

情報工学実験1

「ネットワーク管理コマンド活用」

組 名： 1 班
学籍番号： 095707B
氏 名： 大城佳明
提出日： 2010年5月11日

目次

1	課題1	4
1.1	実行結果	4
1.2	解析	4
1.3	ping の応答	5
1.3.1	例	5
1.3.2	考察	5
1.4	ping の応答 (フィルター)	5
1.4.1	実行結果	5
1.4.2	考察	5
2	課題2	6
2.1	実行結果	6
2.1.1	8184bytes 送った場合	6
2.1.2	8185bytes 送った場合	6
2.2	考察	6
2.3	理由	7
2.3.1	制限をかけない場合どのようなことが起こるか。	7
2.3.2	DoS 攻撃	7
2.3.3	結論	7
3	課題3	8
3.1	実行結果	8
3.2	解析	8
3.3	正しく表示されない	9
4	課題4	9
4.1	コマンド「-i」オプション	9
4.1.1	「-i」オプションとは	9
4.1.2	実行結果	9
4.1.3	説明	10
4.1.4	考察	10
4.2	コマンド「-r」オプション	11
4.2.1	「-r」オプションとは	11
4.2.2	実行結果	11
4.2.3	説明	11
4.3	コマンド「-s」オプション	12
4.3.1	「-s」オプションとは	12
4.3.2	実行結果	12
4.3.3	説明	13
4.4	コマンド「-l」オプション	14
4.4.1	「-l」オプションとは	14
4.4.2	実行結果	14
4.4.3	説明	14
4.4.4	考察	15

5	課題5	15
5.1	実行結果「ifconfig (インターフェイス名)」	15
5.2	説明	16
5.3	実行結果「ifconfig -a」	17
5.4	考察	17
6	課題6	18
6.1	変更前	18
6.2	実行	18
6.3	変更後	18
7	課題7	19
7.1	追加	19
7.1.1	変更前	19
7.1.2	実行	19
7.1.3	変更後	20
7.2	削除	20
7.2.1	変更前	20
7.2.2	実行	20
7.2.3	変更後	21
8	課題8	21
8.1	設定前	21
8.2	実行	22
8.3	設定後	22
9	課題9	22
9.1	正引き	22
9.1.1	対話モード	23
9.1.2	非対話モード	23
9.2	逆引き	23
9.2.1	対話モード	23
9.2.2	非対話モード	24
10	課題10	24
10.1	SOA レコード	24
10.1.1	実行結果	24
10.1.2	説明	25
10.2	NS レコード	25
10.2.1	実行結果	25
10.2.2	説明	25
10.3	MX レコード	25
10.3.1	実行結果	25
10.3.2	説明	25

11	課題 1 1	26
11.1	実行前	26
11.2	実行結果	26
11.3	考察	26
12	課題 1 2	27
12.1	課題 9 の内容	27
12.1.1	host コマンド	27
12.1.2	dig コマンド	27
12.2	課題 1 0 の内容	28
12.2.1	host コマンド	28
12.2.2	dig コマンド	29
12.3	課題 1 1 の内容	29
12.3.1	host コマンド	29
12.3.2	dig コマンド	30

1 課題 1

各自のコンピュータから他のコンピュータへ以下の ping コマンド実行し、表示される結果について説明せよ。また、もし相手のコンピュータが正しくネットワークに接続されているのに ping 応答が帰ってこない場合は、その理由を考察せよ。

1.1 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ ping -c3 nirai
02 PING nirai.ie.u-ryukyu.ac.jp (133.13.48.2): 56 data bytes
03 64 bytes from 133.13.48.2: icmp_seq=0 ttl=63 time=6.239 ms
04 64 bytes from 133.13.48.2: icmp_seq=1 ttl=63 time=4.328 ms
05 64 bytes from 133.13.48.2: icmp_seq=2 ttl=63 time=3.150 ms
06 — nirai.ie.u-ryukyu.ac.jp ping statistics —
07 3 packets transmitted, 3 packets received, 0% packet loss
08 round-trip min/avg/max/stddev = 3.150/4.572/6.239/1.273 ms
```

1.2 解析

- 02 PING nirai.ie.u-ryukyu.ac.jp (133.13.48.2): 56 data bytes について詳しく説明する。
 - 「nirai.ie.u-ryukyu.ac.jp」は ping した先のホスト名である。
 - 「(133.13.48.2)」は ping した先の IP アドレスである。
 - 「56 data bytes」は送る ICMP パケットの容量である。
- 03 64 bytes from 133.13.48.2: icmp_seq=0 ttl=63 time=6.239 ms について詳しく説明する。
 - 「64 bytes」は「133.13.48.2」の IP アドレスから返って来たパケットである。
 - 送ったパケット (58 data bytes) よりも 8 byte 多いのはネットワーク層に送る時に IP ヘッダ部分がついたためである。
 - 「icmp_seq=0」はシーケンス番号といい、どの ping に応答したかを示している。
 - 「ttl=63」について詳しく説明する。
 - 「Time To Live」の略
 - 存在可能時間という意味である。
 - パケットが永遠に存在することを防ぐために設定される値で、ルータを一つ通過する度に一つ減る。
 - TTL の値が間違いなら、それぞれのパケットが異なったルートを通っていること示す。
 - 「time=6.239ms」は送信して返答までに 6.239 ミリ秒かかったこと示している。
- 03~05 は ping を 3 回繰り返した事を示している。
- 07 3 packets transmitted, 3 packets received, 0% packet loss について詳しく説明する。
 - 「3 packets transmitted」とは 3 回パケットを送った事を示している。
 - 「3 packets received」は 3 回送れた事を示している。
 - 「0% packet loss」は送れなかった確率の事で、0%なら全て送れたことを示している。
- 「08 round-trip min/avg/max/stddev = 3.150/4.572/6.239/1.273 ms」はそれぞれランドトリップタイムの最短時間/平均時間/最長時間/平均偏差を示している。

1.3 ping の応答

1.3.1 例

○返ってくる	×返って来ない
yahoo.co.jp	自宅 (学内から自宅)
mixi.co.jp	cc.u-ryukyu.ac.jp (1 回だけ○)
cao.co.jp (内閣府)	kantei.co.jp (首相官邸)
whitehouse.gov (ホワイトハウス)	senete.gov (アメリカ合衆国上院)

1.3.2 考察

1. 考えられる原因

- (a) 相手先ノードが死んでいる。
- (b) 経路の途中にあるいずれかのルータがパケットを正しく中継していない。
- (c) ファイアウォールで ping を禁止している。
- (d) 相手によってブロックされている。

2. 自宅へ ping 出来なかったのは (c) の原因ではないかと考えられる。

3. cc.u-ryukyu.ac.jp には 1 回だけ許可が許される設定がされているのではないと思われる。

4. cao と kantai の違いは国内向けか海外向けかで変わるのではないと思われる。

5. 海外向けの場合は ping に制限をかけないと、国内向けと違って閲覧する人が多いため、回線がパンクして重くなる可能性があるので送れなかったと思われる。

1.4 ping の応答 (フィルター)

1.4.1 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ ping -c3 au.kddi.com
02 PING au.kddi.com (61.200.220.161): 56 data bytes
03 36 bytes from 61.200.161.238: Communication prohibited by filter
04 Vr HL TOS Len ID Flg off TTL Pro cks Src Dst
05 4 5 00 5400 ae93 0 0000 31 01 a84e 10.0.14.94 61.200.220.161
06 — au.kddi.com ping statistics —
07 3 packets transmitted, 0 packets received, 100% packet loss
```

1.4.2 考察

1. 03 の「Communication prohibited by filter」からわかるように、フィルターがかかって ping が出来ない。

2. 05 より ping の出来る IP アドレスと出来ない IP アドレスがあると思われる。

2 課題2

課題1と同様に、他のコンピュータへpingコマンドを実行する際、以下のようにパケットサイズをデフォルト値ではなく、より大きなサイズにした場合、エコー要求を送る相手のコンピュータによってエコー応答が返ってくる場合とそうでない場合がある。パケットサイズの違いによってエコー応答が返ってくる場合とそうでない場合の実例を示し、そうなる理由を考察せよ。

2.1 実行結果

2.1.1 8184bytes 送った場合

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ ping -c3 -s 8184 nirai.ie.u-ryukyu.ac.jp
02 PING nirai.ie.u-ryukyu.ac.jp (133.13.48.2): 8184 data bytes
03 8192 bytes from 133.13.48.2: icmp_seq=0 ttl=63 time=9.398 ms
04 8192 bytes from 133.13.48.2: icmp_seq=1 ttl=63 time=10.462 ms
05 8192 bytes from 133.13.48.2: icmp_seq=2 ttl=63 time=11.070 ms
06 — nirai.ie.u-ryukyu.ac.jp ping statistics —
07 3 packets transmitted, 3 packets received, 0% packet loss
08 round-trip min/avg/max/stddev = 9.398/10.310/11.070/0.691 ms
```

2.1.2 8185bytes 送った場合

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ ping -c3 -s 8185 nirai.ie.u-ryukyu.ac.jp
02 PING nirai.ie.u-ryukyu.ac.jp (133.13.48.2): 8185 data bytes
03 ping: sendto: Message too long
04 ping: sendto: Message too long
05 ping: sendto: Message too long
06 — nirai.ie.u-ryukyu.ac.jp ping statistics —
07 3 packets transmitted, 0 packets received, 100% packet loss
```

2.2 考察

1. 実行結果からわかるように8184bytesのパケットでは送れたが、8185bytesのパケットでは送れなかった。
2. 8184bytesについて詳しく説明する。
 - (a) ICMPパケットを8184byte送っているが実際は送るのはIPヘッダがあるので8192bytesである。
 - (b) $8192\text{bytes} = 2^3\text{kbytes} = 8\text{kbytes}$ である。
 - (c) 8kbytes以下でしかICMPパケットは送れない事がわかる。
3. nirai.ie.u-ryukyu.ac.jp以外にも送れるパケットは同じなのか調べてみた。
 - (a) yahoo.co.jp...8184(8192)bytess
 - (b) gogle.co.jp...8184(8192)bytes
 - (c) mixi.co.jp...8184(8192)bytes

(d) youtube...64(72)bytes

実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ ping -c3 -s 65 youtube.com
02 PING youtube.com (74.125.45.100): 65 data bytes
03 72 bytes from 74.125.45.100: icmp_seq=0 ttl=46 time=205.830 ms
04 wrong total length 92 instead of 93
05 72 bytes from 74.125.45.100: icmp_seq=1 ttl=46 time=206.070 ms
06 wrong total length 92 instead of 93
07 72 bytes from 74.125.45.100: icmp[_seq=2 ttl=46 time=206.991 ms
08 wrong total length 92 instead of 93
09 — youtube.com ping statistics —
10 3 packets transmitted, 3 packets received, 0% packet loss
11 round-trip min/avg/max/stddev = 205.830/206.297/206.991/0.500 ms
```

4. 制限がかけられていなければこの PC からは 8184bytes 送れる。

2.3 理由

2.3.1 制限をかけない場合どのようなことが起こるか。

1. システムやネットワークに大量のトラフィックを生じると、正当なネットワーク トラフィックが流れない状態になる。
2. クライアントとサーバの間の接続を中断させて、サービスにアクセスできないよう状態になる。
3. IP で許容される最大サイズ (65,535 バイト) より大きなパケットがデバイスに送信した場合。受信側のシステムがクラッシュする原因となる。

2.3.2 DoS 攻撃

1. 攻撃は通常、組織の機能を麻痺させることを目的として行われる。
2. 個々のコンピュータまたはコンピュータ群に対して行われる積極的な攻撃である。
3. 攻撃のターゲットとなり得るのは、エンドユーザ システム、サーバ、ルータ、ネットワーク リンクである。
4. DoS 攻撃は 2 種類ある。
 - (a) SYN (同期) フラッド
 - (b) Ping of Death (PoD)

2.3.3 結論

1. クラッシュや DoS 攻撃などを防ぐためにはネットワークに確実に保護する必要がある。
2. 送れるパケットに制限をかける必要がある。

3 課題3

各自のコンピュータから他のコンピュータ（できれば学科外のコンピュータ）へ traceroute コマンド実行し、表示される結果について説明せよ。なお、課題1の ping と同様の理由で、traceroute の結果が正しく表示されない場合があるため、本課題は ping エコー応答があるコンピュータに対して行うこと。

3.1 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ traceroute cyberbb.com
02 traceroute to cyberbb.com (128.121.122.35), 64 hops max, 40 byte packets
03 1 10.0.15.254 (10.0.15.254) 1.165 ms 0.855 ms 2.405 ms
04 2 133.13.48.254 (133.13.48.254) 1.510 ms 1.517 ms 1.438 ms
05 3 133.13.254.57 (133.13.254.57) 1.238 ms 1.214 ms 1.244 ms

< 06~16 省略 >

17 14 * * *
18 15 ae-2.r20.lsanca03.us.bb.gin.ntt.net (129.250.3.125) 149.900 ms 149.136 ms 149.070 ms
19 16 as-0.r21.snjsca04.us.bb.gin.ntt.net (129.250.4.96) 159.043 ms 162.309 ms 158.580 ms
20 17 ae-0.r20.snjsca04.us.bb.gin.ntt.net (129.250.2.96) 163.784 ms 159.027 ms 233.602 ms
21 18 ae-2.r20.mlpsca01.us.bb.gin.ntt.net (129.250.5.6) 159.116 ms 341.422 ms 159.389 ms
22 19 * * *
23 20 ae-0.r00.mlpsca01.us.wh.verio.net (129.250.26.161) 159.554 ms 159.008 ms 158.608 ms
24 21 ge-25.a0354d.mlpsca01.us.wh.verio.net (128.121.129.90) 159.885 ms 158.817 ms 158.902 ms
25 22 cyberbb.jp (128.121.122.35) 159.548 ms 159.828 ms 158.168 ms
```

3.2 解析

- 02 traceroute to cyberbb.com (128.121.122.35), 64 hops max, 40 byte packets について詳しく説明する。
 - 「traceroute to cyberbb.com」は traceroute をした先のホスト名である。
 - 「(128.121.122.35)」は traceroute した先の IP アドレスである。
 - 「64 hops max」は最大で 64 の経路情報を表示する事を示している。
 - 「40 byte packets」は 40 byte packets 送る事を示している。
- 03 1 10.0.15.254 (10.0.15.254) 1.165 ms 0.855 ms 2.405 ms について詳しく説明する。
 - 最初の「1」は順序番号を示している。
 - 「10.0.15.254」はホスト名を示しているが、無い場合は IP アドレスを表示する。
 - 「(10.0.15.254)」は IP アドレスを表示している。
 - 「1.165 ms 0.855 ms 2.405 ms」は3つのパケットのラウンドトリップタイムを表示している。
 - それぞれ1往復目、2往復目、3往復目を示している。
- 最後の番号が「22」なので経路は22個のルーターを通過して来ることがわかる。

3.3 正しく表示されない

- 17,22 の「***」について詳しく説明する。
 - (a) traceroute はそれぞれのルータから ICMP Time Exceed エラー 4 を受け取る事によって経路を表示している。
 - (b) ルータからエラーが返らず、traceroute コマンドがタイムアウトしている場合もある。
 - (c) セキュリティ上の要件から ICMP パケットをフィルタしている場合もある。
 - (d) 何度やっても同じ結果が起きたので (c) の可能性が高い。
- おもに ISP の管理するルータで多いようだ。

4 課題4

各自のコンピュータで、netstat コマンドの「-i」「-r」「-s」「-l」オプションについて実行例を示し、表示される結果について説明せよ。

4.1 コマンド「-i」オプション

4.1.1 「-i」オプションとは

1. インターフェイス別のパケット統計を表示する。
2. 送受信パケットの総数やエラーの数などが表示する。

4.1.2 実行結果

01	Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs	Coll
02	lo0	16384	<Link#1>		146533	0	146533	0	0
03	lo0	16384	localhost	fe80::1	146533	-	146533	-	-
04	lo0	16384	localhost	::1	147464	-	147464	-	-
05	gif0*	1280	<Link#2>		0	0	0	0	0
06	stf0*	1280	<Link#3>		0	0	0	0	0
07	en0	1500	<Link#4>	00:23:df:ab:28:98	0	0	0	0	0
08	en1	1500	<Link#5>	00:23:6c:91:c7:e9	806019	0	595158	0	0
09	en1	1500	yoshiaki-os	fe80::223:6cff:fe	806019	-	595158	-	-
10	en1	1500	10/20	10.0.14.94	806019	-	595158	-	-
11	en1	1500	2001:2f8:1c	2001:2f8:1c:d051:	806019	-	595158	-	-

< 12~16 省略 >

4.1.3 説明

1. Name : ネットワークインターフェイス名

gif	仮想デバイス。IPv6 と IPv4 間など、違う IP 間でのトンネリングを可能にする。
stf	仮想デバイス。IPv6 から IPv4 へのカプセル化を可能にする。Six To Four。
トンネリング	ネットワーク上のある二点間を仮想的に直接接続を確立する事。
en	イーサネットデバイス。en0 が有線で en1 が無線。
lo	ループバックデバイス。
fw	FireWire

2. Mtu : 一回に送信できるパケットサイズの上限
3. Network : ネットワークアドレス
4. Address : ホスト名、IP アドレス
5. Ipkts : 起動してからの受信パケット数
6. Ierrs : 起動してからの入力エラー数
7. Opkts : 起動してからの送信パケット数
8. Oerrs : 起動してからの送信エラー数
9. Coll : 起動してから検出されたコリジョン数

4.1.4 考察

1. 実行した PC の IP アドレスは「10.0.14.94」である。
 - (a) 「10.0.14.94」は 10 にあることがわかる。
 - (b) ネットワーク名は「10/20」であることがわかる。
 - (c) 受信パケット数は「806019」であることがわかる。
 - (d) 送信パケット数は「595158」であることがわかる。
 - (e) エラーは発生していない。
2. 実行した PC の MAC アドレスは「00:23:6c:91:c7:e9」である。
 - (a) 「00:23:6c:91:c7:e9」は 08 にあることがわかる。
 - (b) IP アドレスの値と一緒にあることがわかる。
3. ネットに繋がっていなかった場合

(a) 実行結果

01	Name	Mtu	Network	Address	Ipkts	Ierrs	Opkts	Oerrs	Coll
02	lo0	16384	<Link#1>		147299	0	147299	0	0
03	lo0	16384	localhost	fe80::1	147299	-	147299	-	-
04	lo0	16384	127	localhost	147299	-	147299	-	-
05	lo0	16384	localhost	::1	147299	-	147299	-	-
06	gif0*	1280	<Link#2>		0	0	0	0	0
07	stf0*	1280	<Link#3>		0	0	0	0	0
08	en0	1500	<Link#4>	00:23:df:ab:28:98	0	0	0	0	0
09	en1	1500	<Link#5>	00:23:6c:91:c7:e9	805866	0	594933	0	0
< 10~13 省略 >									

(b) en1 が少なくなっている。

(c) IP アドレスがなくなっていることがわかる。

(d) 09 より mac アドレスはあることがわかる。

4.2 コマンド「-r」オプション

4.2.1 「-r」オプションとは

1. ネットワークのルーティング情報を表示する。

4.2.2 実行結果

01	Routing tables							
02	Internet:							
03	Destination	Gateway	Flags	Refs	Use	Netif	Expire	
04	default	10.0.15.254	UGSc	85	8	en1		
05	10/20	link#5	UCS	5	0	en1		
06	10.0.5.112	0:23:6c:91:c7:e7	UHLW	0	294	en1	724	
07	10.0.6.88	f8:1e:df:e8:83:e	UHLW	0	0	en1	1126	
08	10.0.13.95	0:23:6c:91:cc:2	UHLW	0	80	en1	800	
09	10.0.14.94	localhost	UHS	0	0	lo0		
10	10.0.15.254	0:7:4f:c8:6f:fc	UHLW	85	21	en1	492	
11	10.0.15.255	link#5	UHLWb	2	84	en1		
< 12~23 省略 >								

4.2.3 説明

1. 02 はネットワークのルーティング情報を表示する。

(a) Internet : Pv4 のルーティング情報。

(b) Internet6 : IPv6 のルーティング情報。

2. Destination : 宛先ネットワークまたはホスト名
3. Gateway : ゲートウェイ
4. Flags : 経路の特性。

U	ルーティングが有効
H	対象がホスト
G	対象はゲートウェイ
D	動的に変更されるルーティング
S	静的に設定されたルーティング

5. Refs : 今現在このルーティング情報を参照しているコネクション数
6. Use : この経路を経由して送信されたパケット数
7. Netif : 送信ネットワークインタフェース名
8. Expire : ルーティング情報の有効期限

4.3 コマンド 「-s」 オプション

4.3.1 「-s」 オプションとは

1. TCP、UDP、IP、ICMP における内部統計情報を全て表示する。
2. 各プロトコルごとの IN/OUT パケット数やエラー数などの詳細。

4.3.2 実行結果

```

01  tcp:
02      1246679  packets sent
03          202604 data packets (93393317 bytes)
04          2104 data packets (1303352 bytes) retransmitted
05          0 resends initiated by MTU discovery
06          515345 ack-only packets (25035 delayed)
07          0 URG only packets
08          1 window probe packet
09          447076 window update packets
10          182676 control packets
11      1761015  packets received
12          233575 acks (for 91464639 bytes)
13          36245 duplicate acks
14          0 acks for unsend data
15          1488333 packets (1852566906 bytes) received in-sequence
16          2641 completely duplicate packets (2614438 bytes)
17          46 old duplicate packets
18          165 packets with some dup. data (11307 bytes duped)

      < 19~248 省略 >

```

4.3.3 説明

1. 01 tcp:はプロトコルを示している。
2. 省略されているが「tcp」以外にも 11 個のプロトコルの統計情報が表示されている。
3. 表示されているプロトコルを一つ一つ説明する。

tcp	<ul style="list-style-type: none"> ・ ネットワーク層の IP と、セッション層以上のプロトコルの橋渡しをする。 ・ 低速だが信頼性が高い。
udp	<ul style="list-style-type: none"> ・ ネットワーク層の IP と、セッション層以上のプロトコルの橋渡しをする。 ・ 高速だが信頼性が低い。
ip	<ul style="list-style-type: none"> ・ アドレッシングやルーティングの方法を規定するプロトコル。 ・ インターネットの基礎部分となる重要な役割を持つ。
icmp	<ul style="list-style-type: none"> ・ ip のエラーメッセージや制御メッセージを転送するプロトコル。 ・ ping や traceroute などが利用する。
igmp	<ul style="list-style-type: none"> ・ IP と同じネットワーク層プロトコルである。 ・ IP マルチキャストで配送を受けるために構成されるホストのグループを制御する。
ipsec	<ul style="list-style-type: none"> ・ インターネット暗号通信を行うためのプロトコル。 ・ IP データグラムの発信元が正しいことを保証する。 ・ 改ざんされていないことを保証する。
ip6 icmp6 ipsec6	<ul style="list-style-type: none"> ・ ip,icmp,ipsec の IPv6 版。 ・ 使用頻度は、ほとんど変わらない。
rip6	<ul style="list-style-type: none"> ・ 隣接ホストと経路情報を交換し、経路を決定するルーティングプロトコル
pfkey	<ul style="list-style-type: none"> ・ USAGI による手動鍵設定ツール ・ 暗号化のためのプロトコル

4. 02～10 はパケットの送信ことを示している。
 - (a) 03 より約 20 万パケットを送信する事がわかる。
 - (b) 04 は再送数である。
 - (c) 06 は ACK だけの数（遅延）である。
 - (d) 07 は URG だけの数である。
 - (e) 08 はウインドウ検査数である。
 - (f) 09 はウインドウ更新数である。
 - (g) 10 は制御パケット数である。
5. 11～18 はパケットの受信を示している。
 - (a) 12 は ACK 数（バイト数）である。
 - (b) 13 は重複した ACK の数である。
 - (c) 14 は未送信データ ACK の数である。
 - (d) 15 は正順数（バイト数）である。
 - (e) 16 は完全重複数（バイト数）である。
 - (f) 18 は部分重複数（バイト数）である。
6. とても長いので省略してある。

4.4 コマンド「-l」オプション

4.4.1 「-l」オプションとは

1. 接続待ち (listen) 状態にあるソケットのみを表示します。

4.4.2 実行結果

01	Active Internet connections								
02	Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)			
03	tcp4	0	0	10.0.14.94.63512	naha.ie.u-ryukyu.nntp	ESTABLISHED			
04	tcp4	0	0	10.0.14.94.62667	p1065-ipbf07yama.34471	ESTABLISHED			
05	tcp4	78	0	10.0.14.94.58792	naha.ie.u-ryukyu.nntp	CLOSE_WAIT			
06	tcp4	0	0	192.168.24.51.51390	vctc005.leaseweb.http	ESTABLISHED			
07	udp4	0	0	10.0.14.94.ntp	*.*				
< 8~61 省略 >									
62	Active LOCAL (UNIX) domain sockets								
63	Address	Type	Recv-Q	Send-Q	Inode	Conn	Refs	Nextref	Addr
64	80bb0	stream	0	0	0	68707f8	0	0	
65	68707f8	stream	0	0	0	8080bb0	0	0	
66	8080dd0	stream	0	0	0	8080ee0	0	0	
67	8080ee0	stream	0	0	0	8080dd0	0	0	
68	4d183b8	stream	0	0	0	0	0	0	
69	4d18110	stream	0	0	0	6870dd0	0	0	/var/run/mDNSResponder
70	6870dd0	stream	0	0	0	4d18110	0	0	
71	6870000	stream	0	0	0	0	0	0	
< 72~236 省略 >									

4.4.3 説明

1. 01~61 はインターネットのプロトコル情報。

- (a) Proto: ソケットのプロトコル名
- (b) Recv-Q; 受信キューに溜まっているデータバイト数
- (c) Send-Q: 送信キューに溜まっているデータバイト数
- (d) Local Address: ローカル (接続元) ホストの IP アドレス、ポート番号
- (e) Foreign Address: 接続先ホストの IP アドレス、ポート番号
- (f) (state): 接続の状態

ESTABLISHED	接続が確立されているソケット
CLOSED	未使用なソケット
LISTEN	接続待ちのソケット

2. 62~236 はホスト内で閉じたネットワークのプロトコルの情報

- (a) Address : ドメインコントロールブロックの内部メモリ番号
- (b) Type : ソケットのデータ通信型
- (c) stream : ストリーム (コネクション) のソケット。通常 TCP は stream
- (d) dgram : データグラム (コネクションレス) のソケット。通常 UDP は dgram
- (e) Inode : inode 番号
- (f) Conn : stream 型ソケットの相手コントロールブロックの内部メモリ番号
- (g) Refs : dgram 型ソケットの最後に受信した相手コントロールブロックの内部メモリ番号
- (h) Nextref : dgram 型ソケットの最後に送信した相手コントロールブロックの内部メモリ番号

4.4.4 考察

1. 実行した PC の IP アドレスは「10.0.14.19」であるから 03~05 であることがわかる。
2. naha.ie.u-ryukyu.nntp を使用している。
3. nntp : インターネットアプリケーションプロトコルのひとつである。
おもに、ネットニュース (Usenet) の記事を読むことと記事を投稿することのために使われる。
4. IP アドレスが同じでもポート番号が違くと違う回線と判断している。
5. この時は接続が確立されているのは3つだけである。
6. 06 の IP アドレスは自宅の IP アドレスである。

5 課題5

各自のコンピュータで、ifconfig コマンドの「ifconfig (インターフェイス名)」オプションについて実行例を示し、表示される結果について説明せよ。また、「-a」オプションとの表示結果の違いについて説明せよ。

5.1 実行結果「ifconfig (インターフェイス名)」

```

01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ ifconfig en0
02 en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
03 ether 00:23:df:ab:28:98
04 media: autoselect status: inactive
05 supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <full- duplex> 10baseT/
  UTP <full-duplex,flow-control> 10baseT/UTP <full-duplex,hw-loopback> 100baseTX <half-duplex> 1
  00baseTX <full-duplex> 100baseTX <full-duplex,flow-control> 100baseTX <full-duplex,hw-loopback>
  1000baseT <full-duplex> 1000baseT <full-duplex,flow-control> 1000baseT <full-duplex,hw-loopback>

```


5.2 説明

1. インターフェイス名を「en0」とした。

2. flag についてまとめる。

UP	起動している事を示す
LOOPBACK	ループバックをサポート
RUNNING	このインターフェイスを使用してパケットの送受信を行っている
MULTICAST	マルチキャストをサポート

3. flag<> の中にはインターフェイスの現在の状態を表示する。

BROADCAST	<ul style="list-style-type: none">・ブロードキャストをサポートしている事を示す。・ブロードキャストとはネットワーク内で不特定多数に対して一斉にパケットを送信する事。
LOOPBACK	<ul style="list-style-type: none">・ループバックをサポートしている事を示す。・ループバックとは自分自身にパケットを送信する事。
MULTICAST	<ul style="list-style-type: none">・インターフェイスがマルチキャストをサポートしている事を示す。・マルチキャストとは複数の相手を指定してパケットを送信する事。
RUNNING	<ul style="list-style-type: none">・このインターフェイスを使用してパケットの送受信を行っている
SIMPLEX	<ul style="list-style-type: none">・単方向通信を行う事を示す。
SMART	<ul style="list-style-type: none">・(h4ox) 不明。・HDD の SMART 機能の事

4. mtu : mtu 一回の転送で送信できるデータの最大値 (Byte)

5. 03 は実行した PC の MAC アドレスである。

6. 05 は対応してるケーブルを表示している。

- (a) 10baseT/UTP : Ethernet の規格の一つ。
- (b) 10baseT/UTP : Fast Ethernet の規格の一つ。
- (c) half-duplex : 半二重
- (d) full-duplex : 全二重
- (e) ?ow-control : フロー制御
- (f) hw-loopback : ループバック

5.3 実行結果「ifconfig -a」

```
01      lo:  flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
02          inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
03          inet 127.0.0.1 netmask 0xff000000
04          inet6 ::1 prefixlen 128
05      gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
06      stf0: flags=0<> mtu 1280
07      en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
08          ether 00:23:df:ab:28:98
09          media: autoselect status: inactive
10          supported media: none autoselect 10baseT/UTP<half-duplex> 10baseT/UTP <full-duplex>
11          10baseT/UTP <full-duplex,flow-control> 10baseT/UTP <full-duplex,hw-loopback> 100base
12          TX <half-duplex> 100baseTX <full-duplex> 100baseTX <full-duplex,flow-control> 100base
13          TX <full-duplex,hw-loopback> 1000baseT <full-duplex> 1000baseT <full-duplex,flow-contro
14          l> 1000baseT <full-duplex,hw-loopback>
11      en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
12          inet6 fe80::223:6cf:fe91:c7e9%en1 prefixlen 64 scopeid 0x5
13          inet6 2001:2f8:1c:d051:223:6cf:fe91:c7e9 prefixlen 64 autoconf
14          inet 10.0.14.94 netmask 0xfffff000 broadcast 10.0.15.255
15          ether 00:23:6c:91:c7:e9
16          media: autoselect status: active
17          supported media: autoselect
18      vmnet8: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
19          inet 192.168.161.1 netmask 0xfffff00 broadcast 192.168.161.255
20          ether 00:50:56:c0:00:08
21      vmnet1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
22          inet 192.168.12.1 netmask 0xfffff00 broadcast 192.168.12.255
23          ether 00:50:56:c0:00:01
```

5.4 考察

1. inet : IP アドレス
2. netmask : ネットマスク
3. broadcast : ブロードキャストアドレス
4. 「ifconfig (インターフェイス名)」と「ifconfig -a」の大きな違いは表示する量である。
5. 「ifconfig (インターフェイス名)」は指定したインターフェイスだけ表示する。
6. 「ifconfig -a」はすべてのインターフェイスが表示される。
7. インターフェイスの種類

lo	ローカルループバック
gif	IPv4 と IPv6 のトンネルインターフェース
stf	6to4 トンネルインタフェース
en	Midway に基づいた ATM インタフェース用のデバイスドライバ
vmnet	VMware が作成する仮想 Ethernet アダプタ

6 課題6

各自のコンピュータで、ifconfig コマンドを使って、IP アドレス、サブネットマスク、ブロードキャストアドレスを設定せよ。その際、設定する IP アドレスは、クラス A,B,C のいずれかの任意のプライベートアドレスとすること。また、これらが正しく設定されているか ifconfig コマンドを使って確認せよ（表示結果から示せ）。

6.1 変更前

```
01 en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
02 ether 00:23:df:ab:28:98
03 media: autoselect status: inactive
04 supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <full- duplex> 10baseT/
   UTP <full-duplex,flow-control> 10baseT/UTP <full-duplex,hw-loopback> 100baseTX <half-duplex> 1
   00baseTX <full-duplex> 100baseTX <full-duplex,flow-control> 100baseTX <full-duplex,hw-loopback>
   1000baseT <full-duplex> 1000baseT <full-duplex,flow-control> 1000baseT <full-duplex,hw-loopback>
```

1. インターフェイスは「en0」を使用した。
2. まだ IP アドレス、ネットマスク、デフォルトゲートウェイはなにも設定されていないので表示されていない。

6.2 実行

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ sudo ifconfig en0 192.16.1.31 255.255.255.0 192.16.1.255
02 Password:
```

1. IP アドレス：192.16.1.31
2. ネットマスク：255.255.255.0
3. デフォルトゲートウェイ：192.16.1.255

6.3 変更後

```
01 en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
02 inet 192.16.1.31 netmask 0xfffff00 broadcast 192.16.1.255
03 ether 00:23:df:ab:28:98
04 media: autoselect status: inactive
05 supported media: none autoselect 10baseT/UTP <half-duplex> 10baseT/UTP <full- duplex> 10baseT/
   UTP <full-duplex,flow-control> 10baseT/UTP <full-duplex,hw-loopback> 100baseTX <half-duplex> 1
   00baseTX <full-duplex> 100baseTX <full-duplex,flow-control> 100baseTX <full-duplex,hw-loopback>
   1000baseT <full-duplex> 1000baseT <full-duplex,flow-control> 1000baseT <full-duplex,hw-loopback>
```

1. 02 より IP アドレスは「192.16.1.31」に設定された。
2. ネットマスクは「0xfffff00」に設定された。
3. ブロードキャストアドレスは「192.16.1.255」に設定されてた。

4. #ifconfig < インターフェイス名 >< IP アドレス >< ネットマスク >< ブロードキャストアドレス > と入力したら変更出来る。

7 課題7

各自のコンピュータで、route コマンドを使って任意の学科ネットワークサブネット（例えば、サーバセグメント（133.13.48.0/24）やクラスAセグメント（133.13.49.0/24））に対して、静的経路の追加および削除を行ってみよ。また、追加・削除が正しく行えているか netstat -r コマンドを使って確認せよ（表示結果から示せ）。なお、ネットワーク接続形態（無線 LAN 接続 or 有線 LAN 接続）によって、ゲートウェイアドレスが異なるので注意すること。

7.1 追加

7.1.1 変更前

01	Routing tables						
02	Internet:						
03	Destination	Gateway	Flags	Refs	Use	Netif	Expire
04	default	10.0.15.254	UGSc	13	8	en1	
05	10/20	link#5	UCS	13	0	en1	
	< 06~17 省略 >						
18	10.0.15.255	link#5	UHLWb	1	14	en1	
19	123.45.6.7	8.9.8.7	UGHS	0	0	en1	
20	127	localhost	UCS	0	0	lo0	
21	localhost	localhost	UH	1	480429	lo0	
22	169.254	link#5	UCS	0	0	en1	
23	192.168.12	link#7	UC	2	0	vmnet1	
24	192.168.12.1	0:50:56:c0:0:1	UHLW	0	826	lo0	
25	192.168.161	link#6	UC	1	0	vmnet8	
	< 26~45 省略 >						

7.1.2 実行

01	yoshiaki-oshiro-no-macbook-2: yoshiaki\$ sudo route add -net 133.13.53.0 10.0.15.254 255.255.255.0
02	add net 133.13.53.0: gateway 10.0.15.254

1. サーバセグメントを設定する。
2. IP アドレス：133.13.58.0
3. デフォルトゲートウェイ：10.0.15.254
4. ネットマスク：255.255.255.0

7.1.3 変更後

```
01 Routing tables
02 Internet:
03 Destination      Gateway      Flags  Refs  Use  Netif  Expire
04     default      10.0.15.254  UGSc   13    8   en1
05     10/20        link#5      UCS    13    0   en1

    < 06~17 省略 >

18 10.0.15.255      link#5      UHLWb   1    14   en1
19 123.45.6.7       8.9.8.7     UGHS    0     0   en1
20      127         localhost   UCS     0     0   lo0
21 localhost        localhost   UH      1 480429 lo0
22 133.13.53/24     10.0.15.254 UGSc    0     0   en1
23 169.254          link#5      UCS     0     0   en1
24 192.168.12       link#7      UC      2     0   vmnet1
25 192.168.12.1     0:50:56:c0:0:1 UHLW    0    826  lo0
26 192.168.161     link#6      UC      1     0   vmnet8

    < 27~45 省略 >
```

1. 「22 133.13.53/24 10.0.15.254 UGSc 0 0 en1」が追加されている。
2. Flags が UGSc よりルーティングが有効、対象はゲートウェイ、静的に設定されたルーティングである事がわかる。
3. 以上のことよりちゃんと追加されてた事がわかる。

7.2 削除

7.2.1 変更前

7.1.3 をそのまま使う。

7.2.2 実行

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ sudo route delete -net 133.13.53.0 10.0.15.254
02 255.255.255.0
03 Password:
04 delete net 133.13.53.0: gateway 10.0.15.254
```

1. IP アドレス、デフォルトゲートウェイ、ネットマスクは追加と同じである。
2. 追加と違ってパスワードを要求された。

7.2.3 変更後

```
01 Routing tables
02 Internet:
03 Destination      Gateway      Flags  Refs  Use  Netif  Expire
04     default      10.0.15.254  UGSc   27    30   en1
05     10/20        link#5       UCS    17     0   en1

    < 06~17 省略 >

18  10.0.15.255     link#5      UHLWb   1    14   en1
19  123.45.6.7      8.9.8.7     UGHS    0     0   en1
20      127         localhost    UCS    0     0   lo0
21  localhost       localhost    UH      1  481035  lo0
22  169.254         link#5       UCS    0     0   en1
23  192.168.12      link#7       UC      2     0   vmnet1
24  192.168.12.1    0:50:56:c0:0:1  UHLW    0    826   lo0
25  192.168.161     link#6       UC      1     0   vmnet8

    < 26~45 省略 >
```

1. 探しても見当たらない。
2. ちゃんと削除されたのがわかる。

8 課題8

各自のコンピュータで、route コマンドを使ってデフォルトゲートウェイ（無線LAN接続の場合は10.0.15.254）を設定せよ。また、デフォルトゲートウェイが正しく設定されているか netstat -r コマンドを使って確認せよ（表示結果から示せ）。

8.1 設定前

```
01 Routing tables
02 Internet:
03 Destination      Gateway      Flags  Refs  Use  Netif  Expire
04     10/20        link#5       UCS     6     0   en1
05  10.0.1.13       link#5      UHLW    0     0   en1
06  10.0.3.1        link#5      UHLW    0     0   en1
07  10.0.11.100     0:23:6c:91:ad:8b  UHLW    0    120   en1    1191

    < 08~45 省略 >
```

1. そのままだと変更出来ない。
2. 「sudo route delete default 10.0.15.254」で default を削除した。
3. default は設定されていない状態になっている。

8.2 実行

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ sudo route add default 10.0.1.13
02 Password:
03 add net default: gateway 10.0.1.13
```

1. デフォルトゲートウェイを「10.0.1.13」に設定した。
2. 03 より設定されたことがわかる。

8.3 設定後

```
01 Routing tables
02 Internet:
03 Destination  Gateway  Flags  Refs  Use  Netif  Expire
04      default  10.0.1.13  UGSc   7    0    en1
05      10/20    link#5    UCS    6    0    en1

< 06~45 省略 >
```

1. 04 よりデフォルトが「10.0.1.13」に設定されていることがわかる。
2. UGSc になっているので正しく設定されていることがわかる。

9 課題9

nslookup の対話モード・非対話モードの両方で、任意のホスト名から IP アドレスを検索（正引き）し、表示される結果について説明せよ。また、任意の IP アドレスからホスト名を検索（逆引き）し、表示される結果について説明せよ。

9.1 正引き

正引き：ホスト名 から IP アドレス を調べること

9.1.1 対話モード

1. 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ nslookup
02 > nirai
03 Server: 133.13.48.3
04 Address: 133.13.48.3#53
05 Name: nirai.ie.u-ryukyu.ac.jp
06 Address: 133.13.48.2
```

2. 説明

- (a) 「nslookup」で対話モードになる。
- (b) 02でドメイン名を入力した。
- (c) Sever : DNSのサーバー名
- (d) Address : DNSのサーバーのIPアドレス
- (e) #53はポート番号である。
- (f) Name : 調べるホスト名
- (g) Address : NameのIPアドレス

9.1.2 非対話モード

1. 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ nslookup nirai
02 Server: 133.13.48.3
03 Address: 133.13.48.3#53
04 Name: nirai.ie.u-ryukyu.ac.jp
05 Address: 133.13.48.2
```

2. 説明

- (a) 「nslookup <ドメイン名>」で非対話モードになる。
- (b) 基本的には対話モードと同じである。

9.2 逆引き

逆引き : IP アドレスからホスト名を調べること

9.2.1 対話モード

1. 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ nslookup
02 > 133.13.48.2
03 Server: 133.13.48.3
04 Address: 133.13.48.3#53
05 2.48.13.133.in-addr.arpa name = nirai.ie.u-ryukyu.ac.jp.
```


2. (a) 正引きと同様「nslookup」で対話モードになる。
 - (b) 02でIPアドレスを入力した
 - (c) Server : DNS サーバー名
 - (d) Address : Server の IP アドレス
 - (e) 05 の「2.48.13.133.in-addr.arpa」は実際の逆引きコードのドメイン名である。
 - (f) name : ホスト名

9.2.2 非対話モード

1. 実行結果

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ nslookup 133.13.48.2
03 Server: 133.13.48.3
04 Address: 133.13.48.3#53
05 2.48.13.133.in-addr.arpa name = nirai.ie.u-ryukyu.ac.jp.
```

2. (a) 「nslookup <IP アドレ >」で非対話モードになる。
 - (b) 基本的には対話モードと同じである

10 課題 10

nslookup の対話モードで、レコードの変更を行い、SOA レコード、NS レコード、MX レコードについて、任意のドメイン名を検索し、表示される結果について説明せよ。なお、レコード変更は、nslookup の対話モードで以下のコマンドを実行することで行える。

10.1 SOA レコード

10.1.1 実行結果

```
01 >set type=SOA
02 >ie.u-ryukyu.ac.jp
03 Server: 133.13.48.3
04 Address: 133.13.48.3#53
05 Routing tablesie.u-ryukyu.ac.jp
06     origin = futenma.ie.u-ryukyu.ac.jp
07     mail addr = hostmaster.ie.u-ryukyu.ac.jp
08     serial = 2009050909
09     refresh = 28800
10     retry = 7200
11     expire = 604800
12     minimum = 86400
```

10.1.2 説明

1. SOA は Start Of Authority の略で、「権威の開始」という意味である。
2. 主に、スレーブ・ネームサーバがマスター・ネームサーバに問い合わせる時間間隔などが設定されている。
3. 06～12の説明

origin	DNS サーバ名
mail addr	メールアドレス
serial	ゾーンファイルのバージョンを示す数字
refresh	情報をリフレッシュするまでの時間
retry	情報の更新が出来なかった場合、再度リフレッシュまでの時間
expire	キャッシング保持してから、捨てるまでの時間
minimum	引けないという情報をキャッシュしておく時間

10.2 NS レコード

10.2.1 実行結果

```
01 > set type=NS
02 > ie.u-ryukyu.ac.jp
03 Server: 133.13.48.3
04 Address: 133.13.48.3#53
05 ie.u-ryukyu.ac.jp nameserver = nirai.ie.u-ryukyu.ac.jp.
06 ie.u-ryukyu.ac.jp nameserver = kanai.ie.u-ryukyu.ac.jp.
```

10.2.2 説明

1. そのドメインに対するネームサーバの情報が表示される。
2. nameserver : DNS サーバ名
3. 実行結果より nirai と kanai の二つがあることがわかる。

10.3 MX レコード

10.3.1 実行結果

```
01 > set type=MX
02 > ie.u-ryukyu.ac.jp
03 Server: 133.13.48.3
04 Address: 133.13.48.3#53
05 ie.u-ryukyu.ac.jp mail exchanger = 100 nirai.ie.u-ryukyu.ac.jp.
```

10.3.2 説明

1. そのドメインに対するメールサーバの情報が表示される。
2. mail exchanger : <プリファレンス値><メールサーバ名>
3. プリファレンス：メールサーバが複数存在する場合に、どれを優先的に利用するか優先度を表す。

11 課題 1 1

nslookup の対話モードで、resolv.conf に設定されているデフォルトの DNS サーバではなく、他の任意の DNS サーバを使って課題 8 と同様に任意のホスト名から IP アドレスを検索し、その結果を示せ。

11.1 実行前

1. 使用しているサーバを調べる。

```
01 > server
02 Default server: 133.13.48.3
03 Address: 133.13.48.3#53
04 Default server: 133.13.48.2
05 Address: 133.13.48.2#53
```

2. デフォルトゲートウェイは2つあることがわかる
3. 実際にはどれを使っているのかを調べる。

```
01 >nirai
02 Default server: 133.13.48.3
03 Address: 133.13.48.3#53
    < 03~04 省略 >
```

4. 実行前に設定されているデフォルトの DNS サーバは「133.13.48.3」である
5. 133.13.48.3 は kanai を使用している。

11.2 実行結果

```
01 > server 133.13.48.2
02 Default server: 133.13.48.2
03 Address: 133.13.48.2#53
04 > nirai
05 Server: 133.13.48.2
06 Address: 133.13.48.2#53
07 Name: nirai.ie.u-ryukyu.ac.jp
08 Address: 133.13.48.2
```

11.3 考察

1. 01~03 の説明をする
 - (a) 使用するサーバの変更をしている
 - (b) 「133.13.48.2」を使用する
 - (c) 「133.13.48.2」は nirai である
2. 04 は正引きして「nirai」を調べている
3. 05,06 より「133.13.48.2」を使用していることがわかる
4. 07,08 より正しく正引きが出来ていることがわかる

12 課題 1 2

最新の BIND9 系では、nslookup に代わって、host コマンド、dig コマンドなどの使用が推奨されている。これらのコマンドを使って、課題 9~11 と同じ結果を得るにはどのような操作が必要か示せ。

1. 「host」は DNS サーバで名前解決する情報について問い合わせをするコマンドである。
2. 「dig」はネームサーバに対して問い合わせを行い、その応答結果を表示するコマンドである

12.1 課題 9 の内容

12.1.1 host コマンド

1. 正引き

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ host nirai
02 nirai.ie.u-ryukyu.ac.jp has address 133.13.48.2
03 nirai.ie.u-ryukyu.ac.jp has IPv6 address 2001:2f8:1c:d048::850d:3002
```

2. 逆引き

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ host 133.13.48.2
02 2.48.13.133.in-addr.arpa domain name pointer nirai.ie.u-ryukyu.ac.jp.
```

3. 説明

- (a) 正引きは「host <ホスト名>」で出来る
 - i. IP アドレスは IPv4 と IPv6 の両方表示されている
- (b) 逆引きは「host <IP アドレス>」で出来る
 - i. nslookup と表示する内容は同じである

12.1.2 dig コマンド

1. 正引き

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ dig nirai
02 ; <<>> DiG 9.4.3-P3 <<>> nirai
03 ;; global options: printcmd
04 ;; Got answer:
05 ;; ->>HEADER;; opcode: QUERY, status: NXDOMAIN, id: 57808
06 ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
07 ;; QUESTION SECTION:
08 ;nirai. IN A
09 ;; AUTHORITY SECTION:
10 . 10400 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2010050900 1800
11 900 604800 86400
12 ;; Query time: 4 msec
13 ;; SERVER: 133.13.48.3#53(133.13.48.3)
14 ;; WHEN: Mon May 10 01:10:57 2010
15 ;; MSG SIZE revd: 98
```

2. 逆引き

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ dig -x 133.13.48.3
    < 02~08 省略 >
09 ;; ANSWER SECTION:
10 3.48.13.133.in-addr.arpa. 86500 IN PTR kanai.ie.u-ryukyu.ac.jp.
11 ;; AUTHORITY SECTION:
12 48.13.133.in-addr.arpa. 86500 IN NS kanai.ie.u-ryukyu.ac.jp.
13 48.13.133.in-addr.arpa. 86500 IN NS nirai.ie.u-ryukyu.ac.jp.
    < 13~22 省略 >
```

1. 説明

- (a) 正引きは「dig < ホスト名 >」で出来る
 - i. 13 でサーバのアドレスがわかる
- (b) 逆引きは「dig -x <IP アドレス >」で出来る
 - i. 10 でドメイン名がわかる
 - ii. 12,13 でサーバ名がわかる
- (c) 出力されていることについて説明する

status	・ 正しく情報得られたときは NOERROR ・ ドメイン名が存在しないときは NXDOMAIN と表示される
flags	・ この応答がどういう意味を持つのか示すフラグ
QUESTION	・ 引数で入力されたもの
ANSWER	・ 引数に対する回答。ここを見ればよい
AUTHORITY	・ サーバ名
ADDITIONAL	・ 追加項目

12.2 課題 10 の内容

12.2.1 host コマンド

1. SOA コード

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ host -t soa ie.u-ryukyu.ac.jp
02 ie.u-ryukyu.ac.jp has SOA record futenma.ie.u-ryukyu.ac.jp. hostmaster.ie.u-ryukyu.ac.jp.
    2009050909 28800 7200 604800 86400
```

2. NS コード

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ host -t ns ie.u-ryukyu.ac.jp
02 ie.u-ryukyu.ac.jp name server nirai.ie.u-ryukyu.ac.jp.
03 ie.u-ryukyu.ac.jp name server kanai.ie.u-ryukyu.ac.jp.
```

3. MX コード

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ host -t mx ie.u-ryukyu.ac.jp
04 ie.u-ryukyu.ac.jp mail is handled by 100 nirai.ie.u-ryukyu.ac.jp.
```

4. 説明

- (a) SOA コードは「host -t soa < ホスト名 >」で出来る
- (b) NS コードは「host -t ns < ホスト名 >」で出来る

- (c) MX コードは「host -t mx < ホスト名 >」で出来る
- (d) つまり「host -t < モード >< ホスト名 >」で出来ることがわかる

12.2.2 dig コマンド

1. SOA コード

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ dig -t soa ie.u-ryukyu.ac.jp
    < 02~08 省略 >
09 ;; ANSWER SECTION:
10 ie.u-ryukyu.ac.jp. 86500 IN SOA futenma.ie.u-ryukyu.ac.jp. hostmaster.ie.u-ryukyu.ac.jp. 20090509
    09 28800 7200 604800 86400
    < 11~22 省略 >
```

2. NS コード

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ dig -t ns ie.u-ryukyu.ac.jp
    < 02~08 省略 >
09 ;; ANSWER SECTION:
10 ie.u-ryukyu.ac.jp. 86500 IN NS kanai.ie.u-ryukyu.ac.jp.
11 ie.u-ryukyu.ac.jp. 86500 IN NS nirai.ie.u-ryukyu.ac.jp.
    < 12~23 省略 >
```

3. MX コード

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ dig -t mx ie.u-ryukyu.ac.jp
    < 02~08 省略 >
09 ;; ANSWER SECTION:
10 ie.u-ryukyu.ac.jp. 86500 IN MX 100 nirai.ie.u-ryukyu.ac.jp.
    < 10~22 省略 >
```

4. 説明

- (a) SOA コードは「dig -t soa < ホスト名 >」で出来る
- (b) NS コードは「dig -t ns < ホスト名 >」で出来る
- (c) MX コードは「dig -t mx < ホスト名 >」で出来る
- (d) つまり「dig -t < モード >< ホスト名 >」で出来ることがわかる
- (e) よって dig コマンドも host コマンドも同じように使える

12.3 課題 11 の内容

12.3.1 host コマンド

1. 課題 11 より初めに設定されているデフォルトの DNS サーバは「133.13.48.3」である

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ host ie.u-ryukyu.ac.jp 133.13.48.2
02 Using domain server:
03 Name: 133.13.48.2
04 Address: 133.13.48.2#53
05 Aliases:
06 ie.u-ryukyu.ac.jp has address 133.13.48.7
07 ie.u-ryukyu.ac.jp mail is handled by 100 nirai.ie.u-ryukyu.ac.jp.
```

2. 「133.13.48.2」のサーバを使用する
3. 03より「133.13.48.2」が使用されているのがわかる
4. 06,07より正しく設定されているのがわかる
5. 「host <ドメイン名><サーバのIPアドレス>」で出来る

12.3.2 dig コマンド

1. 初めに設定されているデフォルトのDNSサーバは「133.13.48.3」である

```
01 yoshiaki-oshiro-no-macbook-2: yoshiaki$ dig ie.u-ryukyu.ac.jp @133.13.48.7
    < 02~08 省略 >
09 ;; ANSWER SECTION:
10 ie.u-ryukyu.ac.jp. 86500 IN A 133.13.48.7
    < 11~19 省略 >
20 ;; Query time: 22 msec
21 ;; SERVER: 133.13.48.7#53(133.13.48.7)
22 ;; WHEN: Mon May 10 03:04:52 2010
23 ;; MSG SIZE revd: 179
```

2. 「133.13.48.7」のサーバを使用する
3. 21より「133.13.48.7」が使用されているのがわかる
4. 10より正しく設定されているのがわかる
5. 「host <ドメイン名>@<サーバのIPアドレス>」で出来る