より古かったら暗号化はサポートしていない！

Readme for CiscoWorks LAN Management Solution 3.0 December 2007 Update on Windows
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html
ここも参照

## Cisco RADIUS(AAA) debug コマンド

IOS ルータ設定例でトンネル伝送する分割の NEM モードの EzVPN(EzVPN でリソースの制限 )
http://www.cisco.com/JP/support/public/mt/tac/100/1004762/ezvpn-svr-rtr.shtml

http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfppp.html#wpxref24802
debug radius
debug radius brief

debug aaa accounting
show aaa servers

debug radius
show accounting
show radius statistics

## WPAD(proxy.pac)

IIS で拡張子 pac ファイルの MIME 登録
http://www.atmarkit.co.jp/fwin2k/win2ktips/888iismime/iismime.html

## スパム対策

http://www.soi.wide.ad.jp/class/20050041/slides/01/
http://www.soi.wide.ad.jp/class/20060031/slides/11/

## ファイル添付

## IEEE 802.11i-2004 と 802.1X-2004 の規格書

## ネットワーク関連の規格書入手方法

http://itpro.nikkeibp.co.jp/article/COLUMN/20051115/224581/?ST=nettech

## Cisco で Appletalk 確認方法

AEP(appletalk ping, routing,zone)

DDR を使用した AppleTalk over ISDN
http://www.cisco.com/JP/support/public/mt/tac/100/1000789/appletalk_isdn_ddr.shtml

## NetWare(IPX/SPX) プロトコル

検証環境
クライアント
Win2000/XP/2003 に「Novell NetWare Client for Windows XP/2000」を追加 (Novell からフリーで提供 )
サーバ
1.NetWare6.5 (30 日評価版 ) を Novell から DL する。（アカウント登録必要 )

```
Netware6.5 は IPX に対応 ( おそらく Linux ベース )
```

2.Linux で、IPX/SPX を使い、「mars-nwe(NetWare エミュレータ )」をインストールしてテストする。

参考
http://euc.jp/os/nwprimer.ja.html
http://euc.jp/os/rpl.ja.html

## AppleTalk プロトコル

プロトコルフォーマットとレイヤ解説
http://www.protocols.com/pbook/appletalk.htm

参考図書 抜粋 (http://www.istc.kobe-u.ac.jp/contents/about_istc/mage/mage25/ishisada/ishisada.html)
32. Gursharan S.Sidhu ほか著 , アキューコミュニケーションズ訳:『Inside Appletalk：日本語版』, アジソン・ウェスレイ・パブリッシャーズ・ジャパン ,1992.9, 1 冊.
33. Apple Computer.Inc：『AppleTalk network system overview：日本語版』, アジソン・ウェスレイ・パブリッシャーズ・ジャパン ,1990.10,200 p.
Macintosh のネットワークプロトコルとして有名な AppleTalk ですが、分かりやすい図書がないのが残念です。おおまかにつかむのには［33］あたりしか見あたりません。後に出てくる［43］でも、ほぼ同程度の知識は得られます。
43. 奥田一人：『Mac ＋ UNIX ネットワーキング』, 工学図書 ,1995.8,373p

## VRRP と HSRP について

http://1x4x9.net/2008/07/hsrpvrrp.html

## Cisco の推奨設定 (OSPF の解説 )

http://tiida.cocolog-nifty.com/netblog/cat1674494/index.html

## Cisco SNMP Link Up/Down Trap

簡易ネットワーク管理プロトコル (SNMP) トラップの理解
http://www.cisco.com/JP/support/public/mt/tac/100/1000453/snmp_trap.shtml
Cisco 標準の SNMP Link Up/Down Trap は IETF 標準とは別物です。
CISCO-GENERAL-TRAP (MIB) を参照

## Syslog RFC3164 ファシリティとサーベリティの値

http://www.amris.co.jp/netdocs/rfc3164_j.html

## IOS フューチャとリリース番号

White Paper： Cisco IOS リファレンス ガイド
http://www.cisco.com/japanese/warp/public/3/jp/service/tac/620/1-j.shtml

## WLC から LAP( 無線 AP) への IP 設定方法 WLAPP

LWAPP 解説
http://itpro.nikkeibp.co.jp/article/COLUMN/20080128/292241/

無線 LAN WLC の設定 その 1
http://www.n-study.com/network/2007/10/lan_wlc_1.html

Wireless LAN コントローラ (WLC) 設計および機能 FAQ
http://www.cisco.com/JP/support/public/mt/tac/100/1005593/wlc-design-ftrs-faq.shtml

LWAPP トラフィック研究
http://www.cisco.com/JP/support/public/mt/tac/101/1019989/lwapp-traffic-study.shtml

Lightweight アクセス ポイントの制御 (WLC のマニュアル )
http://cco-rtp-1.cisco.com/japanese/warp/public/3/jp/service/manual_j/wr/wlc/wlccg4/chapter06/15301_01_6.shtml
http://cco-rtp-1.cisco.com/japanese/warp/public/3/jp/service/manual_j/wr/wlc/wlccg4/chapter07/15301_01_7.shtml#32267

**注意：WLC には内部 DHCP サーバと外部 DHCP サーバの設定がある。**
**このうち、内部 DHCP サーバの機能に DHCP オプション 43 を付加する機能はない！**

Lightweight Cisco Aironet アクセス ポイント用 DHCP オプション 43 の設定例
http://www.cisco.com/JP/support/public/mt/tac/100/1005529/dhcp-option-43.shtml

## Catalyst SNMP での管理方法の推奨事項

http://www.cisco.com/JP/support/public/ht/tac/100/1007782/103-j.shtml
http://www.cisco.com/JP/support/public/mt/tac/100/1001683/103.shtml
http://www.cisco.com/en/US/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml
Cisco IOS が動作している Catalyst 6500/6000 シリーズおよび Catalyst 4500/4000 シリーズ スイッチのベスト プラクティス
http://www.cisco.com/japanese/warp/public/3/jp/service/tac/473/185-j.shtml
キーワード CCO/ catalyst 6500 mib chassis best

## スイッチのバックプレーンは半二重通信が主だった

クロスバースイッチ方式
http://amecoro.seesaa.net/article/101028405.html

## ping 中断

ping 中断
Ctrl-Shift-6

telnet セッション終了
Ctrl-Shift-6 x

## Cisco CPU 使用率で閾値設定

SNMP を使った Cisco IOS デバイス上の CPU 使用率収集方法
http://www.cisco.com/JP/support/public/ht/tac/100/1007918/collect_cpu_util_snmp-j.shtml

キーワード： Cisco Process MIB CPU しきい値テーブルの設定
http://www.cisco.com/japanese/warp/public/3 /jp/service/manual_j/sw/me/me34 easscg2 /chapter28 /9639 _03_28.shtml

ベースライン プロセス： ベスト プラクティス White Paper
閾値設定するときの良い方法
http://cco.cisco.com/JP/support/public/ht/white_paper/100/1006434/HAS_baseline-j.shtml

## DHCP

・DHCP による、Web Proxy の自動割り当ての動作

通常は、端末の URL に proxy.pac( 実態は Web サーバ上の JavaScript) を取りに行かせる。
http://www.atmarkit.co.jp/fwin2k/win2ktips/031autoproxy/autoproxy.html

## Cisco

・Catalyst の IOS で IP Base では OSPF に対応していない。

おそらく IP Service 以上が必須。
White Paper： Cisco IOS リファレンス ガイド
http://www.cisco.com/JP/support/public/mt/tac/100/1002212/1.shtml

・Catalyst3550 でポートミラーでタグ VLAN でキャプチャする方法

ハードウェア :
IOS:

Cat3550 の config 設定後にスイッチの再起動が必要！
再起動していないと、タグが除去されて、パケットが転送される。

## plala の NTP サーバ

| | 東日本エリアの方 | 西日本エリアの方 |
|---|---|---|

| | | |
|---|---|---|
| プライマリ | ntp1.plala.or.jp | ntp2.plala.or.jp |
| セカンダリ | ntp2.plala.or.jp | ntp1.plala.or.jp |

## SSL キャプチャ

SSL 通信を複合化するツール

ssldump

ただし、ローカルの通信において有効だと思う