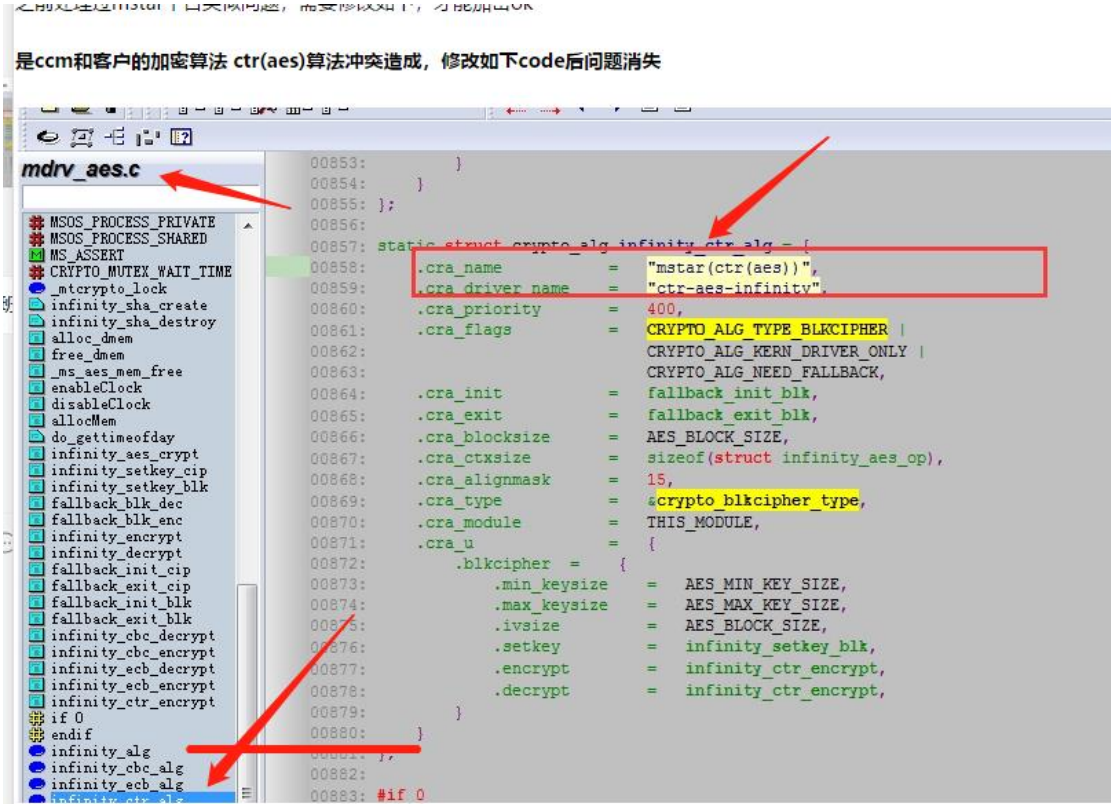
加密路由器连不上问题解决方法：

需要 kernel config 的 CONFIG_CRYPTO_CCM 设置 y，并且这个要改名（和 kernel ccm 冲突）



之前处理过mstar 平台类似问题，需要修改如下，才能加密OK

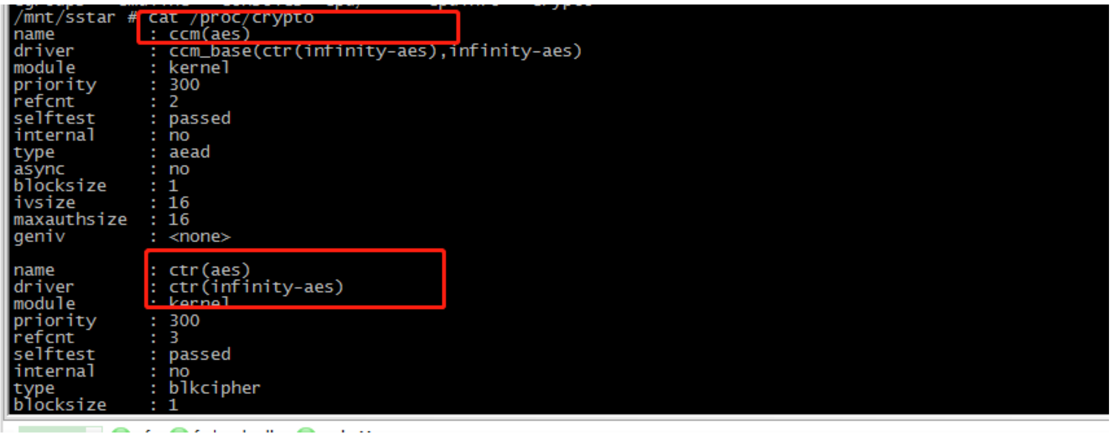
是ccm和客户的加密算法 ctr(aes)算法冲突造成，修改如下code后问题消失

mdrv_aes.c

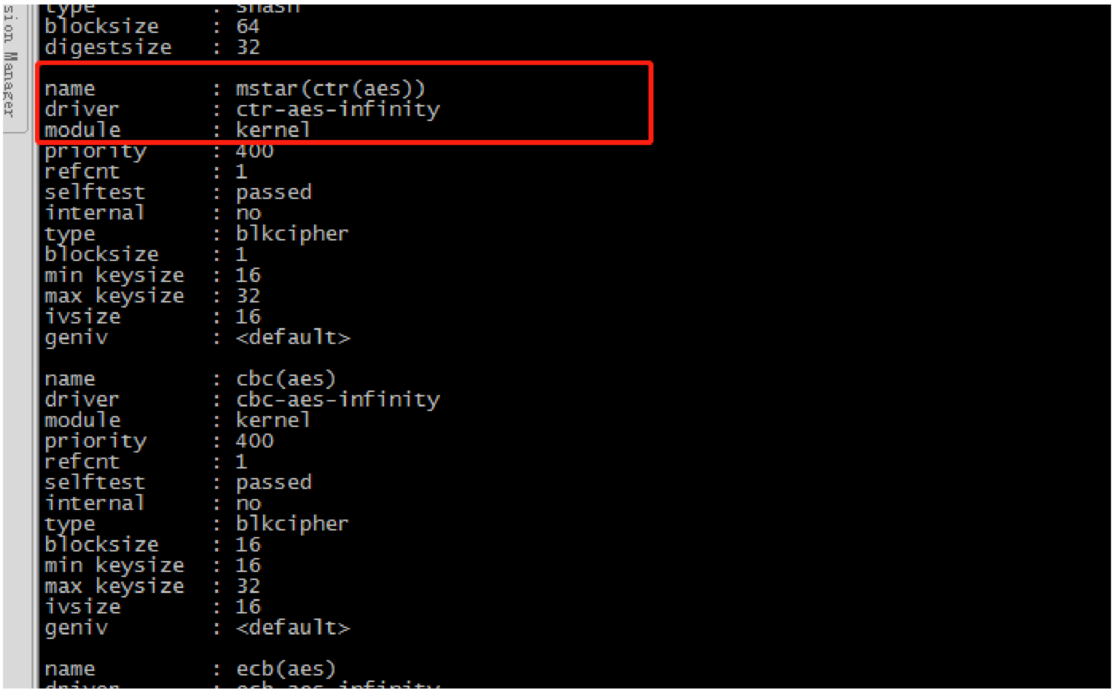
```
MSOS_PROCESS_PRIVATE
MSOS_PROCESS_SHARED
MS_ASSERT
CRYPTO_MUTEX_WAIT_TIME
_mtcrypto_lock
infinity_sha_create
infinity_sha_destroy
alloc_dmem
free_dmem
_ms_aes_mem_free
enableClock
disableClock
allocMem
do_gettimeofday
infinity_aes_crypt
infinity_setkey_cip
infinity_setkey_blk
fallback_blk_dec
fallback_blk_enc
infinity_encrypt
infinity_decrypt
fallback_init_cip
fallback_exit_cip
fallback_init_blk
fallback_exit_blk
infinity_cbc_decrypt
infinity_cbc_encrypt
infinity_ecb_decrypt
infinity_ecb_encrypt
infinity_ctr_encrypt
if 0
endif
infinity_alg
infinity_cbc_alg
infinity_ecb_alg
infinity_ctr_alg
```

```
        }
    }
};

static struct crypto_alg infinity_ctr_alg = {
    .cra_name               =   "mstar(ctr(aes))",
    .cra_driver_name        =   "ctr-aes-infinity",
    .cra_priority           =   400,
    .cra_flags              =   CRYPTO_ALG_TYPE_BLKCIPHER |
                                CRYPTO_ALG_KERN_DRIVER_ONLY |
                                CRYPTO_ALG_NEED_FALLBACK,
    .cra_init               =   fallback_init_blk,
    .cra_exit               =   fallback_exit_blk,
    .cra_blocksize          =   AES_BLOCK_SIZE,
    .cra_ctxsize            =   sizeof(struct infinity_aes_op),
    .cra_alignmask          =   15,
    .cra_type               =   &crypto_blkcipher_type,
    .cra_module             =   THIS_MODULE,
    .cra_u                  =   {
        .blkcipher  =   {
            .min_keysize    =   AES_MIN_KEY_SIZE,
            .max_keysize    =   AES_MAX_KEY_SIZE,
            .ivsize         =   AES_BLOCK_SIZE,
            .setkey         =   infinity_setkey_blk,
            .encrypt        =   infinity_ctr_encrypt,
            .decrypt        =   infinity_ctr_encrypt,
        }
    }
};

#if 0
```

cat /proc/crypto 确认是否生效



```
/mnt/sstar # cat /proc/crypto
name         : ccm(aes)
driver       : ccm_base(ctr(infinity-aes),infinity-aes)
module       : kernel
priority     : 300
refcnt       : 2
selftest     : passed
internal     : no
type         : aead
async        : no
blocksize    : 1
ivsize       : 16
maxauthsize  : 16
geniv        : <none>

name         : ctr(aes)
driver       : ctr(infinity-aes)
module       : kernel
priority     : 300
refcnt       : 3
selftest     : passed
internal     : no
type         : blkcipher
blocksize    : 1
```



```
type         : shash
blocksize    : 64
digestsize   : 32

name         : mstar(ctr(aes))
driver       : ctr-aes-infinity
module       : kernel
priority     : 400
refcnt       : 1
selftest     : passed
internal     : no
type         : blkcipher
blocksize    : 1
min keysize  : 16
max keysize  : 32
ivsize       : 16
geniv        : <default>

name         : cbc(aes)
driver       : cbc-aes-infinity
module       : kernel
priority     : 400
refcnt       : 1
selftest     : passed
internal     : no
type         : blkcipher
blocksize    : 16
min keysize  : 16
max keysize  : 32
ivsize       : 16
geniv        : <default>

name         : ecb(aes)
driver       : ecb-aes-infinity
```