APPENDIX A

アドレス、プロトコル、およびポートの概要

この付録では、次の項目に関する簡単な説明を示します。

- IP アドレスおよびサブネット マスク
- プロトコルおよびアプリケーション
- TCP ポートおよび UDP ポート
- ICMP タイプ

IP アドレスおよびサブネット マスク

ここでは、ACE での IP アドレスの使用方法について説明します。IP アドレスは、ドット付き 10 進表記で表記される 32 ビットの数値です。2 進数から 10 進数に変換された 4 つの 8 ビット フィールド（オクテット）が、ドットで区切られて表記されます。IP アドレスの最初の部分はホストが属するネットワークを表し、後ろの部分はそのネットワークの特定のホストを表します。ネットワーク番号フィールドはネットワーク プレフィクスと呼ばれます。特定のネットワークに属するすべてのホストは同じネットワーク プレフィクスを共有しますが、それぞれ固有のホスト番号が必要です。クラスフル IP の場合、アドレスのクラスによってネットワーク プレフィクスとホスト番号との境界の位置が定められています。

ここで説明する内容は、次のとおりです。

クラス

IP ホスト アドレスは、クラス A、クラス B、クラス C の 3 種類のアドレス クラスに分けられます。クラスによって、ネットワーク プレフィクスとホスト番号との境界が 32 ビット アドレス内のそれぞれどこに置かれるかが固定的に定義されています。クラス D アドレスは、マルチキャスト IP 用に予約されています。各クラスについて次に説明します。

- クラス A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）では、第 1 オクテットだけをネットワーク プレフィクスとして使用します。
- クラス B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）では、第 2 オクテットまでをネットワーク プレフィクスとして使用します。
- クラス C アドレス（192.0.0.xxx ～ 223.255.255.xxx）では、第 3 オクテットまでをネットワーク プレフィクスとして使用します。

クラス A アドレスには 16,777,214 個のホスト アドレスが含まれ、クラス B アドレスには 65,534 個のホストが含まれるため、サブネット マスクを使用してこれらの大規模なネットワークを小さいサブネットに分けることができます。

プライベート ネットワーク

ネットワークに多数のアドレスが必要で、それらのアドレスをインターネットでルーティングする必要がない場合、Internet Assigned Numbers Authority（IANA; インターネット割り当て番号局）の推奨するプライベート IP アドレスを使用することができます（RFC 1918 を参照）。アドバタイズしてはいけないプライベートネットワークとして、次のアドレス範囲が指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクによって、1 つのクラス A、B、または C ネットワークを複数のネットワークに変換することができます。サブネット マスクを使うと、ホスト番号のビットをネットワーク プレフィクスに追加して、拡張ネットワーク プレフィクスを作成できます。たとえば、クラス C ネットワーク プレフィクスは、常に IP アドレスの最初の 3 つのオクテットで構成されます。しかしクラス C 拡張ネットワーク プレフィクスは、第 4 オクテットの一部も使用します。

サブネット マスクについては、ドット付き 10 進表記の代わりに 2 進表記を使うと理解しやすくなります。サブネット マスクのビットは、インターネット アドレスと 1 対 1 で対応しています。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィクスに含まれる場合、サブネット マスクのビットは 1 になります。
- IP アドレス内の対応するビットがホスト番号に含まれる場合、サブネット マスクのビットは 0 になります。

例 1 — クラス B アドレス 129.10.0.0 の第 3 オクテット全部を、ホスト番号ではなく拡張ネットワーク プレフィクスの一部として使用する場合、サブネットマスク 11111111.11111111.11111111.00000000 を指定します。サブネット マスクによって、クラス B アドレスがクラス C アドレスと同等になり、ホスト番号は最後のオクテットだけで構成されます。

例 2 — 第 3 オクテットの一部だけを拡張ネットワーク プレフィクスに使用する場合、サブネット マスクを 11111111.11111111.11111000.00000000 のように指定します。この例では、第 3 オクテットの 5 ビットだけが拡張ネットワーク プレフィクスに使用されます。

サブネット マスクは、ドット付き 10 進マスクまたは / *ビット*（「スラッシュ *ビット数*」）マスクで表記できます。例 1 の場合、ドット付き 10 進マスクを使用すると、2 進表記の各オクテットを 10 進数に変換して 255.255.255.0 になります。/ *ビット数*マスクの場合は、1 の個数を指定するので、/24 になります。例 2 の場合、10 進数だと 255.255.248.0、/ ビットだと /21 になります。

また、第 3 オクテットの一部を拡張ネットワーク プレフィクスに使うことで、複数のクラス C ネットワークを 1 つの大きなネットワーク（または*スーパーネット*）にまとめることができます。192.168.0.0/20 はその一例です。

ここで説明する内容は、次のとおりです。

- サブネット マスクの判別
- サブネット マスクで使用するアドレスの判別

サブネット マスクの判別

必要なホスト数に適したサブネット マスクを判別するには、表 A-1 を参照してください。

表 A-1　ホスト、ビット、およびドット付き 10 進マスク

ホスト[1]	/ ビット マスク	ドット付き 10 進マスク
16,777,216	/8	255.0.0.0（クラス A ネットワーク）
65,536	/16	255.255.0.0（クラス B ネットワーク）
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8,192	/19	255.255.224.0
4,096	/20	255.255.240.0
2,048	/21	255.255.248.0
1,024	/22	255.255.252.0

表 A-1　ホスト、ビット、およびドット付き 10 進マスク（続き）

ホスト[1]	/ ビット マスク	ドット付き 10 進マスク
512	/23	255.255.254.0
256	/24	255.255.255.0（クラス C ネットワーク）
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255（単一ホスト アドレス）

1. サブネットの先頭と末尾の番号は予約されています。単一のホストを表す /32 は除きます。

サブネット マスクで使用するアドレスの判別

ここでは、クラス C およびクラス B 規模のネットワークでサブネット マスクを使用する場合に、使用できるネットワーク アドレスを判別する方法について示します。

- クラス C 規模のネットワーク アドレス
- クラス B 規模のネットワーク アドレス

クラス C 規模のネットワーク アドレス

ホスト数が 2 ～ 254 のネットワークでは、第 4 オクテットは 0 から始まるホスト アドレス数の倍数になります。次に、192.168.0.x の 8 ホストのサブネット（/29）の例を示します。

マスク /29（255.255.255.248）のサブネット	アドレスの範囲[1]
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31

マスク /29（255.255.255.248）のサブネット	アドレスの範囲[1]
…	…
192.168.0.248	192.168.0.248 ～ 192.168.0.255

1. サブネットの先頭と末尾のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 または 192.168.0.7 は使用できません。

クラス B 規模のネットワーク アドレス

ホスト数が 254 ～ 65,534 のネットワークでサブネット マスクを使用する場合、使用できるネットワーク アドレスを判別するには、すべての拡張ネットワーク プレフィクスについて第 3 オクテットの値を判別する必要があります。たとえば、10.1.*x*.0 などのアドレスをサブネット化するとします。このアドレスの 第 2 オクテットまでは、拡張ネットワーク プレフィクスに使用されるので固定です。第 4 オクテットはすべてのビットがホスト番号に使用されるので、0 になります。

第 3 オクテットの値を判別するには、次の手順に従います。

ステップ 1　65,536（第 3 および第 4 オクテットを使用した場合の総アドレス数）を必要なホスト アドレスの数で割り、ネットワークから作成できるサブネット数を算出します。

たとえば、65,536 をホスト数 4096 で割るとサブネット数は 16 になります。

したがって、クラス B 規模のネットワークには、それぞれ 4096 のアドレスを含む 16 のサブネットが存在できることになります。

ステップ 2　256（第 3 オクテットに含まれる値の数）をサブネット数で割り、第 3 オクテットの値の倍数を判別します。

この例では、256 ÷ 16 = 16 になります。

第 3 オクテットは、0 から始まる 16 の倍数になります。

したがって、ネットワーク 10.1 の 16 のサブネットは、次のようになります。

マスク /20（255.255.240.0）のサブネット	アドレスの範囲[1]
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
…	…
10.1.240.0	10.1.240.0 ～ 10.1.255.255

1. サブネットの先頭と末尾のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 または 10.1.15.255 は使用できません。

プロトコルおよびアプリケーション

ここでは、ACE の設定に関連するプロトコルとアプリケーションについて説明します。ACE はルーテッド モードの場合、マルチキャスト プロトコルまたはルーティング プロトコルを通過させません。

使用できるリテラル値は、**ah**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**pcp**、**snp**、**tcp**、**udp** です。プロトコルを番号で指定することもできます。

表 A-2 に、プロトコルのリテラル値に対応する番号を示します。

表 A-2　プロトコルのリテラル値

リテラル	番号	説明
ah	51	IPv6 の Authentication Header（AH; 認証ヘッダー）、RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）
esp	50	IPv6 の Encapsulated Security Payload（ESP）、RFC 1827
gre	47	Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）
icmp	1	Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）、RFC 792
igmp	2	Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）、RFC 1112
igrp	9	Interior Gateway Routing Protocol（IGRP）
ip	0	Internet Protocol（IP; インターネット プロトコル）
ipinip	4	IP-in-IP カプセル化
nos	94	Network Operating System（NOS; ネットワーク OS）、Novell NetWare
pcp	108	Payload Compression Protocol（PCP）
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol（TCP）、RFC 793
udp	17	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、RFC 768

IANA の Web サイトで、プロトコル番号をオンラインで参照することができます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートおよび UDP ポート

表 A-3 に、リテラル値およびポート番号を示します。どちらも ACE のコマンドで入力できます。次の点に注意してください。

- ACE では SQL*Net にポート 1521 を使用します。これは、Oracle で SQL*Net に使用されるデフォルト ポートです。ただし、この値は IANA のポート割り当てとは合致しません。
- ACE は、ポート 1645 と 1646 で Remote Authentication Dial-In User Service（RADIUS）を受信します。RADIUS サーバが標準ポート 1812 と 1813 を使用する場合は、**aaa-server**、**radius-authport**、および **aaa-server radius-acctport** コマンドを使用して、ACE がこれらのポートを使用するよう設定します。
- Domain Name System（DNS; ドメイン ネーム システム）アクセス用のポートを割り当てるには、**dns** ではなく **domain** を使用します。**dns** キーワードは、**dnsix** のポート番号に変換されます。

IANA の Web サイトで、ポート番号をオンラインで参照することができます。

http://www.iana.org/assignments/port-numbers

表 A-3　ポートのリテラル値

リテラル	プロトコル	番号	説明
aol	TCP	5190	AOL
bgp	TCP	179	Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、RFC 1163
biff	UDP	512	メール システムがユーザに新しいメールを受信したことを通知するために使用
bootpc	UDP	68	Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
bootps	UDP	67	BOOTP サーバ
chargen	TCP	19	Character Generator
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	**exec** と類似するが、**cmd** には自動認証がある
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding（CTIQBE）
daytime	TCP	13	日時、RFC 867
discard	TCP, UDP	9	廃棄
domain	TCP, UDP	53	DNS
dnsix	UDP	195	DNSIX セッション管理モジュール監査リダイレクタ
echo	TCP, UDP	7	エコー
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	File Transfer Protocol（FTP; ファイル転送プロトコル）、制御ポート
ftp-data	TCP	20	FTP、データ ポート
gopher	TCP	70	Gopher
https	TCP	443	HyperText Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）、SSL
hostname	TCP	101	NIC ホスト ネーム サーバ
ident	TCP	113	Ident 認証サービス
imap4	TCP	143	Internet Message Access Protocol（IMAP）バージョン 4
irc	TCP	194	Internet Relay Chat（IRC; インターネット リレー チャット）プロトコル

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
isakmp	UDP	500	Internet Security Association and Key Management Protocol（ISAKMP）
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol（LDAP）
ldaps	TCP	636	LDAP（SSL）
lpd	TCP	515	Line Printer Daemon（LPD）— プリンタ スプーラ
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	MobileIP エージェント
nameserver	UDP	42	ホスト ネーム サーバ
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nntp	TCP	119	Network News Transfer Protocol（NNTP）
ntp	UDP	123	Network Time Protocol（NTP; ネットワーク タイム プロトコル）
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pcanywhere-data	TCP	5631	pcAnywhere データ
pim-auto-rp	TCP, UDP	496	Protocol Independent Multicast（PIM）、逆経路フラッディング、dense（稠密）モード
pop2	TCP	109	Post Office Protocol（POP）— バージョン 2
pop3	TCP	110	POP — バージョン 3

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	RADIUS
radius-acct	UDP	1646	RADIUS（アカウンティング）
rip	UDP	520	Routing Information Protocol（RIP）
secureid-udp	UDP	5510	SecureID over UDP
smtp	TCP	25	Simple Mail Transport Protocol
snmp	UDP	161	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）
snmptrap	UDP	162	SNMP ― トラップ
sqlnet	TCP	1521	Structured Query Language（SQL; 構造化照会言語）ネットワーク
ssh	TCP	22	Secure Shell（SSH; セキュア シェル）
sunrpc (rpc)	TCP, UDP	111	Sun Remote Procedure Call（RPC; リモート プロシージャ コール）
syslog	UDP	514	システム ログ
tacacs	TCP, UDP	49	TACACS+（Terminal Access Controller Access Control System Plus）
talk	TCP, UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	Trivial File Transfer Protocol（TFTP）
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）
who	UDP	513	Who
whois	TCP	43	Who Is

表 A-3　ポートのリテラル値（続き）

リテラル	プロトコル	番号	説明
www	TCP	80	World Wide Web（WWW; ワールドワイド ウェブ）
xdmcp	UDP	177	X Display Manager Control Protocol（X DMCP）

ICMP タイプ

表 A-4 に、ACE のコマンドで入力できる ICMP タイプの番号および名前を示します。

表 A-4　ICMP タイプ

ICMP 番号	ICMP 名
0	echo-reply（エコー応答）
3	unreachable（到達不能）
4	source-quench（ソース クエンチ）
5	redirect（リダイレクト）
6	alternate-address（代替アドレス）
8	echo（エコー）
9	router-advertisement（ルータ アドバタイズメント）
10	router-solicitation（ルータ送信要求）
11	time-exceeded（時間超過）
12	parameter-problem（パラメータ問題）
13	timestamp-request（タイムスタンプ要求）
14	timestamp-reply（タイムスタンプ応答）
15	information-request（情報要求）
16	information-reply（情報応答）
17	mask-request（マスク要求）
18	mask-reply（マスク応答）
31	conversion-error（変換エラー）
32	mobile-redirect（モバイル リダイレクト）