

Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 52
Evidence Collection in Switches and Routers

[FL] Welcome to this session on Network Security and Forensics. In the last two sessions, you would have seen the use of intrusion detection system like snort. We were looking at how to install snort and how to configure snort; what we will do in the next few set of lectures is that we will look at the switches, the routers, the firewall.

And then at the end we will also look at how to configure firewalls and this firewall is going to be a Linux based firewall we will be using our own see there we will see that there are different types of firewalls. And then we will be using our own Linux based firewalls we will be using something known as IP tables to fix the firewall configuration.

So, before that we will try to understand about switches what type of logs these kinds of switches provide? What type of log these kinds of routers provide? Many of these switches and routers you can either buy a commercial product or you could actually design your own switches or routers. Especially routers I mean you can use Linux as the OS there is something known as Zebra.

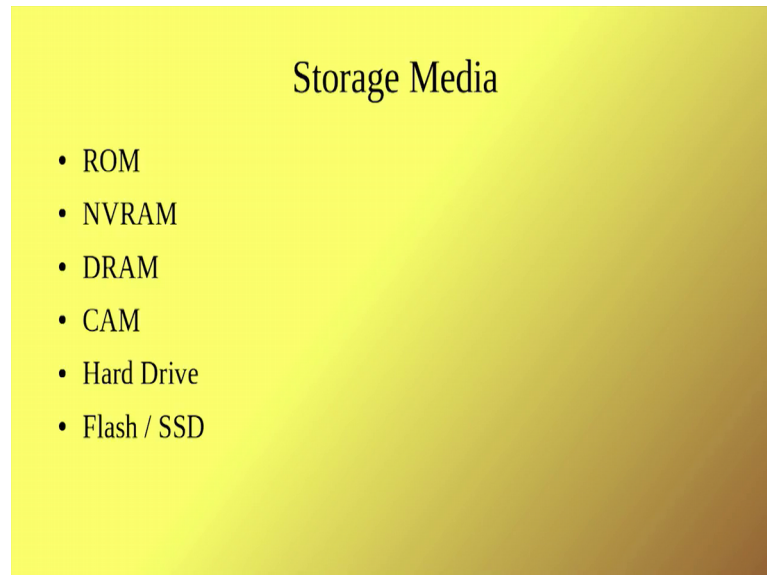
You can use Zebra OS and then build your own router why should this be important? Because sometimes; sometimes as a forensic person you do not want to trust some of the routers that you get from the vendor. So, you might have to I mean you might have to monitor certain data that flows through. So, what you could do is you could do is you put your router in between and just said those data to flow via your router and then capture the logs.

So, under such circumstance its better that as a forensic expert you have your own router which you can I mean many of the organization because it is something bad has happened they will allow you to do it and its better I mean you have a knowledge of your own router and of course that is not a part of this course.

So coming back to the switch, routers and then firewalls we had discussed very early during this network security course that sometimes you have to capture volatile data ok.

Now there are various types of storage media that you have to come across when you are trying to capture data.

(Refer Slide Time: 02:45)



One could be ROM read only memory and this is much more easier to get this data because its only read only then there is this non volatile ram then this DRAM dynamic ramsm then you have this content addressable memories, then you have a hard drives you might have flash or SSD.

Because now out of all these things ok. So, things like CAM DRAM all these two components at least they store something like the route tables or the IP tables they are used mostly for some type of caching the data or the routing tables. So, you will not have this value all along say for example, in a CAM Content Addressable Memory see it stores the routing table and routing table as you know could be dynamic.

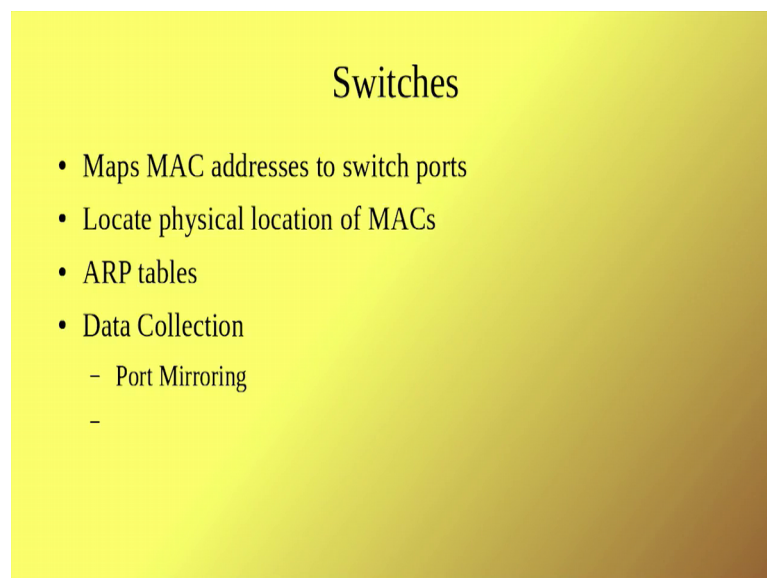
So if a particular route is not accessed to quite frequently the CAM actually move that route out or flush it out of its memory. And in that case you will actually lose the route which was there for some sometime, but then it has now disappeared because the system itself flush the route ok. So, this for example, someone might try to log I mean create a path for a short period of time to snoop into your data and once you do that this entry will actually get stored into a CAM.

So, for example, someone is trying to do the man in the middle at a CAM or a person in the middle at a CAM to be precise ok. And what you will do is you will try to connect this router and what happens is once you connect the router, the routing table gets updated ok. Now this routing table gets updated and gets stored in the CAM content addressable many for some time as long as the there is a data flow between this person's computer and the other router.

Once that connection is gone the value in the CAM will be retained for a short period of time and then it will be removed it is automatically flushed ok. There are commands in Cisco routers to look at the CAM tables, there are commands look at the routing tables and all these commands are there in Cisco routers; I mean it depends on who is your vendor juniper has its own set of commands COYS has its own sets of commands Cisco has its own set of commands.

So, you should be familiar with how to collect this kind of configuration stuff and once something bad has happened the hard drive; I mean you know the regular forensic take the hard drive out and things like that. So, let us come to the thee devices that we are going to look at we already had a brief look at firewalls, but we will go into some more details into firewalls and also do some kind of practice sections on firewall.

(Refer Slide Time: 05:51)



Before that let us look at switches what does the switch do? Ok a switch has bunch of ports. So, you could have a 8 port switch or a 16 port switch or a 64 port switch etcetera

and these switches maps the MAC address to the switch ports ok. So, the advantage and what usually the administrators do is; they will map these your device the physical location of your device to particular switch ports.

For example, if I have a switch port switch in my in this room all the computers will connect to that switch; that means, the switch is in a particular location and the computers that are connected to the switch can be identified to state that it is in this location for example, in this room ok. So, that is one advantage of having a switch switches ok; switches actually tell you sometimes what happens is that switches is in different places and then you get the connection, but whatever you do you can actually find out the physical location.

The second one is the ARP tables ARP which is Address Resolution Protocol; maps your IP addresses and the MAC addresses ok. So, the switches maintain this I mean these this what should I say I mean if I have a machine ok, I can actually look at this ARP the mapping within the IP address and the Ethernet address. For example, I configure Ethernet port in my machine and then I have my Ethernet address as well as the IP address. Now if I do a ping to some other machine I can take the Ethernet address and the IP address of the machine.

Now the point is the switch lies in between. So, it can tell you what where is that particular device is located ok. So, using this ARP tables and the switch together I will be able to physically identify for example, if it is an internal attack in the organization and the some other person in the other room is attacking my computer ok.

So, in that case I will be able to using the IP address the ARP tables and the switch; I will be able to identify which computer is attacking me. Usually with respect to switches you will collect the data by doing something known as port mirroring this is the very expensive activity ok. So, port mirroring is an activity by which any data that comes to us switch is replicated to another port ok.

And this replication rules can be defined like I mean do I want to replicate only certain flows? Do I want to replicate certain packets and so, on; so, this kind of replication rules can be set ok. So, this is one way usually you collect evidence in a switch by doing port mirroring. So, as I told you content acceptable memories are very important the CAM table is extremely volatile ok.

(Refer Slide Time: 08:52)

CAM Tables

- Very fast memory
- Maps MAC Addresses to physical switch ports
 - Switch looks up MAC in table
 - Writes packet to the correct port
- If an attacker is sniffing local traffic it will show up in the CAM table
- The CAM table is very volatile

And it maps the MAC address to physical switch boards. So, CAM table actually I mean it takes the there are various levels I mean you can use a IP address mapping etcetera in a router, but in this case it will map the MAC address to a switch board it is it is actually a very fast memory and as I told you previously if attacker is trying to enter into the network connecting his device.

This will actually show up in the CAM table ok. So, there are commands to view the CAM table; so, here is an example.

(Refer Slide Time: 09:30)

CAM Table

```
ant-fw# show switch mac-address-table
Legend: Age - entry expiration time in seconds

  Mac Address | VLAN | Type | Age | Port
-----|-----|-----|-----|-----
0008.7458.482b | 0001 | dynamic | 205 | Et0/5
000b.cdc2.e491 | 0001 | dynamic | 123 | Et0/3
0012.3f65.a7e1 | 0001 | dynamic | 287 | Et0/2
d0d0.fdc4.0994 | 0001 | static | - | In0/1
ffff.ffff.ffff | 0001 | static broadcast | - | In0/1,Et0/0-7
5475.d0ba.511e | 0002 | dynamic | 246 | Et0/0
d0d0.fdc4.0994 | 0002 | static | - | In0/1
ffff.ffff.ffff | 0002 | static broadcast | - | In0/1,Et0/0-7
Total Entries: 8
```

"Age" is the number of seconds left before the entry expires.

Ok show switch MAC address table and it tells you ok. So, it tells you the age; so, this is very important you see this is the entry expiration time and seconds. If someone has logged in; so, after certain point of time if logs out and there is no data that goes through in this ports say particular port ok, then this entry will be removed and therefore, you tend to lose this.

Therefore, if you are doing a live monitoring you might have to capture this data and store it somewhere. Now this tells you that what is the MAC address, what is the virtual LAN address and where is the dynamic learnt address ok? So, you switches actually you do dynamic learning of address and then what is the port, but it is connected and then what is the age of the entry.

So, how long this entry has been there in this table ok. So, such a information must be corrected; so, this is just one information you can do lot of show commands in the routers and then collect all these logs this is one log of CAM table, but you can take the show configure running config and all those things you can do this is with respect to Cisco router and for other routers the command might vary.

(Refer Slide Time: 10:48)

ARP Tables

- MAC address to IP address resolution
- Format of table entry
 - Location of the ARP request
 - IP Address
 - MAC address
 - Age in seconds from initial ARP request

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.1.215	(incomplete)				eth0
192.168.1.212	(incomplete)				eth0
diinkrouter.local	ether	3c:1e:04:0b:f6:f4	C		wlan0
gateway	ether	74:27:ea:26:28:ea	C		eth0
192.168.1.214	(incomplete)				eth0
192.168.1.213	(incomplete)				eth0
Entries: 6 Skipped: 0 Found: 6					

The next one is the address resolution protocol. So, in the right hand side we have just shown example of verbos description in Linux of what happens if you use a address resolution protocol. So, one of the things tells you is that it tells you what is the hardware type that you are using and the hardware address and then what is the interface.

So, even here you see there is a mapping between the port or the interface along with the MAC address. So, so similar to here; so, there is a port mapping along with the MAC address, so here there is a port mapping. So, in this way you can collect different logs and then start correlating ok. So, this ARP table is used for MAC address to IP address resolution.

So, you have you have port to MAC; MAC to IP address.

(Refer Slide Time: 11:38)

ARP Table

Cisco ASA 5505 firewall

```
ant-fw# show arp
inside 192.168.30.30 0008.742d.2f94 94
inside 192.168.30.100 0008.74fa.a6cc 99
inside 192.168.30.102 0012.7964.f718 470
inside 192.168.30.101 000b.cdc2.e491 480
inside 192.168.30.90 0008.74a0.2e02 4091
outside 172.30.1.5 0001.031a.d5f6 94
outside 172.30.1.254 5475.d0ba.522a 2160
dmz 10.30.30.20 0008.74d5.e0c4 409
```

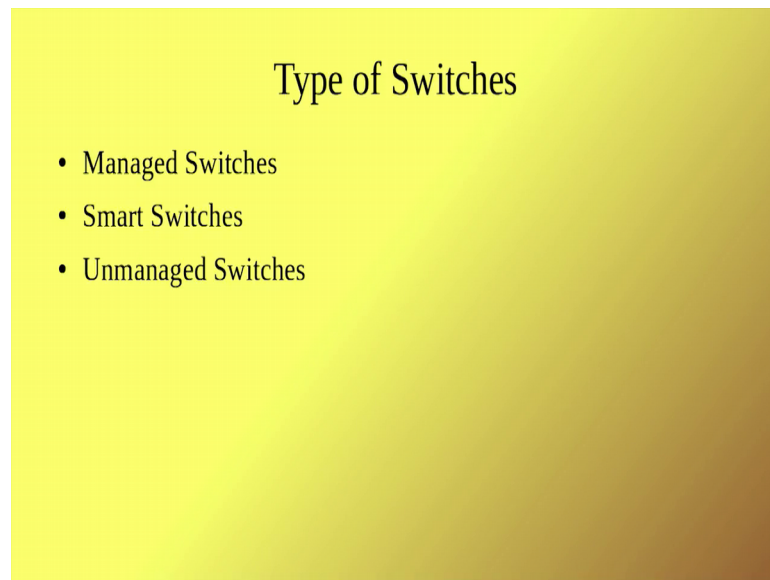
Ubuntu Server

```
$ arp -na
? (192.168.30.101) at 00:0b:cd:c2:e4:91 [ether] on eth0
? (10.30.30.20) at 00:08:74:d5:e0:c4 [ether] on eth1
? (172.30.1.5) at 00:01:03:1a:d5:f6 [ether] on eth2
? (172.30.1.254) at 54:75:d0:ba:52:2a [ether] on eth2
```

So, in a Cisco firewall ok; so, it this show ARP show something like this ok. So, in a firewall we are talking about it demilitarized zone, we are talking about an inside the address, we are talking about an outside address etcetera if you remember. So, it tells you all the details of what is the IP address ok, the inside IP addresses, the outside IP addresses and what is the port to which are the MAC address this internal IP address corresponds to etcetera.

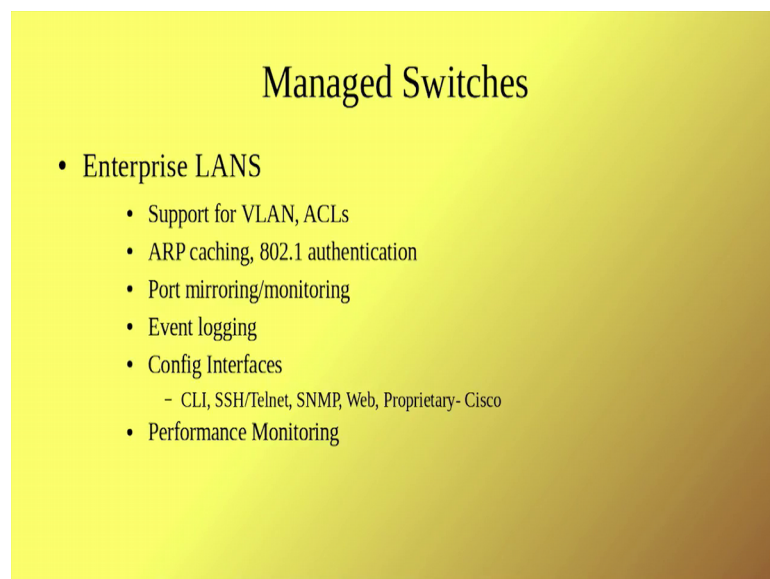
In a Ubuntu server you can get in various formats I showed you one of the format in the previous slide and this is another format depending on what command you use.

(Refer Slide Time: 12:17)



There are three types of switches that you might have to work with the easiest of them is are the switch that is going to give you a lot of problems in unmanaged switch where as to some extent you have a friendly managed switch and smart switch.

(Refer Slide Time: 12:36)



So, what is the difference between these three? Usually managed switches are quite expensive they are used in a enterprise LANS ok, it provides support for virtual LANS and the access control list, it also provides you ARP catching and authentication for

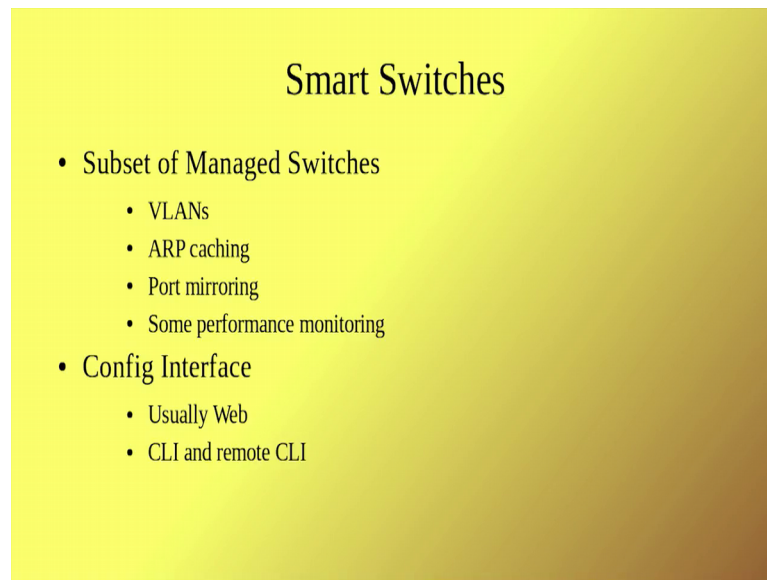
example, the switch can do tacacs or radius based authentication or diameter based authentication whatever it is.

These are configurable port mirroring and a sort of load balancing can also be done during port mirroring or monitoring see what I can do is ok. So, I have to do a live analysis for example, I want to dynamically find out any attack is happening or not. So, what I can do is I can actually take the band width of let us say 1 mega bits per second and then split it into say 500; 0.5 mega bits per second to each of the to the to the different ports and then mirror it.

So, this kind of stuff can be done because when you are doing deep packet inspection or something unide performance and you cannot be taking whole port and then mirroring and then trying to do a deep packet inspection you have to do it offline sometimes. So, you have to do it these managed switches have lot of capabilities ok. So, and they provide lot of locks; so, if you have a managed switch yes it will give you bunch of information ok.

And the advantage of managed switch is that it also provides various types of interfaces ok. You could have a web interface, you could have a template based interface or a shell secure shell etcetera and so, the advantage of managed switches is that it going to throughout lot of logs; it is going to be slightly more intelligent than your dumb switch that you might be using at your house. And this actually helps you with lot of forensic evidence I mean managed switches really dumb lot of information.

(Refer Slide Time: 14:31)

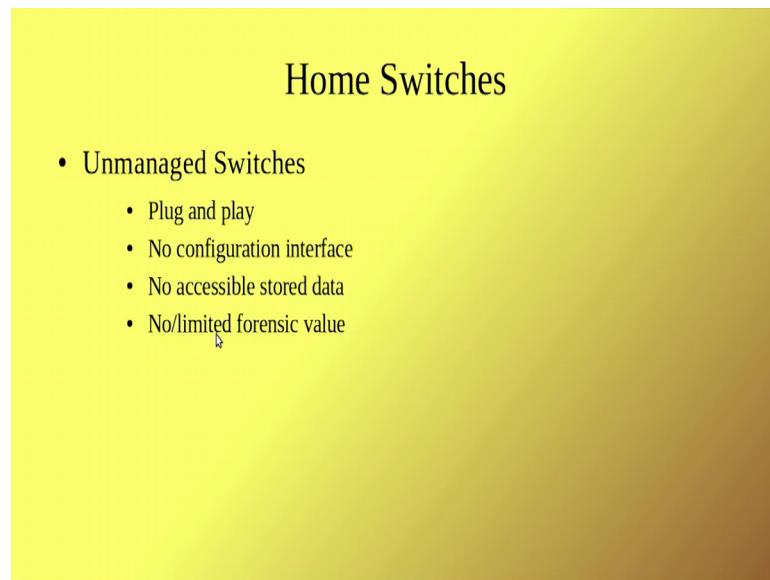


The next is smart switch ok; so, this is not as expensive as a managed switch, but then you it provides certain important features for example, VLANS ARP caching and port mirroring and some performance monitoring all these are part of the enterprise switch also. So, this could provide it usually provides the configuration interface like CLI and all those things I mean an example of this is something that you use in your sometimes this home routers.

So, what wireless routers that you like actually they may not some may not port mirroring may not be there, but there are at least it could have a ARP caching and then it could have some performance monitoring stuff ok. So, at least it tells you; what is the output band width; what is the input band width that is ok.

And definitely they provide you a nice CLI configuration I mean command line interface or web interface. Web interface usually the password is admin. So, you can break any of the wireless router by using this admin.

(Refer Slide Time: 15:35)

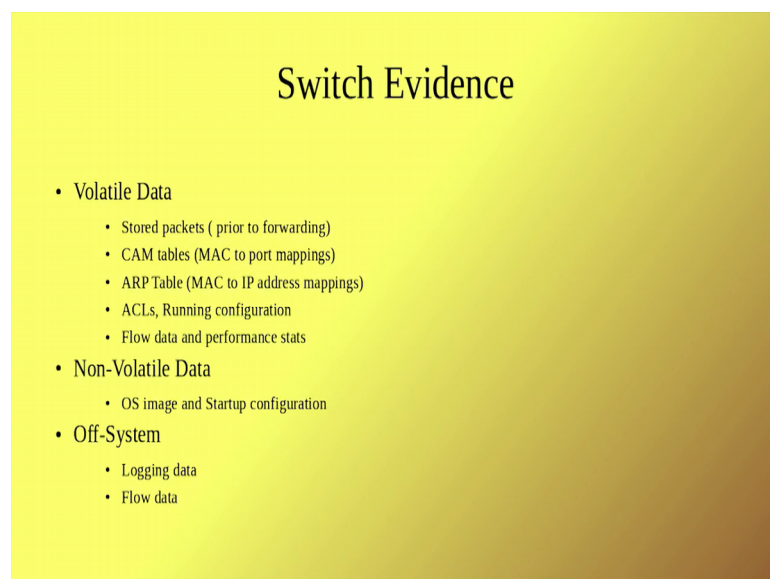


Home Switches

- Unmanaged Switches
 - Plug and play
 - No configuration interface
 - No accessible stored data
 - No/limited forensic value

Anyway sometimes you have switches that are unmanaged they are just plug and play switches similar to something like a hub that we use ok. So, if you want extend some Ethernet connection put and take a device connected to it and this is of limited or no forensic value. So, these kinds of devices are the least preferred if you a forensic person and make your life harder if you want to debug any problem. So, what are the evidence that we can get out of the switch?

(Refer Slide Time: 16:01)



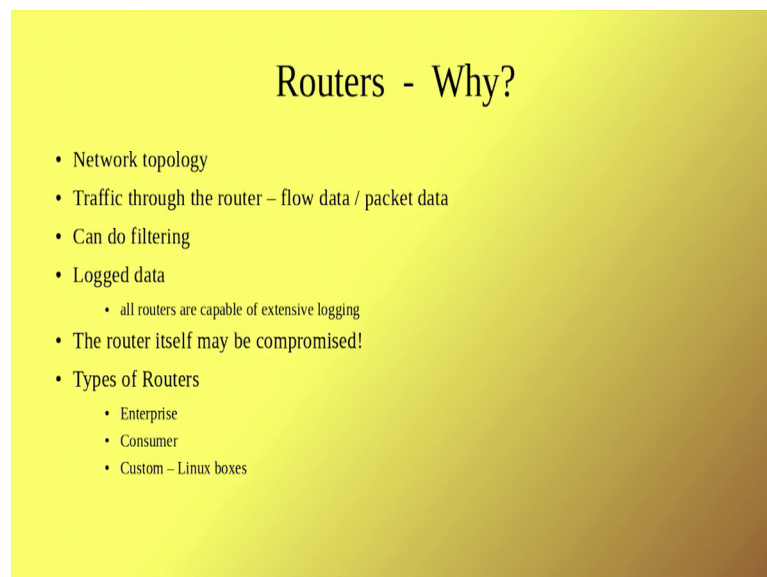
Switch Evidence

- Volatile Data
 - Stored packets (prior to forwarding)
 - CAM tables (MAC to port mappings)
 - ARP Table (MAC to IP address mappings)
 - ACLs, Running configuration
 - Flow data and performance stats
- Non-Volatile Data
 - OS image and Startup configuration
- Off-System
 - Logging data
 - Flow data

Switches usually have lot of volatile data; so, the problem we are going to face is that you might have to collect the data quite often and then store it somewhere. But something like a running configuration or access control list since you provided. These can be captured well these CAM tables ARP tables are all volatile data and sometimes stored packets see you cannot store all the packets. So, you might have to see something like there are two types of architectures one is store and forward architecture and things like that.

So, cut through and store and forward etcetera so, but then store and forward yes you could capture the packets, but in cut through you have to dynamically capture the packets extremely expensive. It could provide you some kind of flow and data performance statistics; the non volatile data that usually you have to acquire is the OS image because see in terms of legal evidence; you have to show that this version of image was running and. So, therefore, these vulnerabilities are there and things like that; so, it is always better to find out what version of image is there and take a back of it and you might have something like a logging data and flow data in some of the managed switches.

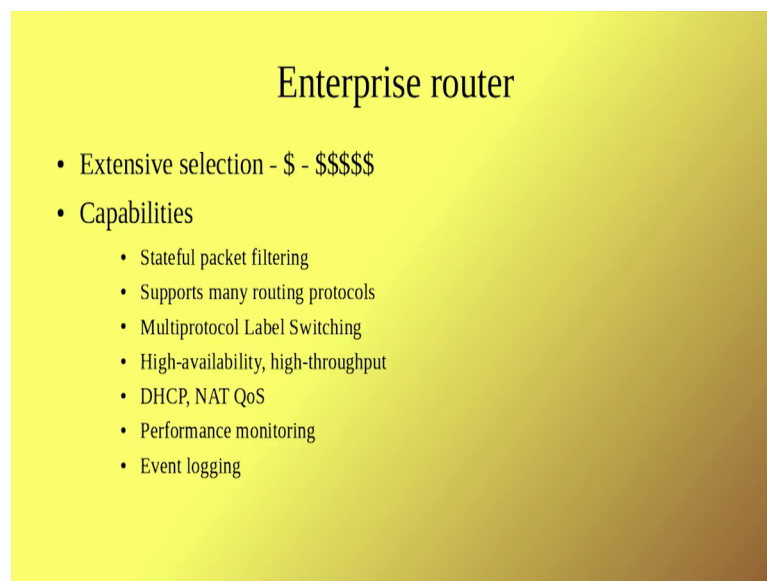
(Refer Slide Time: 07:15)



The next device that we have to look at is routers ok; routers actually the configuration of different types of routers gives you the network topology ok. And the traffic through the router allow flow data and packet data the advantage of routers is that it can do some kind of filtering and the log data all routers are capable of doing extensive logging.

They are capable of providing lot of configuration information sometimes the routers are. So, good that they myself they themselves could be compromised and there are three different types of routers as we done; one is the custom limit boxes as I was telling you could make your own router using Linux boxes and the other is the enterprise router and the customer consumer router. I mean if you go to a ISPS; they have different routers which I mean or capable of taking petabits per second kind of data flow; so, those are very complicated stuff ok.

(Refer Slide Time: 18:23)



So, enterprise router they are slightly expensive ok; the advantage of enterprise router is that they do something known as stateful packet filtering ok. So, what you could do is; so, you know this kind of flows go through certain kind of states for example, in TCP ok. So, what it does is it just it does a syn and then syn ack and then they gives a NAC and closing it says finish fin ack and things like that ok.

And while opening a connection it talks about syn and syn ack ok. So, these kind of you could actually say that I want to filter these kind of packets and these states in a protocol etcetera. So, this kind of stateful filtering for example, I want to monitor a sip based phone call ok. So, then I have to go for stateful filtering I have to take the ends system which are communicating, then I have to tell you that I have to show that this number was dialed and that number corresponds to such a person etcetera.

All these things and say there is connection established phase then once the connection is established I mean the data transfer happens I mean does not go away the controlling server etcetera; all these things have to be taken care. Because once they have to establish a state then have to establish that connection has happened after the state was set to connect etcetera all these things. So, in order to collect all those forensic evidences you might need a stateful filtering.

The next one is the support for many routing protocols ok. So, routers for example, if you just take a routing protocol like you could support a router could support BGP; it could it could support OSP of it could support ISIS, it could support RIP version 1, version 2 etcetera. So, its multiple routing protocol supports and each of the logs could be different you know a log that is generated for RIP different from the log that is generated form BGP.

So, you will have to take care of these aspects also the third is a router we may not actually use a routing protocol, but you will use something known as MPLS Multi Protocol Label Switching where you instead of using the IP address, you put some labels and then route the data based on labels to get faster switching times ok, then the configuration of MPLS and then. In fact, most of the routers use by ISPS use MPLS ok.

And so, you have to take the configuration of MPLS and things like that. These routers have high availability and high throughput they also provide NAC; NAC has been a vein when it comes to forensics because it is NAC can be managed by a local router and you have no idea of who has connected into the networks and NAC is something very difficult for a network forensic guide to work on ok.

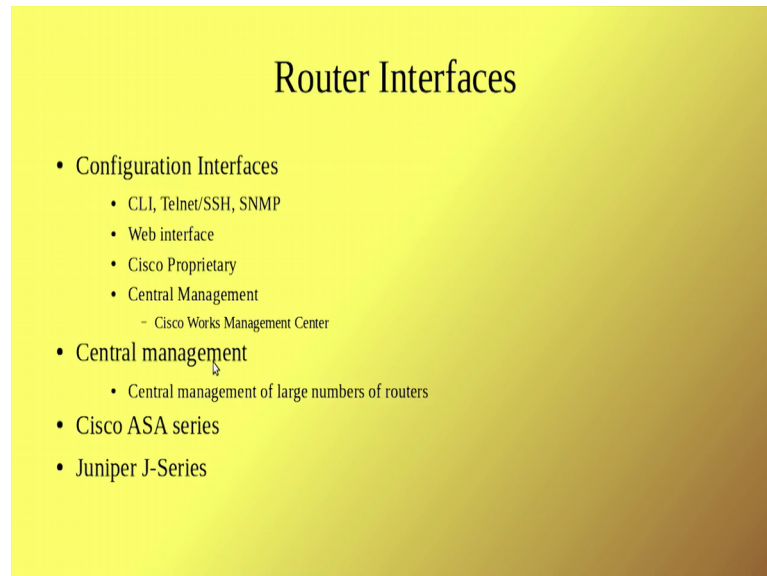
And then it can also do some kind of event logging and you can actually configure certain kind of triggers based on certain events one of the example is DDOS attack you see a large number of packets going to a particular destination then the router can trigger something like you know we are not expecting this kind of packet flow to the particular destination, but there is so, much of packet flow.

So, it can actually trigger a event and this event can be captured it could be kind of an alert that you sent to a management station so many of the times the ISPs themselves will prevent you from this kind of attacks because what happens is when such an attack happens the band width effective band width goes down and customer start complaining

etcetera. So, in order to avoid that problem they might have some kind of event logging mechanisms that they might provide.

So, these are some of the facilities that an enterprise router can have.

(Refer Slide Time: 22:12)



We will take a look at the other types of routers in the next section and we will also take a look at firewalls.

Thank you very much.