Layer 2, routing protocols, router security & forensics

> Nicolas FISCHBACH
IP Engineering Manager - COLT Telecom
nico@securite.org - http://www.securite.org/nico/

> Sébastien LACOSTE-SERIS
IP R&D Manager, Security Officer - COLT Telecom
kaneda@securite.org - http://www.securite.org/kaneda/

C O L T
we make business straight.forward

version 1.0

Agenda

- **Layer 2 protocols and attacks**
  - ARP
  - STP, CDP, DTP, etc.
  - VLANs
  - HSRP/VRRP

- **Router Security**
  - Configuration hardening
  - Integrity checking
  - Forensics

Protocol attacks

» **Well known (not to say old) attacks**
  - > ARP cache/CAM table poisoning, gratuitous ARP messages and ARP/{DHCP,BOOTP} spoofing
  - > Tools : dsniff, hunt, ARP0c, taranis, etc.

» **New (not so old) attacks**
  - > HSRP/VRRP spoofing
  - > STP/VTP/DTP attacks
  - > VLAN jumping/hoping

» **Future (to come) attacks ?**
  - > Advanced routing protocols attacks (eg. IRPAS)
  - > Rootkits and Loadable Kernel Modules

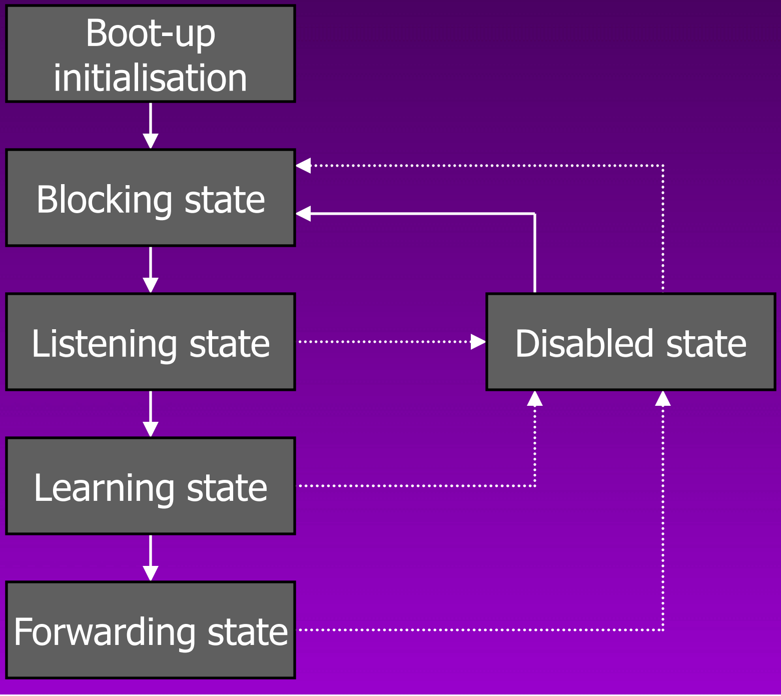
Layer 2 protocols

» **Layer 2 protocols and traffic**

- > ARP - Address Resolution Protocol
- > CDP - Cisco Discovery Protocol
- > VLAN - Virtual LAN
- > STP - Spanning Tree
- > {D/V}TP - Dynamic, VLAN Trunking Protocol
- > Unicast, Broadcast and Multicast addressing and traffic

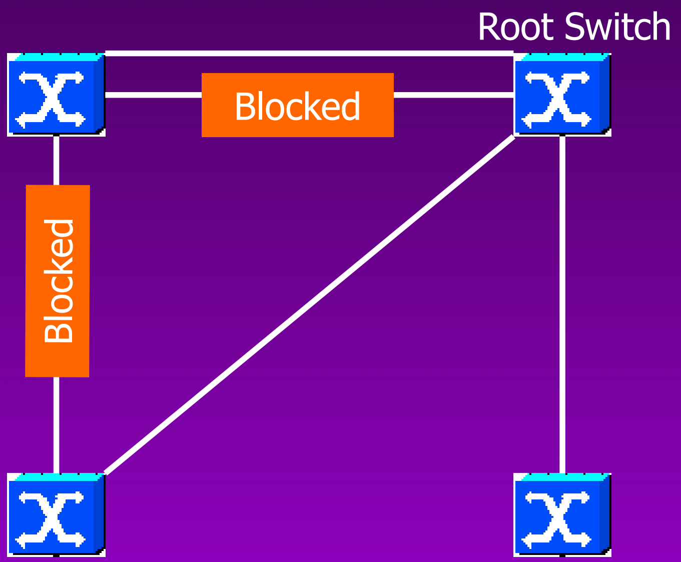
Protocols : STP (1)

- **STP (Spanning Tree Protocol)**
  - > STP prevents loops in the Ethernet network topology
  - > Redundant data path forced into standby (blocked) state
  - > STP enabled on all ports by default
  - > No traffic forwarding during STP processing



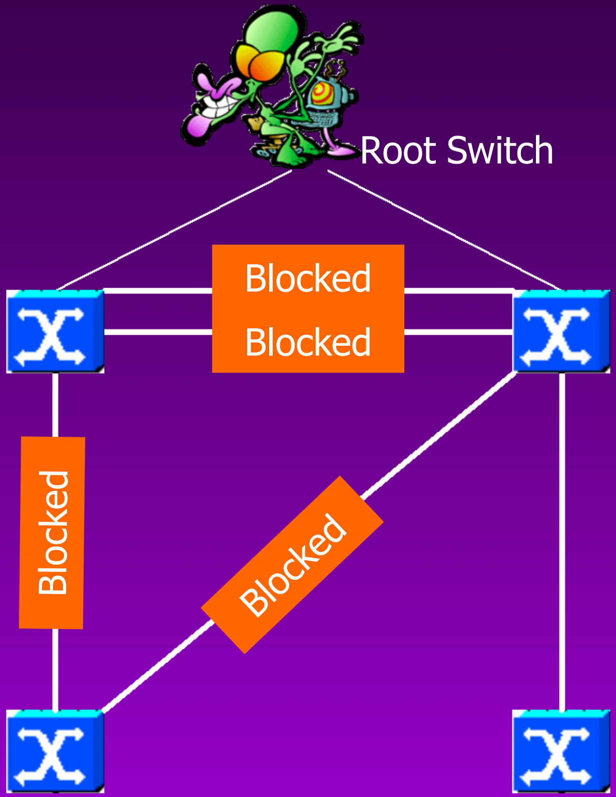
Protocols : STP (2)

- **STP (Spanning Tree Protocol)**
  - > 1. Root Switch Election
  - > 2. STP processing blocks redundant path



Protocols : STP (3)

- **Network Traffic Interception**
  - Must have physical connection to 2 switches
  - Transparent traffic interception



Protocols : STP (4)

- **Other STP attacks**
  - CAM table poisoning
  - DoS
    - Force infinite election
    - Ephemere Root
- **Very hard to track down network topology**

Protocols : STP (5)

» Security measures

- > Monitor which equipment is the root bridge
- > Filter MAC addresses (and add static IP-to-MAC mappings)

```
set port security <mod/port> enable 01-02-03-04-05-06 shutdown
```

- > Activate BPDU-guard (Bridge PDU) to filter STP

```
! MLS (Multi Layer Switch) in hybrid mode (Sup w/ CatOS, MSFC w/ IOS)
set spantree disable
set spantree portfast bpdu-guard-enable

! MLS in native mode (CatIOS on the Sup and MSFC)
spanning-tree portfast bpduguard
```

- > Limit broadcast traffic

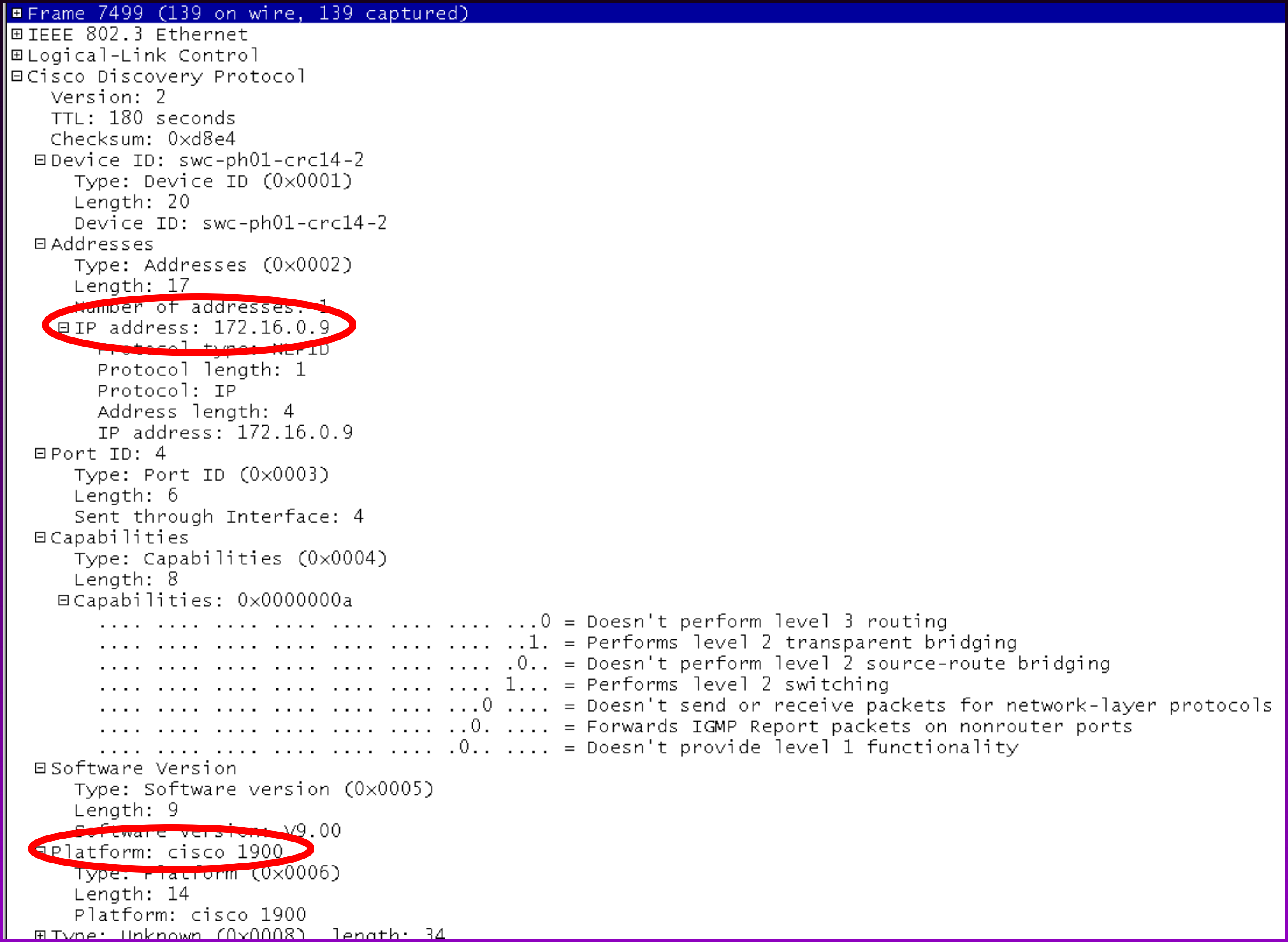
```
set port broadcast <mod/port> 0.01%
```

Protocols : CDP (1)

- **CDP (Cisco Discovery Protocol)**
  - Cisco proprietary
  - Works on any HDLC capable link/device
  - Multicast traffic
  - Information leaked to other peers : device id/name, network address, port id, capabilities, software version, platform and IP network prefix
- **Message format**

<table>
<tr><td colspan="3">SNAP HDLC Protocol Type: 0x2000</td></tr>
<tr><td colspan="3">Destination: 01-00-0C-CC-CC-CC</td></tr>
<tr><td>Version
(1 or 2)</td><td>TTL
(0-255)</td><td>Checksum</td></tr>
<tr><td colspan="3">List of TLVs (Type-Length-Value)</td></tr>
</table>

Protocols : CDP (2)



```
⊞Frame 7499 (139 on wire, 139 captured)
⊞IEEE 802.3 Ethernet
⊞Logical-Link Control
⊟Cisco Discovery Protocol
   Version: 2
   TTL: 180 seconds
   Checksum: 0xd8e4
  ⊟Device ID: swc-ph01-crc14-2
     Type: Device ID (0x0001)
     Length: 20
     Device ID: swc-ph01-crc14-2
  ⊟Addresses
     Type: Addresses (0x0002)
     Length: 17
     Number of addresses: 1
    ⊟IP address: 172.16.0.9
       Protocol type: NLPID
       Protocol length: 1
       Protocol: IP
       Address length: 4
       IP address: 172.16.0.9
  ⊟Port ID: 4
     Type: Port ID (0x0003)
     Length: 6
     Sent through Interface: 4
  ⊟Capabilities
     Type: Capabilities (0x0004)
     Length: 8
    ⊟Capabilities: 0x0000000a
       .... .... .... .... .... .... .... ...0 = Doesn't perform level 3 routing
       .... .... .... .... .... .... .... ..1. = Performs level 2 transparent bridging
       .... .... .... .... .... .... .... .0.. = Doesn't perform level 2 source-route bridging
       .... .... .... .... .... .... .... 1... = Performs level 2 switching
       .... .... .... .... .... .... ...0 .... = Doesn't send or receive packets for network-layer protocols
       .... .... .... .... .... .... ..0. .... = Forwards IGMP Report packets on nonrouter ports
       .... .... .... .... .... .... .0.. .... = Doesn't provide level 1 functionality
  ⊟Software Version
     Type: Software version (0x0005)
     Length: 9
     Software version: V9.00
  ⊟Platform: cisco 1900
     Type: Platform (0x0006)
     Length: 14
     Platform: cisco 1900
  ⊞Type: Unknown (0x0008), length: 34
```

Protocols : CDP (3)

- **Open to DoS attacks**
  - Discovered by FX (see the Cisco Security Notice)
- **Security measures (router)**
  - Global deactivation

```
no cdp run
```

  - Per interface deactivation

```
interface xy
 no cdp enable
```

- **Security measures (switch)**
  - Global/per interface deactivation

```
set cdp disable <mod/port>
```

VLANs : Layer 2 partitioning (1)

- **The problem with VLANs**
  - VLANs have never been designed for security but are used to enforce it
  - (Multi-layer) switches become single point of security failure
  - Do not use the (native) VLAN 1

- **Do not use VMPS**
  - VLAN Management Policy Server allows dynamic VLAN membership based on the MAC address

VLANs : Layer 2 partitioning (2)

- **VLAN jumping/hoping**
  - Is possible : if you use DTP, if a port is in the same VLAN as the trunk's port Native VLAN (inject 802.1q frames)

```
set vlan 2 <mod/port>
clear trunk <mod/port> 1
```

  - VLAN bridges allow bridging between VLANs for non-routed protocols
- **Private VLAN (6k, 4k) and port protected (29xx, 35xx)**
  - Port isolation
  - Devices in the same VLAN can't talk directly to each other

Protocols : VTP

- **VLAN Trunking Protocol**
  - Enables central VLAN configuration (Master/Client)
  - Message format : like CDP (SNAP HDLC 0x2003)
  - Communicates only over trunk ports
- **Attacks**
  - Add/remove VLANs
  - Create STP loops
- **Security measures**
  - Put your switches in transparent VTP mode and use a password

```
set vtp domain <vtp.domain> password <password>
set vtp mode transparent
```

Protocols : DTP

- **Dynamic Trunking Protocol**
  - Enables automatic port/trunk configuration
  - Message format : like CDP (SNAP HDLC 0x2004)
  - All switch ports are in auto mode by default

- **Attacks**
  - 802.11q frames injection
  - VLAN hoping

- **Security measures**
  - Turn DTP off on all the ports

```
set trunk off all
```

Protocols : HSRP/VRRP (1)

- » **HSRP (Hot Standby Routing Protocol)**
  - > Provides next-hop redundancy (RFC2281)
  - > Information disclosure : virtual MAC address
    - 00-00-0c-07-ac-<group>
    - (by default) the HSRP virtual interface doesn't send ICMP redirects
  - > You can have more than 2 routers in a standby group, no need to kill a router, becoming the master is enough

- » **VRRP (Virtual Router Redundancy Protocol - RFC2338)**
  - > Supports MD5 for authentication (IP Authentication Header)

Protocols : HSRP/VRRP (2)

» Security measures

> Use password authentication

```
interface xy
 standby 10 priority 200 preempt
 standby 10 authentication p4ssw0rd
 standby 10 ip x.x.x.x
```

> Change the virtual MAC address

```
interface xy
 standby 10 mac-address <mac-address>
```

> Use IPsec ("Cisco" recommendation) but is not trivial (multicast traffic, order of processing depending on IOS release, limited to a group of 2 routers)

{tcpdump,snoop}ing on routers

- **What can be done with local output**
  - Debug with ACLs

```
access-list 100 …
debug ip packet detail 100
```

  - Always use the buffer and don't debug to the console

```
logging buffered 64000 debugging
```

  - Performance impact : check the router's load with sh proc cpu

- **How to send to a remote device**
  - Use a GRE tunnel to a remote host and inject the traffic back from there (tunnelx)

{tcpdump,snoop}ing on switches

- **No local output**
- **How to send to a remote device**
  - Mirror ports or a VLAN to another port

```
! MLS in hybrid mode
set span <source (mod/port or VLAN)> <destination port>
! MLS in native mode
monitor session <session id> ...
```

  - Can copy only designated traffic to be inspected (VACL w/ “capture” keyword) :

```
set security acl capture-ports <mod/port>
```

  - RSPAN dumps the traffic to a VLAN (needs end-to-end Cat6K)
  - 1 or 2 SPAN port(s) depending on the switch
  - Performance impact close to zero : check the CPU load with ps -c (hidden command)

Configuration basics (1)

» Turn off all the unneeded services

```
no ip bootp server
no tcp-small-servers
no udp-small-servers
```

```
no ip identd
no ip finger
service nagle
```

```
no cdp run
no boot network
no service config
no ip subnet-zero
```

```
no service finger
no service pad
no ip http server
no ip source-route
```

» Use syslog

```
service time log datetime localtime show-timezone msec
service time debug datetime localtime show-timezone msec
logging x.x.x.x
logging trap debugging
logging source loopback0
logging buffered 64000 debugging
```

» Use (authenticated) NTP

```
ntp authentication-key 10 md5 <key>
ntp authenticate
ntp trusted-key 10
ntp server x.x.x.x [key 10]
ntp access-group peer 20
access-list 20 permit host x.x.x.x
access-list 20 deny any
```

Configuration basics (2)

» At the interface level

```
interface xy
 no ip source-route
 no ip directed-broadcast
 no ip proxy-arp
 no ip redirects
 no ip unreachables
 ! IP accounting for the traffic that fails the IP ACLs
 ip accounting access-violations
 no ip mask-reply
 no cdp enable
```

» If multicast is used

```
interface xy
 ! To prevent Auto-RP messages from entering the PIM domain
 ip multicast boundary 10
access-list 10 deny 224.0.1.39
access-list 10 deny 224.0.1.40
```

» Use loopbacks whenever possible

```
interface loopback0
 ip address x.x.x.x 255.255.255.255
```

Admin : SNMP (1)

- **Simple Network Management Protocol**
  - v1 : RFC1157 uses community strings for authentication
  - v2 : RFC1441/1446 adds security (party) and get-bulk
  - v3 : RFC2274 adds integrity checking, encryption and user authentication
- **Known attacks/problems**
  - Admins use RW communities for management
  - Weak communities
  - Replay and DoS attacks
  - Information leak
  - Auto-discovery feature of management tools that “send” your community out of your network range (to external parties)

Admin : SNMP (2)

» IP level filtering

> Define an ACL and activate it on a per interface basis

```
interface Ethernet0/0
 access-group in 100
access-list 100 permit udp host 192.168.1.1 host 192.168.1.2 eq snmp
access-list 100 permit udp host 192.168.1.2 eq snmp host 192.168.1.1
access-list 100 deny udp any any eq snmp log-input
```

» Application level filtering

> Define an ACL and use it for application access control

> Use views to restrict the exposure

```
snmp-server community r3ad view cutdown RO 10
snmp-server community wr1te RW 10
snmp-server view cutdown ip.21 excluded
snmp-server enable traps <…>
snmp-server host x.x.x.x
snmp-server source loopback0
access-list 10 permit x.x.x.x
```

Admin : SNMP (3)

- **SNMP v3**
  - Define a user/group and what the group can do

```
snmp-server group engineering v3 priv read cutdown 10
snmp-server user nico engineering v3 auth md5 myp4ss priv des56 mydes56
snmp-server view cutdown ip.21 excluded
access-list 10 permit x.x.x.x
access-list 10 deny any log
```

- **Two security advisories**
  - The “hidden” ILMI community (show snmp community shows all communities)
  - Read-write community available with a read only access
  - SNMP-wide bug (ASN.1)

Admin : Secure Shell (1)

- **SSHv1 (client and server) support**
  - Routers : as of 12.1(1)T/12.0(10)S (go for an image with 3DES), scp as of 12.2T
  - Switches : CatOS 6.x

- **What are the risks/limitations ?**
  - Cisco's implementation is based on SSH v1 and suffered from the same bugs : key recovery, CRC32, traffic analysis (SSHow), timing analysis and attacks
  - You can't force 3DES only nor use keys
  - Fixed in 12.0(20)S, 12.1(8a)E, 12.2(3), ...

Admin : Secure Shell (2)

SSH configuration

```
hostname <hostname>
ip domain-name <domainname>
crypto key generate rsa
ip ssh timeout 60
ip ssh authentication-retries 3
```

scp configuration

```
ip scp server enable
```

Admin : IPsec (1)

» IPsec configuration

- > Deny all traffic except IPsec related/decrypted

```
interface xy
 ip address y.y.y.y 255.255.255.0
 ip access-group 100 in
access-list 100 permit udp host x.x.x.x host y.y.y.y eq 500
access-list 100 permit esp host x.x.x.x host y.y.y.y
access-list 100 permit ahp host x.x.x.x host y.y.y.y
access-list 100 permit ip <remoteLAN> <localLAN>
```

- > Define a SA (Security Association) : traffic to encrypt

```
access-list 110 permit ip x.x.x.x <wildcard> y.y.y.y <wildcard>
```

- > Define an IKE policy

```
crypto isakmp policy 1
 hash md5
 encryption 3des
 authentication pre-share
 ! DH group (1024 bits)
 group 2
crypto isakmp key <key> address y.y.y.y
```

Admin : IPsec (2)

» IPsec configuration

- > Define the transform-sets (tunnel mode is better, use transport with Win2K -- easier)

```
crypto ipsec transform-set 3desmd5 esp-3des esp-md5-hmac
```

- > Put all together in a crypto-map

```
crypto map mycryptomap 10 ipsec-isakmp
set peer y.y.y.y
set transform-set 3desmd5
match address 110
```

- > And affect it to an interface

```
interface xy
 crypto-map mycryptomap
```

Admin : local users/passwords

- **Local users**
  - Encryption type 7 is reversible, MD5 as of 12.1(8a)E
- **Enable secret**
  - Use MD5 (type 5)

```
service password-encryption
enable secret 5 <…>
```

- **Access method**
  - Remove telnet and enable SSH

```
service tcp-keepalives-in
line vty 0 4
 exec-timeout 0 60
 access-class 10 in
 transport input ssh
 transport output none
 transport preferred none
access-list 10 permit x.x.x.x
```

  - Don't forget the console and AUX port

AAA: Authentication / Accounting

» Authentication/accounting : RADIUS/TACACS+

```
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication enable default tacacs+ enable
aaa accounting exec default start-stop group tacacs+
ip tacacs source-interface loopback0
tacacs-server host x.x.x.x
tacacs-server key K3y
```

» Command accounting (TACACS+ only)

```
aaa accounting commands 15 default start-stop group tacacs+
```

AAA: Authorization

- **Privilege levels**
  - 1 (user EXEC "view only") to 15 (privileged EXEC "enable")
  - No intermediate levels on switches
  - Change the privilege level (reduces information disclosure and avoids a stepping stone)
  - A user can only see parts of the configuration he is allowed to change or gets a view-and-disconnect

```
privilege exec level 15 connect
privilege exec level 15 telnet
privilege exec level 15 ssh
privilege exec level 15 rlogin
privilege exec level 15 show logging
privilege exec level 15 show [ip] access-lists
username seeandgo privilege autocommand show running
```

- **Command authorization**
  - Only supported with TACACS+

AAA: Kerberos (1)

- **Cisco Routers**
  - Kerberized Telnet and password authentication using Kerberos (telnet, SSH and console)
  - Can map instance to Cisco privilege (locally defined)
  - Feature name : Kerberos V client support (Enterprise)
  - Not supported on all hardware (16xx, GSR, etc)

- **Cisco Switches**
  - Telnet only (SSH available as of 6.1 but w/o Kerberos support)
  - At least SE Software Release 5.x
  - Only supported on Catalyst 4K, 5K and 6K/6500 (with SE I, not SE II)

AAA: Kerberos (2)

» Kerberos on a router

```
aaa authentication login default krb5-telnet local
aaa authorization exec default krb5-instance
kerberos local-realm COLT.CH
kerberos srvtab entry host/...
kerberos server COLT.CH 192.168.0.14
kerberos instance map engineering 15
kerberos instance map support 3
kerberos credentials forward
line vty 0 4
ntp server 192.168.0.126
```

» Kerberos on a switch

```
set kerberos local-realm COLT.CH
set kerberos clients mandatory
set kerberos credentials forward
set kerberos server COLT.CH 192.168.0.82 88
set kerberos srvtab entry host/...
set authentication login kerberos enable telnet primary
set authentication enable kerberos enable telnet primary
set ntp client enable
set ntp server 192.168.0.11
```

ACLs (1)

- **IP filtering with ACLs**
  - Is not stateful and doesn't do any reassembly
  - log-input also logs the source interface and the source MAC address
  - Only the first fragment is filtered (unless you use the fragment keyword)
- **Well known ACL types**
  - Standard : source IP address only (1-99, 1300-1999)
  - Extended : limited to IP addresses, protocols, ports, ACK/RST ("established") bit is set, etc. (100-199, 2000-2699, "named" ACLs)

ACLs (2)

- **Other “kinds” of ACLs**
  - > TurboACL : uses a hash table, benefits when 5+ ACEs
  - > Reflexive : enables on-demand dynamic and temporary reply filters (doesn’t work for H.323 like protocols)
  - > Dynamic : adds user authentication to Extended ACLs
  - > Named : allows you to delete individual ACEs
  - > Time-based : adds a time-range option
  - > Context-Based Access-Control : “inspects” the protocol (helper/proxy/fixup-like), used in conjunction with ACLs
  - > MAC : filters on MAC address (700-799 for standard, 1100-1199 for extended)
  - > Protocol : filters on protocol type (200-299)

ACLs (3)

» Example : Extended ACL on a router

```
no access-list 100
access-list 100 permit <…>
access-list 100 deny tcp any range 1 65535 any range 0 65535 log
access-list 100 deny udp any range 1 65535 any range 0 65535 log
access-list 100 deny ip any any log-input
```

» ACLs on a Multi-Layer Switch

- > ACLs defined on Layer 3 (S/E/R/D) are pushed to the NMP (TCAM)
- > Traffic will not hit the MSCF if you don’t use log[-input], ip unreachables, TCP Intercept
- > VACLs (VLAN) : can filter IP level traffic and are pushed from the PFC to the switch

Router integrity checking (1)

- **Four steps to build a tripwire-like for IOS/CatOS**
  - 1. Store your routers and switches configurations in a central (trusted) repository (CVS for example)
  - 2. Get the configuration from the device (scripted telnet in Perl or expect, rsh, tftp, scp) or have the device send you the configuration (needs a RW SNMP access)

```
snmpset -c <community> <routerIP> .1.3.6.1.4.1.9.2.1.55.<tftpserverIP> s <filename>
```

  - 3. Check : automatically (cron/at job), when you see “configured by <xyz>” or a router boot in the logfile or when you get the “configuration changed” SNMP trap

Router integrity checking (2)

- **Four steps to build a tripwire-like for IOS/CatOS**
  - 4. Diff the configuration with your own script or use CVS/Rancid

- **Limitations and details**
  - You still have to trust the running IOS/CatOS (no Cisco "rootkit" yet) and your network (MITM attacks)
  - The configuration is transmitted in clear text over the network (unless you use scp or IPsec to encrypt the traffic)
  - Do not forget that there are two "files": startup-config and running-config
  - Do the same for the IOS/CatOS images
  - Cisco MIBs : CISCO-CONFIG*

Router integrity checking (3)

- **Cisco IOS rootkit/BoF/FS : is it possible ?**
  - Proprietary, closed source OS running on MIPS (newer models) or Mot68K (older models)
  - Closed source but “fork” from (BSD) Unix
    - (zlib/SNMP bugs :-)
  - ELF 32-bit MSB executable, statically linked, stripped
  - What is possible with remote gdb access :
    - gdb {kernel¦pid pid-num} ?
  - Is the ROMMON a good starting point (local gdb) ?

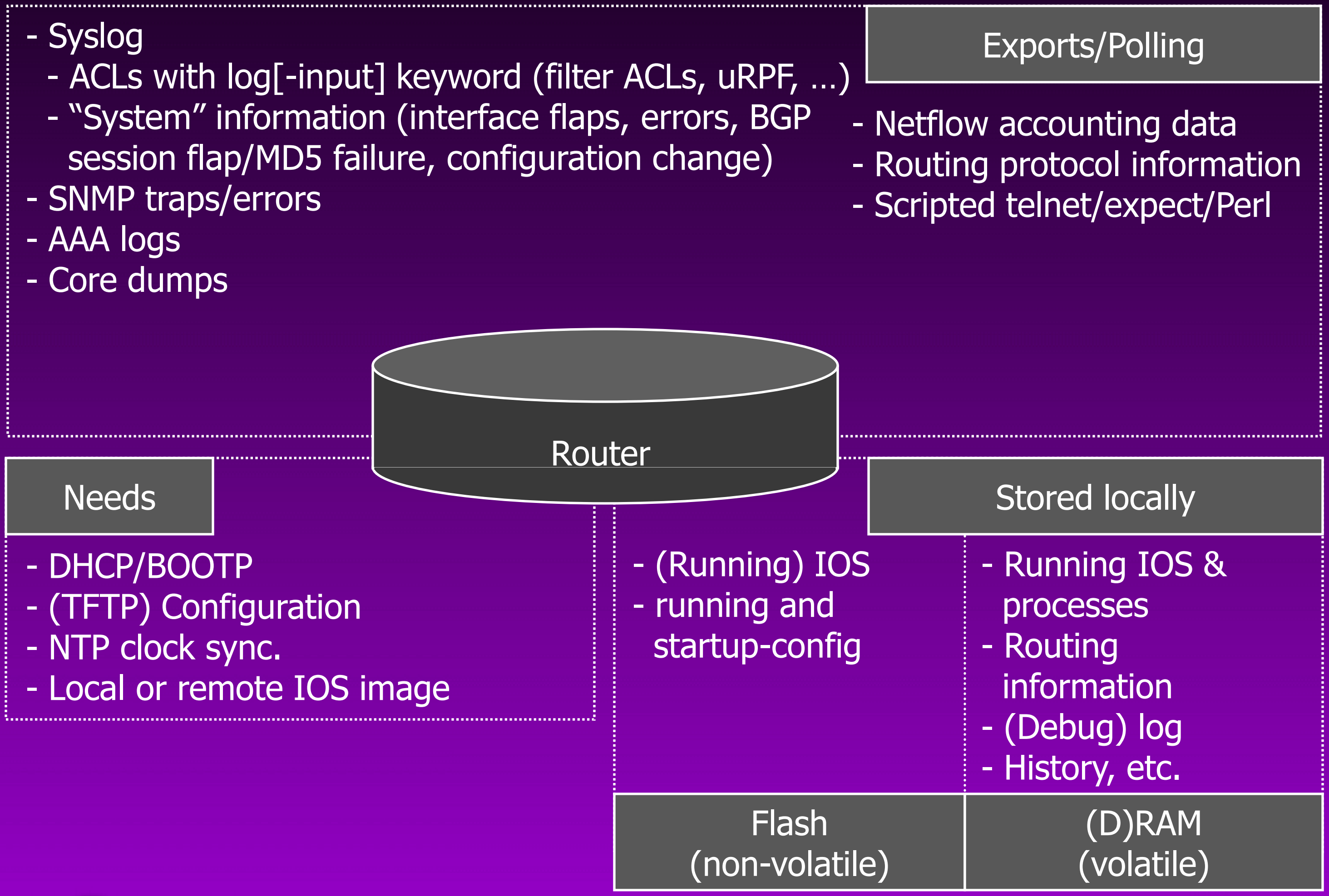
“Inside Cisco IOS software architecture” - Cisco Press :
- “In general, the IOS design emphasizes speed at the expense of extra fault protection”
- “To minimize overhead, IOS does not employ virtual memory protection between processes”
- “Everything, including the kernel, runs in user mode on the CPU and has full access to system resources”

Router integrity checking (4)

- **Cisco IOS rootkit/BoF/FS : open questions/issues**
  - No (known) local tools/command to interact and “play” with the kernel, memory, processes, etc.
  - What can be done in enable engineer mode ?
  - Is it possible to upload a modified IOS image and start it without a reboot (like “Linux two kernel monte”) ?
    - by using dual RPs (Route Processors) - stateful in the future
    - by upgrading LCs only (Line Cards)
  - A lot of different images exist (but providers usually go for ~12.0(x)S) and a tool to patch images would be required
    - 37 feature sets and 2500 images out there (90% IP FS)!
  - What will happen with IOS-NG (support for loadable modules) ?
    - Is Cisco still working on it ? GSR dedicated team ?

Router forensics (1)

» Architecture and data flows



- Syslog
  - ACLs with log[-input] keyword (filter ACLs, uRPF, …)
  - "System" information (interface flaps, errors, BGP session flap/MD5 failure, configuration change)
- SNMP traps/errors
- AAA logs
- Core dumps

Exports/Polling

- Netflow accounting data
- Routing protocol information
- Scripted telnet/expect/Perl

Router

Needs

- DHCP/BOOTP
- (TFTP) Configuration
- NTP clock sync.
- Local or remote IOS image

Stored locally

- (Running) IOS
- running and startup-config

- Running IOS & processes
- Routing information
- (Debug) log
- History, etc.

Flash
(non-volatile)

(D)RAM
(volatile)

Router forensics (2)

» **Checking your remote logs and accounting data**

» **Reading the flash card**

> ftp://ftp.bbc.co.uk/pub/ciscoflash/

» **What to do before/after reboot ?**

> Local buffers/logs

> Reboot with which config-register ? Normal or ROMMON ?

» **How to connect to the router ?**

> Telnet/SSH or local console ?

That's all folks :-)

- **Latest version of this document & presentation including tips/commands to secure routers (IOS) and switches (Cat(I)OS)**

  < http://www.securite.org/presentations/secip/ >

- **Questions ?**

Image: http://www.inforamp.net/~dredge/funkycomputercrowd.html