

Table des matières

Week1	3
Stateless Inspection.....	3
Stateful Inspection.....	5
Firewall Filters- IDS and IPS Systems	6
The Difference between IDS and IPS Systems	9
Network Address Translation.....	9
An Introduction to Local Area Networks	11
Ethernet and LAN - Ethernet Operations	16
Ethernet and LAN - Network Devices.....	20
Introduction to Basic Network Routing.....	25
Layer 2 and Layer 3 Network Addressing.....	26
Address Resolution Protocol	28
Routers and Routing Tables, Part 1.....	30
Routers and Routing Tables, Part 2.....	30
Routers and Routing Tables, Part 3.....	31
Research Network Vendor Training	33
Week 2	33
IP Addressing - The Basics of Binary.....	33
IP Address Structure and Network Classes.....	37
IP Protocol and Traffic Routing	39
Introduction to the IPv6 Address Schema	44
Application and Transport Protocols UDP and TCP, Part 1	46
Application and Transport Protocols UDP and TCP, Part 2	50
DNS and DHCP.....	56
Syslog Message Logging Protocol.....	61
Flows and Network Analysis	65
Port Mirroring and Promiscuous Mode	66
Next Generation Firewalls - Overview	67
NGFW and the OSI Model	69
NGFW Packet Flow Example and NGFW Comparisons	70
Intrusion Detection and Intrusion Prevention Systems	73
High Availability and Clustering	80
Week 3	84

Data Source Types Part 1.....	84
Data Source Types Part 2.....	85
Data Model Types.....	87
Structured Data.....	89
Securing the Crown Jewels.....	92
Leveraging Security Industry Best Practices	93
Structured Data and Relational Databases.....	93
Anatomy of a Vulnerability Assessment Test Report.....	95
Securing Data Sources by Type	95
Securing Databases Wrap Up	97
Data Monitoring	97
Data Alerts	101
Data Activity Reporting	106
Attributes to Include in Logging	111
Failed Access Monitoring.....	115
Failed Access Monitoring.....	117
Suspicious Access Events, Part 1	119
Data Breach Feeds.....	122
Data Breach Feeds.....	122
Week 4	123
Introduction to Injection Flaws	123
OS Command Injection Part 1	125
OS Command Injection Part 2	128
OS Command Injection Part 3	129
SQL Injection Part 1	131
SQL Injection Part 2	133
Other Types of Injection	137
Additional Resources.....	140
Additional Resources	140
OWASP Cheat Sheets.....	141
pentestmonkey.....	141
Database Hacker's Handbook: Defending Database Servers	141
Software Vulnerabilities	141
Common Attacks.....	141
Prevention Measures.....	142

Week1

Stateless Inspection

Networking Fundamentals

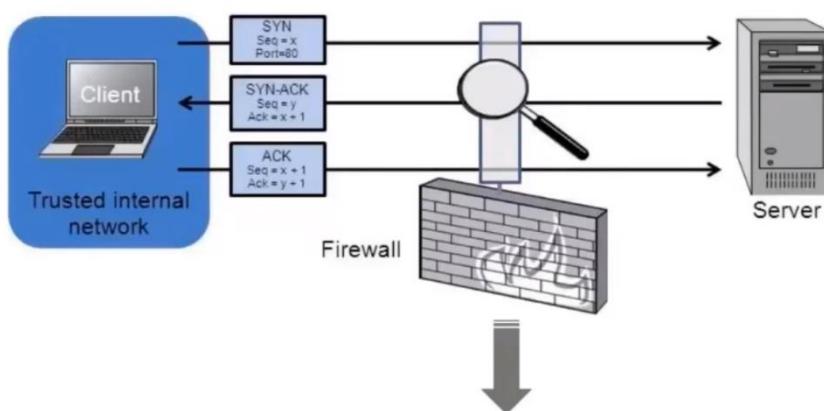
Basic Concepts of Networking Security

Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security

© 2020 IBM Corporation

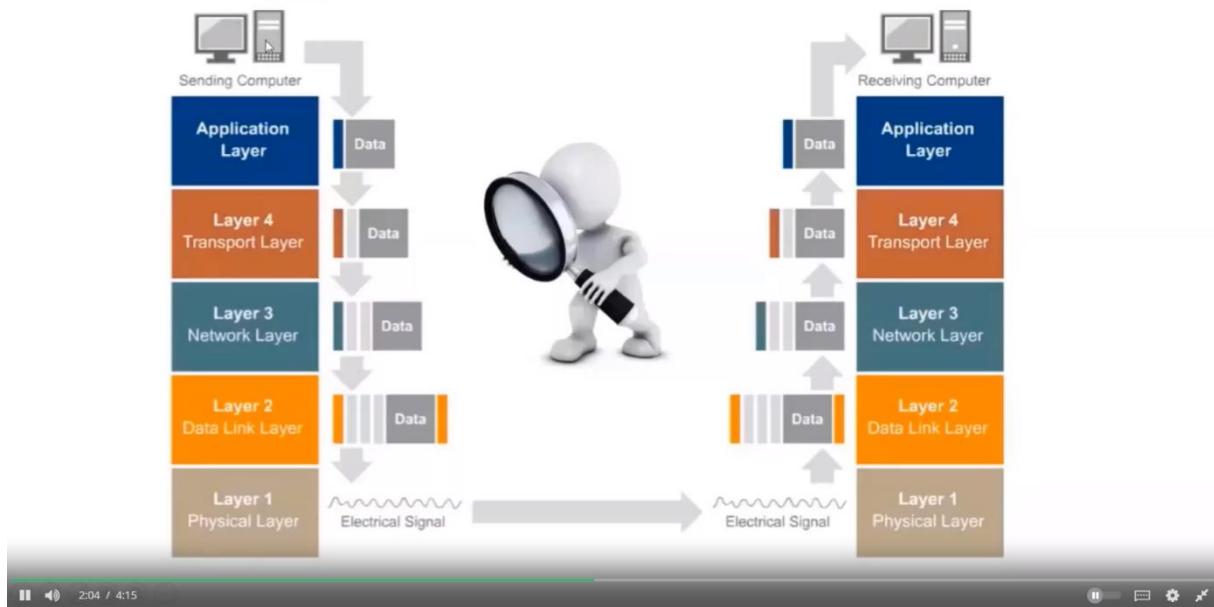
Stateless Inspection



It does not have a session table

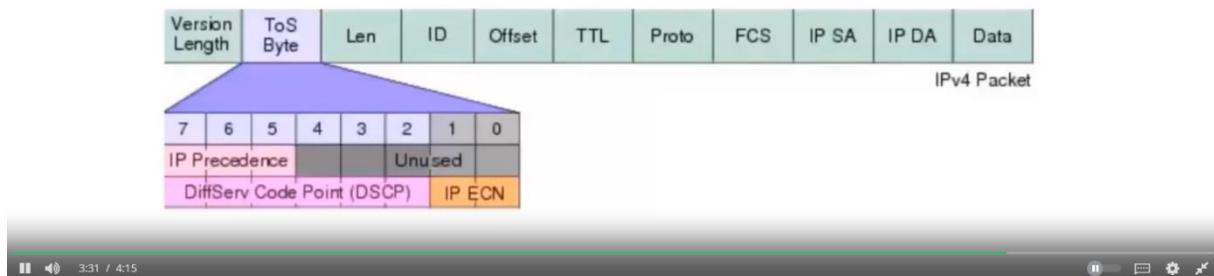


Stateless Inspection



Stateless Inspection Use Cases

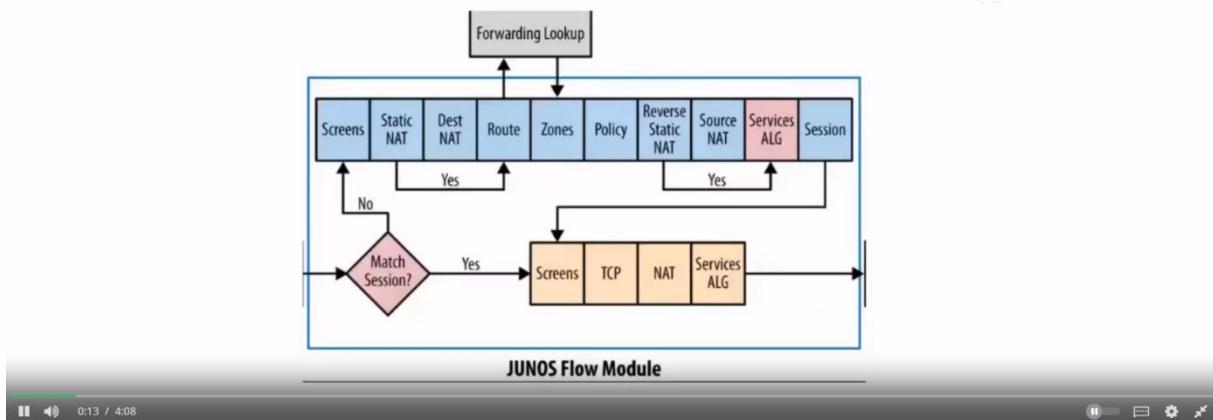
- To protect routing engine resources.
- To control traffic going in or out your organization.
- For troubleshooting purposes.
- To control traffic routing (through the use of routing instances).
- To perform QoS/CoS (marking the traffic).



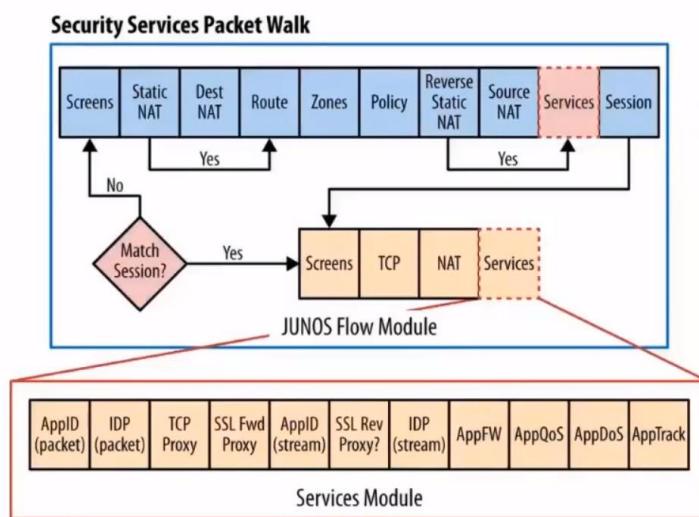
Stateful Inspection

Stateful Inspection

```
user@srx> show security flow session application telnet
Session ID: 57866, Policy name: intrazone-Juniper-SV/4, Timeout: 3394, Valid
In: 172.20.107.10:56290 --> 172.20.207.10:23;tcp If: vlan.107, Pkts: 27, Bytes: 1568
Out: 172.20.207.10:23 --> 172.20.107.10:56290;tcp, If: lt-0/0/0.1, Pkts: 21, Bytes: 1543
```

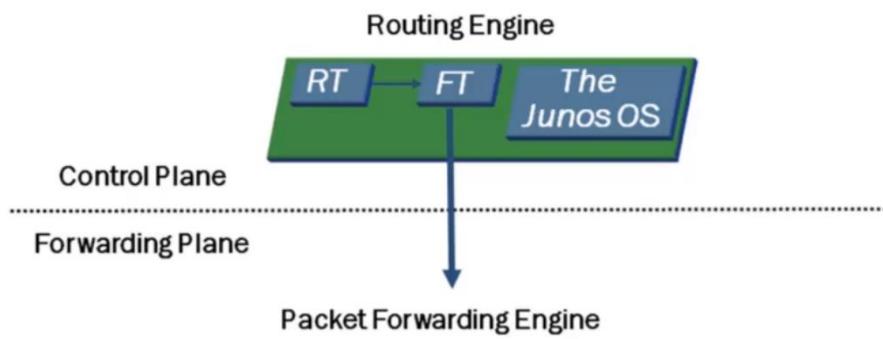


What if we have both types of inspection?



Firewall Filters- IDS and IPS Systems

Firewall Filter (ACLs) / Security Policies Demo...



Intrusion Detection System (IDS)

- An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.
- The IDS is a listen-only device.
- The IDS monitors traffic and reports its results to an administrator.
- Cannot automatically take action to prevent a detected exploit from taking over the system.

Basics of an Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.

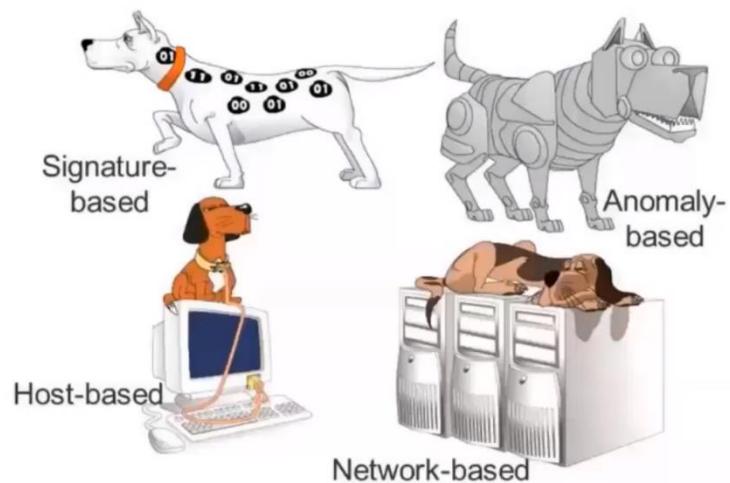
Basics of an Intrusion Prevention System (IPS)

The IPS often sits directly behind the firewall and it provides a complementary layer of analysis that negatively selects for dangerous content.



Unlike the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network.

How does it detect a threat?



The Difference between IDS and IPS Systems

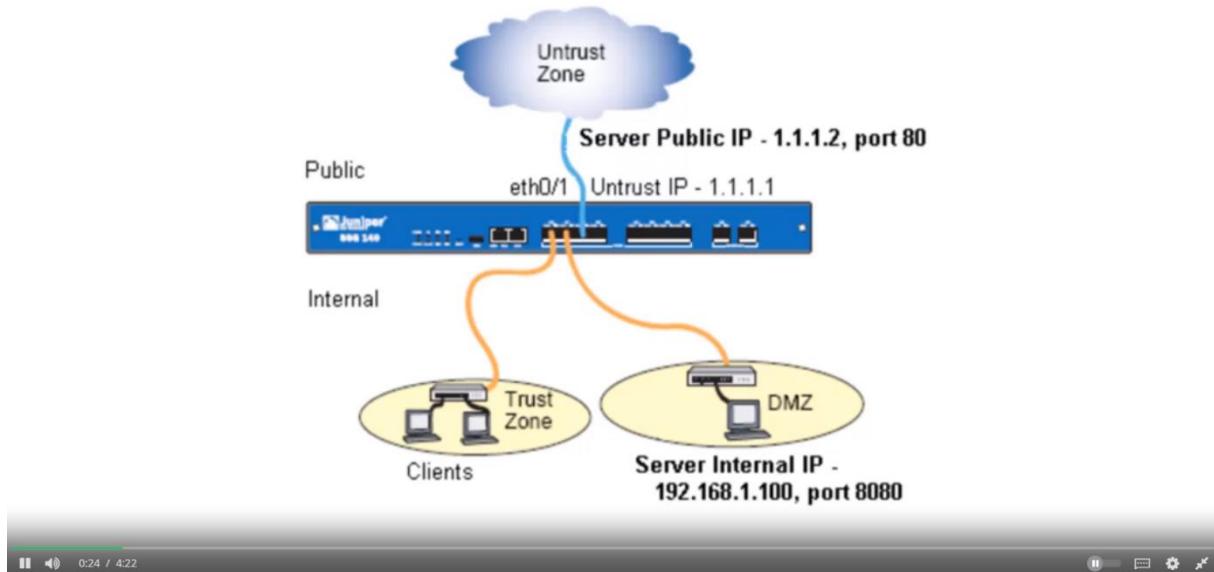
IPS vs IDS

	IPS	IDS
Placement in network infrastructure	Part of the direct line of communication (Inline)	Outside direct line of communication (offline).
System type	Active (monitors and automatically defend) and/or passive.	Passive (monitors and notifies).
Detection mechanism	<ol style="list-style-type: none">1. Statistical anomaly-based detection.2. Signature detection: Exploit-facing signature. Vulnerability-facing signatures.	1. Anomaly based.



Network Address Translation

Network Address Translation



Network Address Translation

- Method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
- Gives you an additional layer of security.
- Allows the IP network of an organization to appear from the outside to use a different IP address space than what it is actually using. Thus, NAT allows an organization with non-globally routable addresses to connect to the Internet by translating those addresses into a globally routable address space.
- It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network.

Types of NAT

→ **Static** address translation (static NAT): Allows one-to-one mapping between local and global addresses.

Dynamic address translation (dynamic NAT): Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.

Overloading: Maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). By using overloading, thousands of users can be connected to the Internet by using only one real global IP address.

An Introduction to Local Area Networks

Ethernet and Local Area Networks

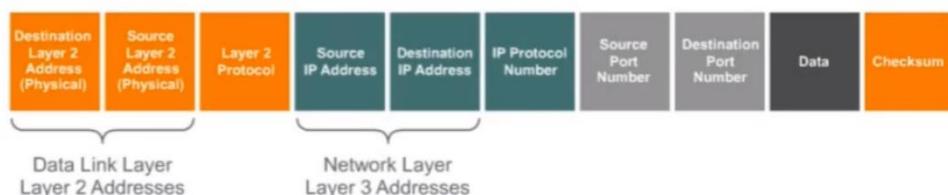
Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security



Objectives

- Describe how Ethernet networks work.
- Differentiate and understand the variety of network devices we have.
- Understand the difference between a collision and a broadcast domain.
- Describe the different ways we have to segment broadcast domains.
- Understand how the Virtual LANs or VLANs work on a Local Area Network.
- Introduce the 2 different addressing schemes we have on today's networks.



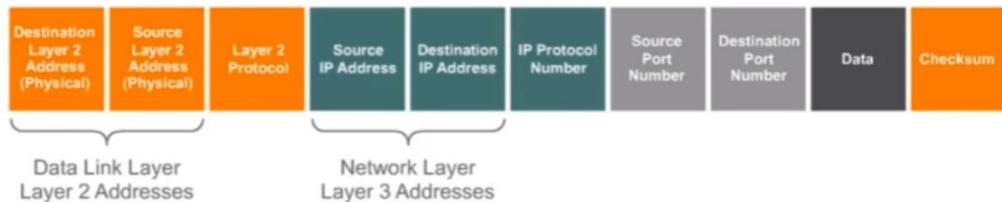
Source: <https://learningportal.juniper.net/>

Network Addressing Part 1

To understand how networks work, it is critical to understand the two different types of addressing networks use.

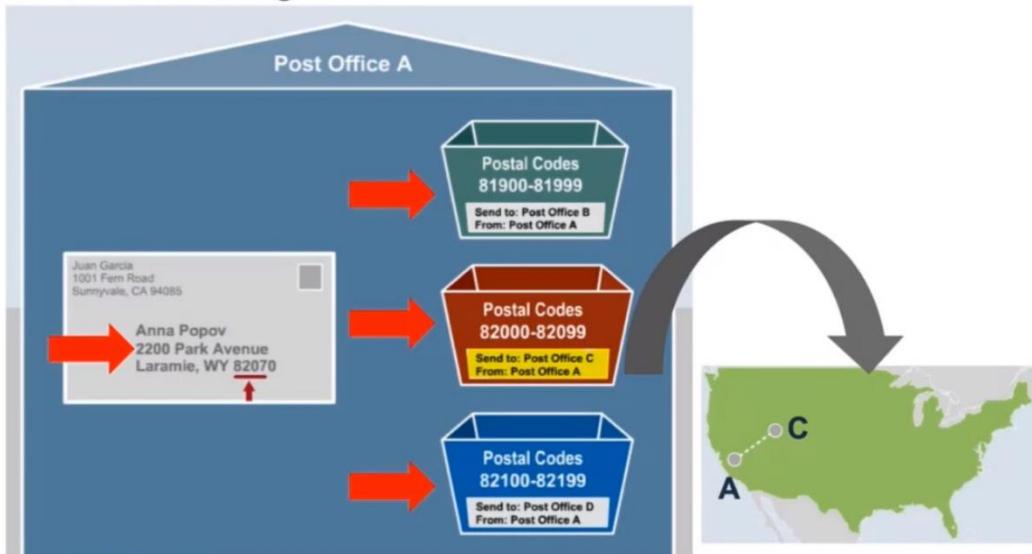
Layer 3 or network layer adds an address to the data as it flows down the stack; then layer 2 or the data link layer adds another address to the data.

Why do we have 2 different addresses?



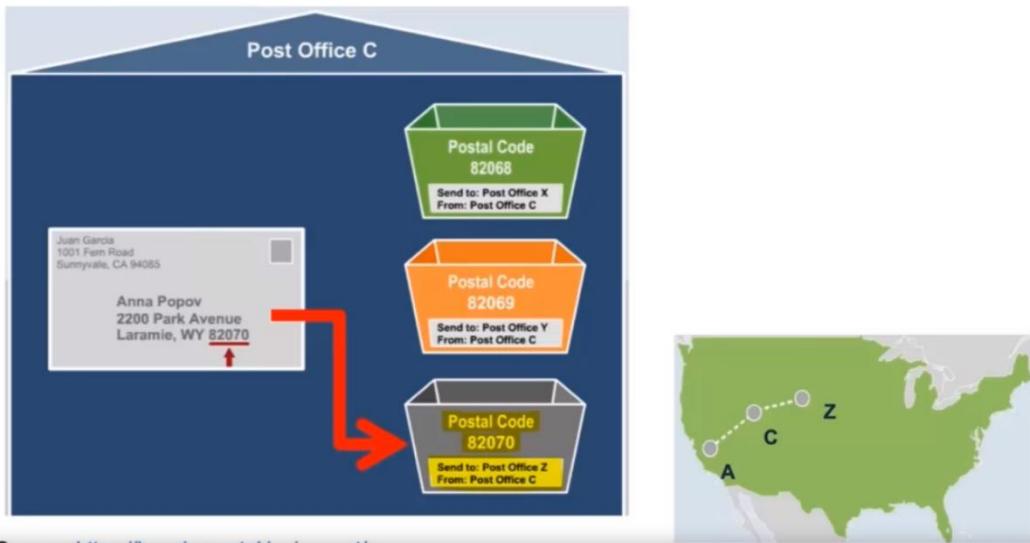
Source: <https://learningportal.juniper.net/>

Network Addressing Part 2



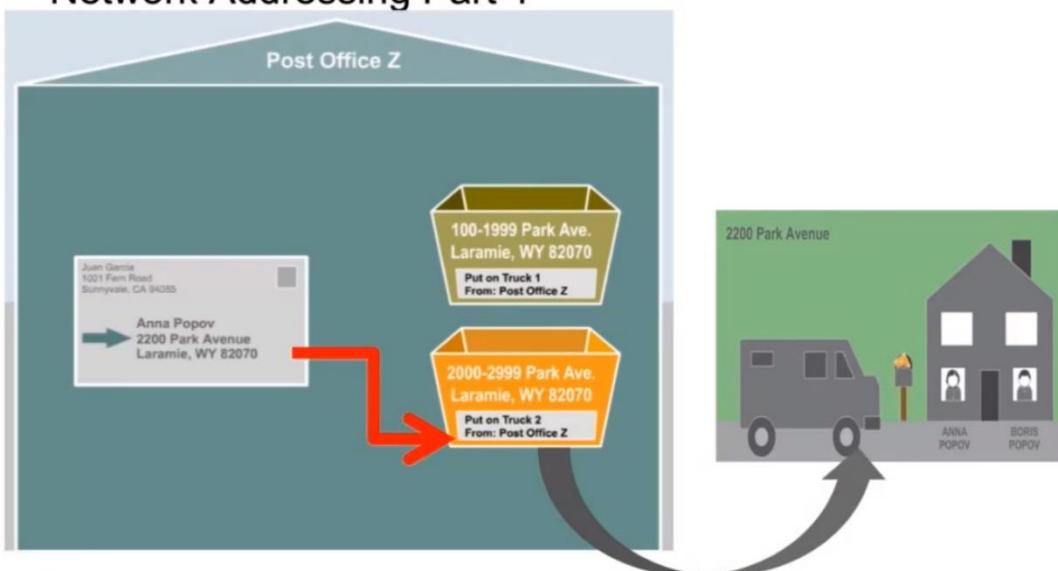
Source: <https://learningportal.juniper.net/>

Network Addressing Part 3



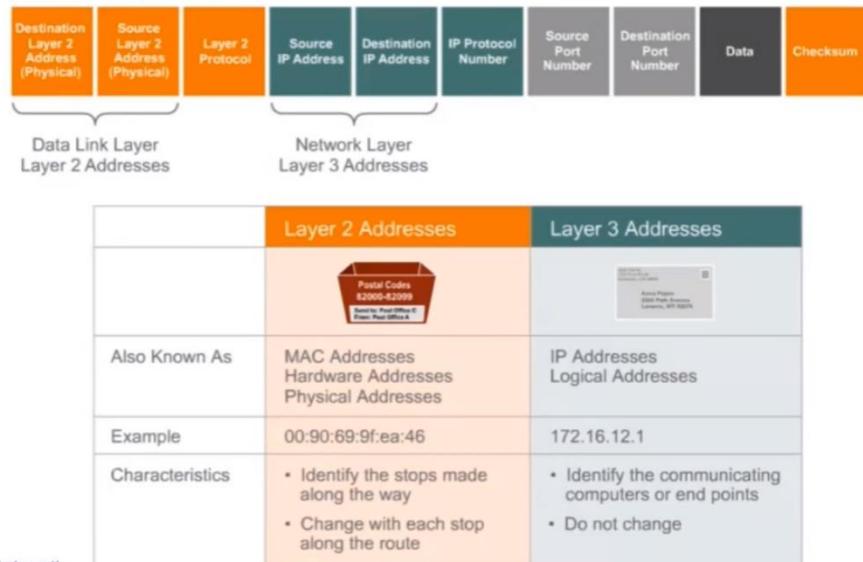
Source: <https://learningportal.juniper.net/>

Network Addressing Part 4



Source: <https://learningportal.juniper.net/>

Network Addressing Part 5

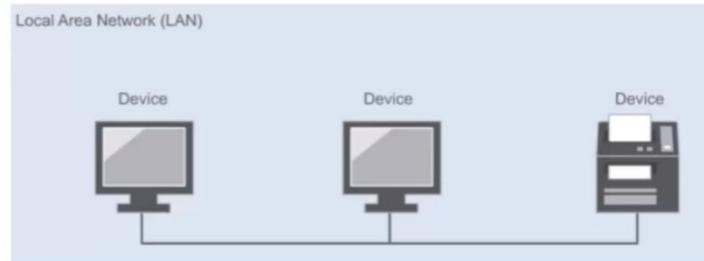


Source: <https://learningportal.juniper.net/>

Introduction to Ethernet Networks Part 2

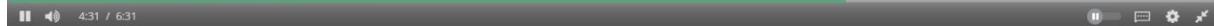
For a LAN to function we need:

- Connectivity between devices
- A set of rules controlling the communication

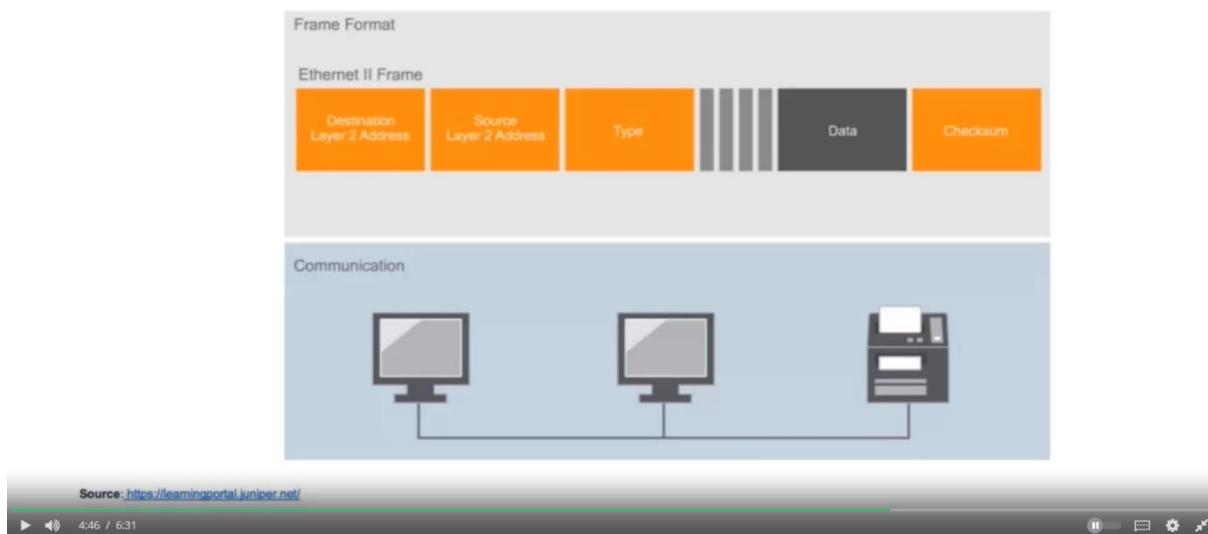


The most common set of rules is called Ethernet

Source: <https://learningportal.juniper.net/>



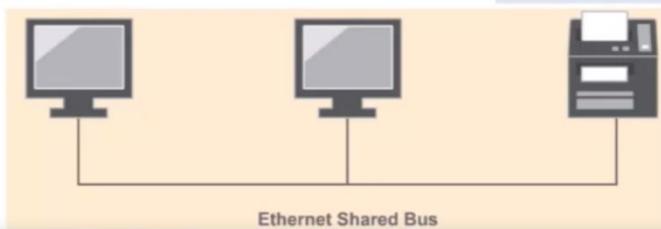
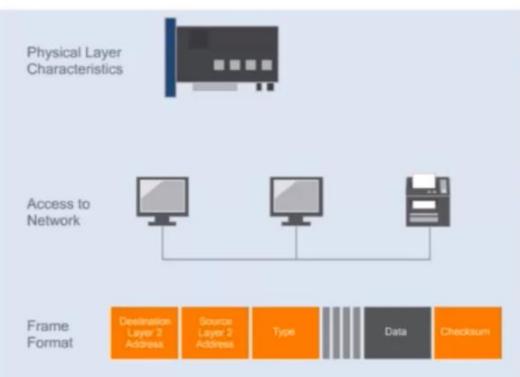
Introduction to Ethernet Networks Part 3



Ethernet and LAN - Ethernet Operations

Ethernet Operations Part 1

Ethernet standards include some components

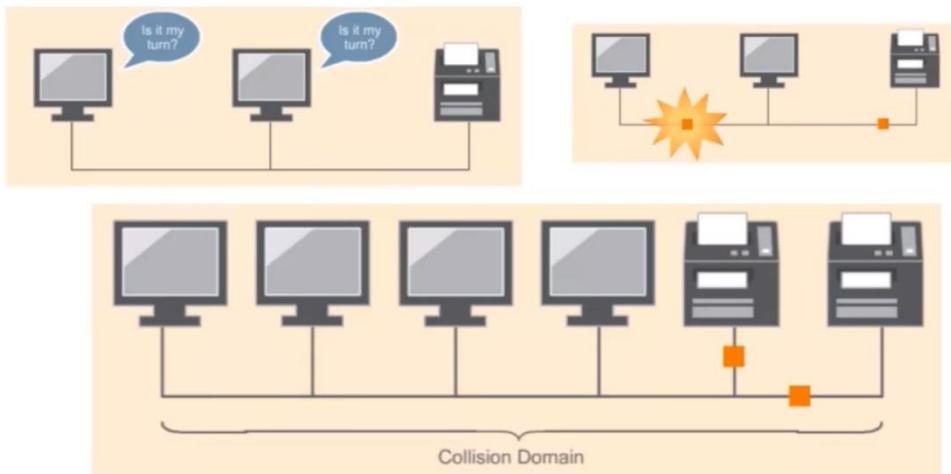


Source: <https://learningportal.juniper.net/>



Ethernet Operations Part 3

How do devices know when it is their turn to transmit data?



Source: <https://learningportal.juniper.net/>



Ethernet Operations Part 4

How do devices know when the data is for them?



Destination Layer 2 address: MAC address of the device that will receive the frame

Source Layer 2 address: MAC address of the device sending the frame

Type: Indicates the layer 3 protocol that is being transported on the frame such as IPv4
IPv6, AppleTalk, etc.

Data: Contains the original data as well as the headers added during the encapsulation process

Checksum: This contains a Cyclic Redundancy Check to check if there are errors on the data

Source: <https://learningportal.juniper.net/>

Ethernet Operations Part 5

Are the Preamble and Start Delimiter part of an Ethernet Frame?

The screenshot shows two network captures in Wireshark. The top capture (Frame 10) has an 'Ethernet II, Src: Apple_97:d0:1d (78:4f:43:97:d0:1d), Dst: Cisco-Li_b3:64:86 (c8:d7:19:b3:64:86)' frame with a 'Frame check sequence: 0xb89f90d3 [incorrect, should be 0xcb9603fe]' error. The bottom capture (Frame 12) has a similar structure but with a correct FCS status. A large downward-pointing arrow is positioned between the two captures, indicating a progression or comparison.

Frame 10 (Incorrect FCS)	Frame 12 (Correct FCS)
Frame 10: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0	Frame 12: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Apple_97:d0:1d (78:4f:43:97:d0:1d), Dst: Cisco-Li_b3:64:86 (c8:d7:19:b3:64:86)	Ethernet II, Src: Apple_97:d0:1d (78:4f:43:97:d0:1d), Dst: Cisco-Li_b3:64:86 (c8:d7:19:b3:64:86)
> Destination: Cisco-Li_b3:64:86 (c8:d7:19:b3:64:86)	> Destination: Cisco-Li_b3:64:86 (c8:d7:19:b3:64:86)
> Source: Apple_97:d0:1d (78:4f:43:97:d0:1d)	> Source: Apple_97:d0:1d (78:4f:43:97:d0:1d)
Type: IPv4 (0x0800)	Type: IPv4 (0x0800)
> Frame check sequence: 0xb89f90d3 [incorrect, should be 0xcb9603fe]	> Frame check sequence: 0xcb9603fe [correct]
[FCS Status: Bad]	[FCS Status: Good]
> Internet Protocol Version 4, Src: 192.168.1.47, Dst: 54.227.194.207	> Internet Protocol Version 4, Src: 192.168.1.47, Dst: 54.227.194.207
> Transmission Control Protocol, Src Port: 55000, Dst Port: 443, Seq: 1, Ack: 1, Len: 59	> Transmission Control Protocol, Src Port: 55000, Dst Port: 443, Seq: 64, Ack: 64, Len: 0

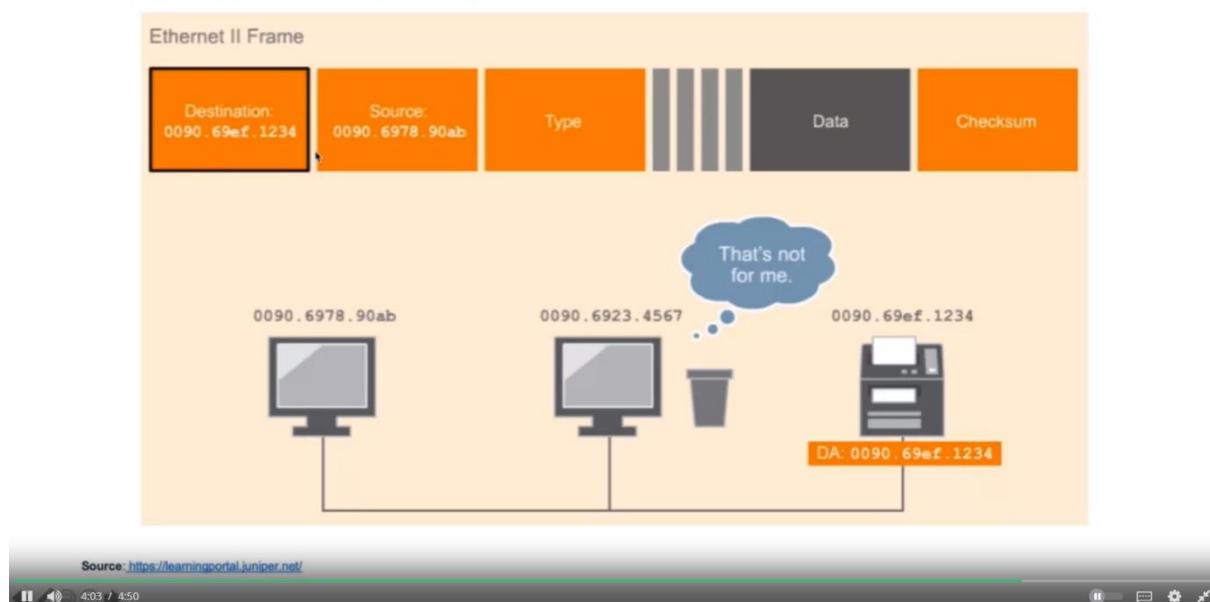
Ethernet Operations Part 6

MAC Address

A MAC address is a 48-bit address that uniquely identifies a device's NIC.
First 3 bytes are for the OUI and last 3 bytes are reserved to identify each NIC.

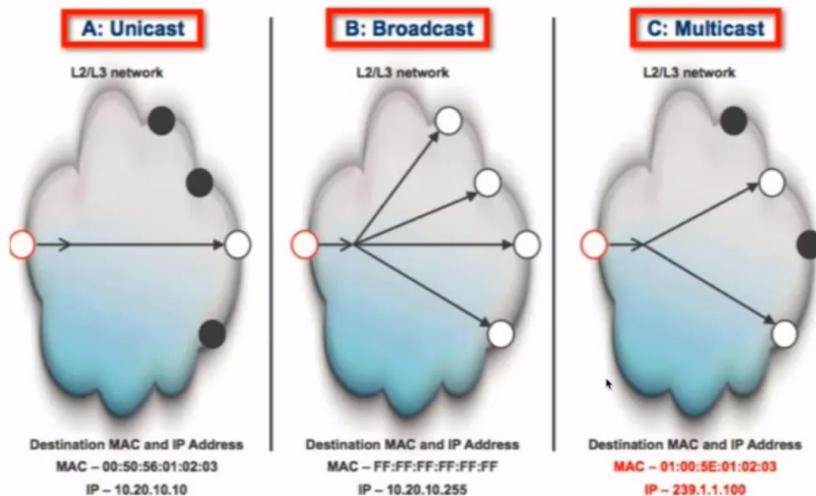


Ethernet Operations Part 7



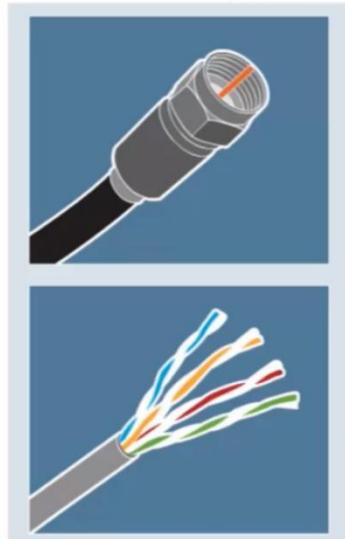
Ethernet Operations Part 8

What if I need to send data to multiple devices?



Source: <http://blogs.vmware.com/vsphere/2013/05/vxlan-series-multicast-basics-part-2.html>

Ethernet and LAN - Network Devices



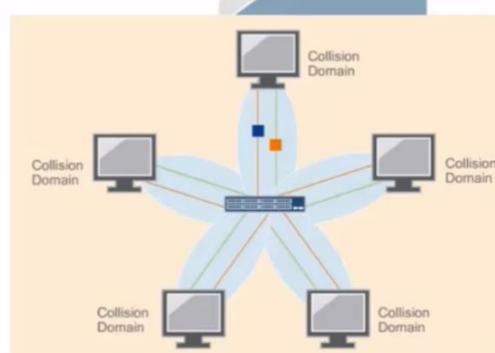
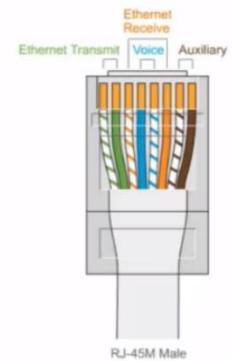
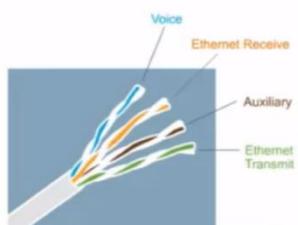
Coaxial Cable

Twisted Pair Cable

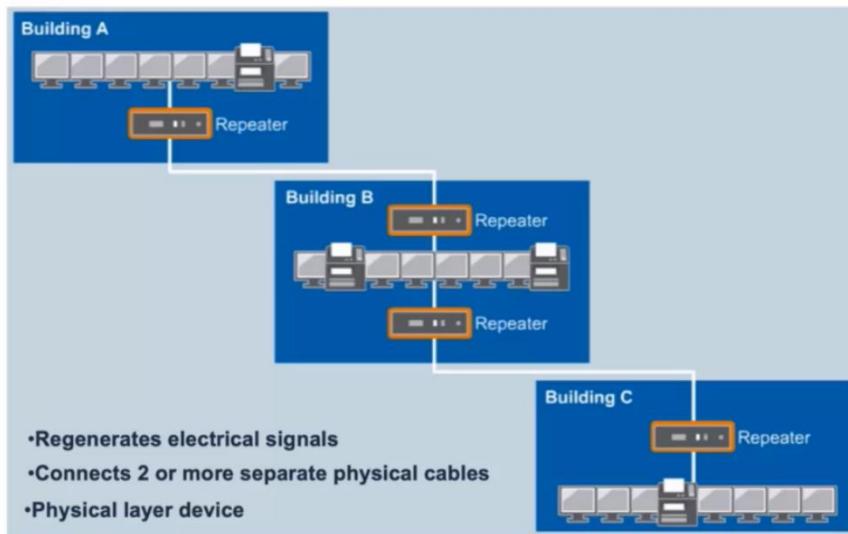
Source: <https://learningportal.juniper.net/>

0:20 / 5:06

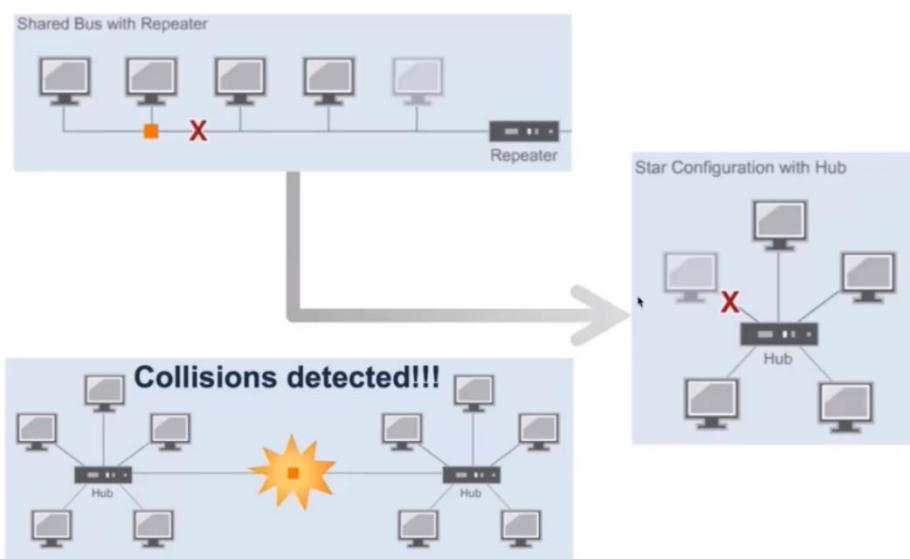
Twisted Pair cabling

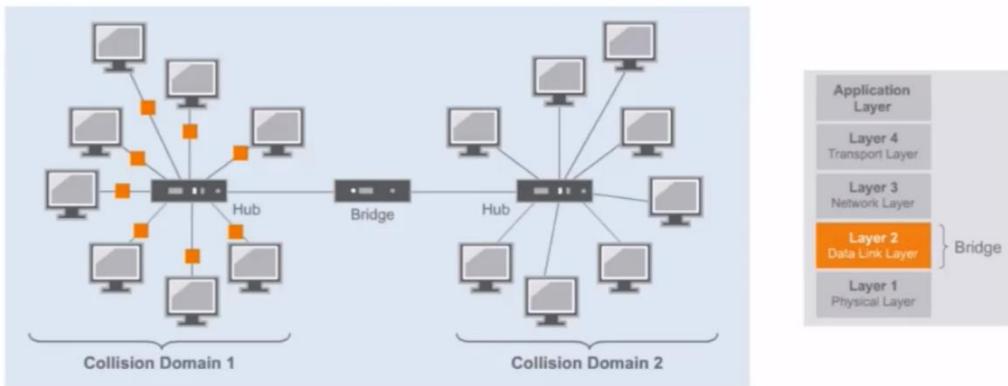


Source: <https://learningportal.juniper.net/>



Source: <https://learningportal.juniper.net/>

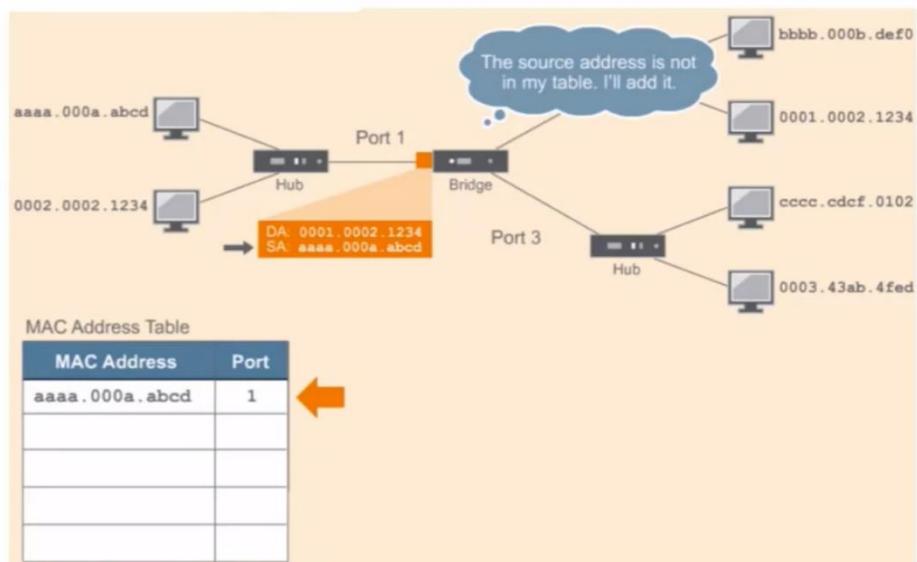




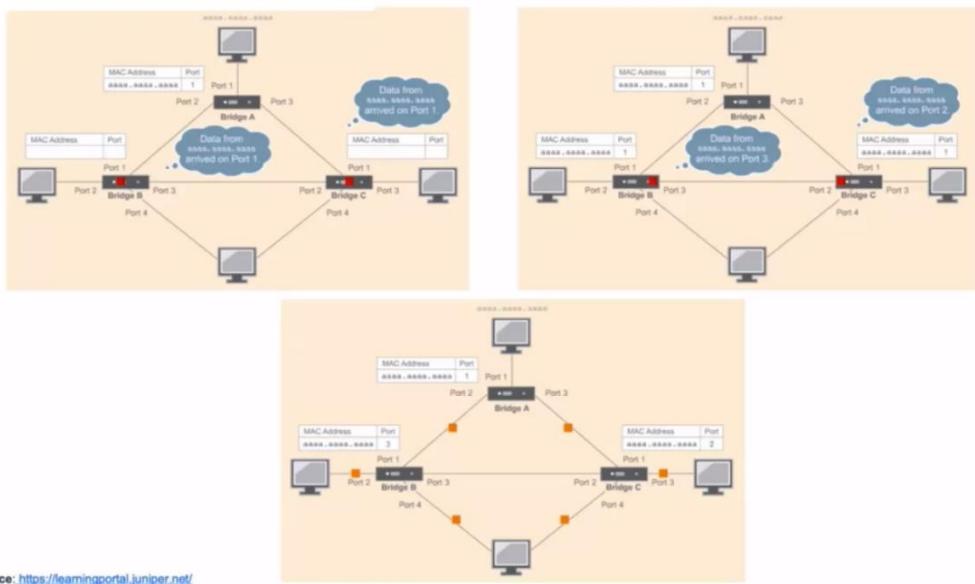
Ethernet bridges has 3 main functions:

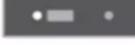
- Forwarding frames
- Learning MAC addresses
- Controlling traffic

Source: <https://learningportal.juniper.net/>



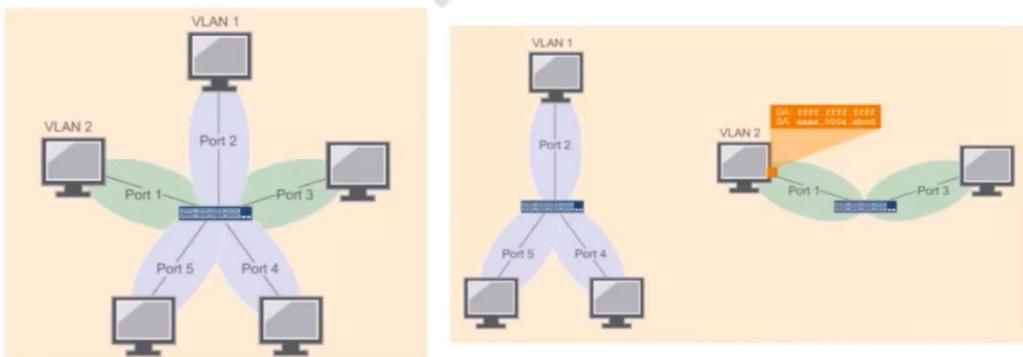
Source: <https://learningportal.juniper.net/>



 Bridge	 Switch
Half-duplex data transmission	Full-duplex data transmission
End-user devices share bandwidth on each port	Each port is dedicated to a single device; bandwidth is not shared
Virtual LANs are not possible	Virtual LANs are possible

Source: <https://learningportal.juniper.net/>

- VLANs provide a way to separate LANs on the same switch.
- Devices in one VLAN do not receive broadcast from devices that are on another VLAN.

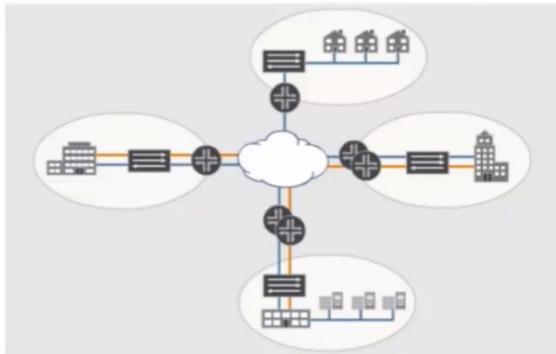


Source: <https://learningportal.juniper.net/>

|| 4:19 / 5:06

Limitations of switches:

- Network loops are still a problem
- Might not improve performance with multicast and broadcast traffic
- Cannot connect geographically dispersed networks.



Source: <https://learningportal.juniper.net/>



Introduction to Basic Network Routing

Basics of Routing and Switching, Network Packets and Structures

Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security



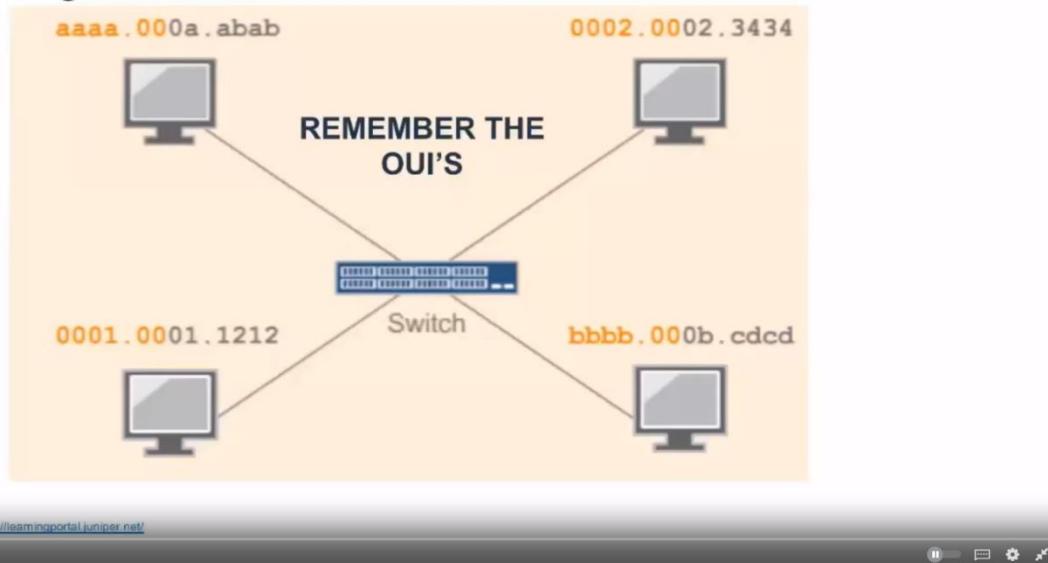
Objectives

- Understand Layer 2 and Layer 3 addressing
- Understand the interconnection of broadcast domains using Layer 3 devices
- Describe the ARP protocol
- Understand packet forwarding through different broadcast domains

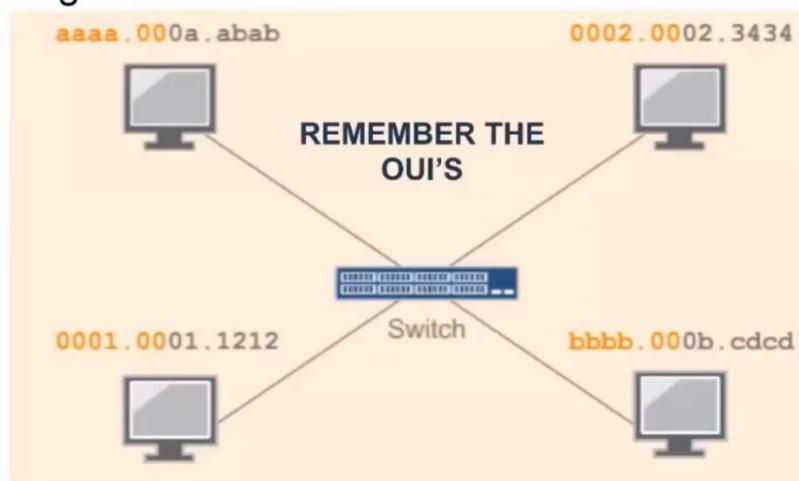


Layer 2 and Layer 3 Network Addressing

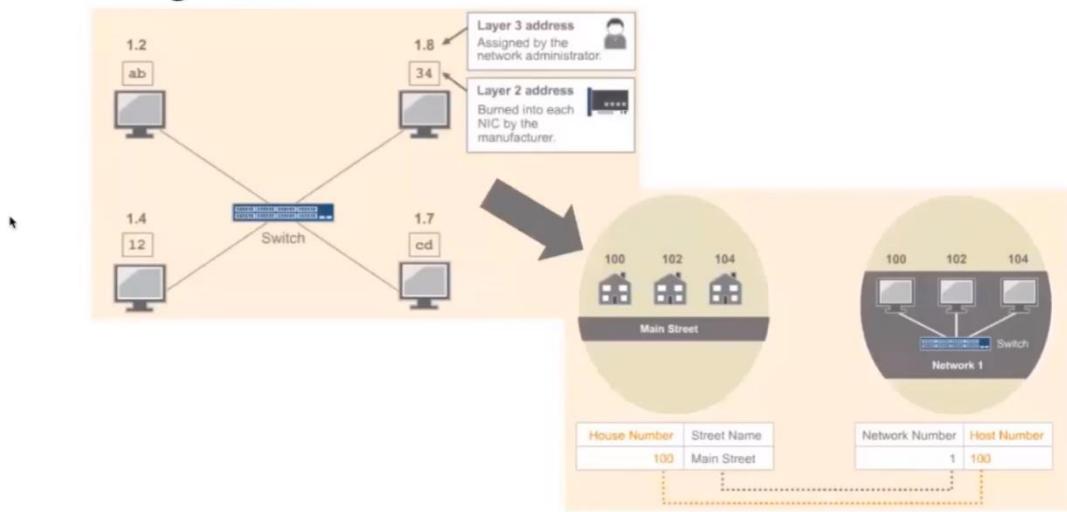
Layer 2 and Layer 3 Addressing



Layer 2 and Layer 3 Addressing



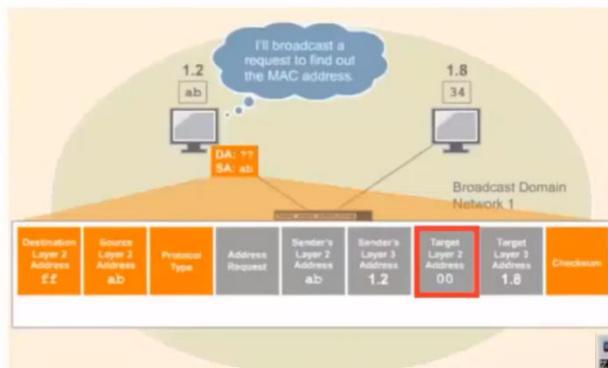
Layer 2 and Layer 3 Addressing Part 2



Source: <https://teamingportal.juniper.net/>

Address Resolution Protocol

Address Resolution Protocol



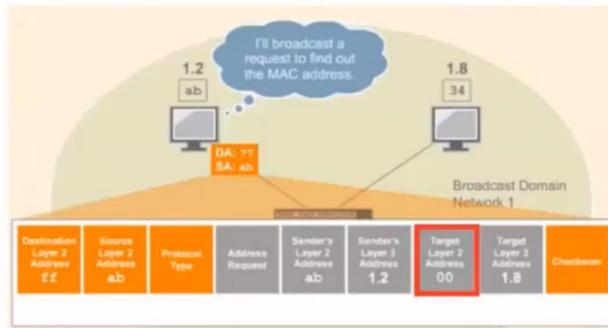
The process of using layer 3 addresses to determine layer 2 addresses is called ARP or Address Resolution Protocol.

ARP TABLE

```
C:\WINDOWS\system32\cmd.exe
Z:\>arp -a
Interface: 10.253.15.72 --- Bx4
Internet Address Physical Address Type
10.253.1.2 00-12-3f-ed-3f-2c dynamic
10.253.1.6 00-13-72-51-d5-a9 dynamic
10.253.1.10 00-03-ff-1f-7f-e9 dynamic
10.253.1.18 00-03-ff-36-9b-00 dynamic
10.253.1.25 00-11-43-de-91-15 dynamic
10.253.1.26 00-11-43-97-97-fc dynamic
10.253.1.27 00-15-22-17-98-07 dynamic
10.253.1.35 00-14-22-17-98-91 dynamic
10.253.1.80.1 00-15-23-46-50-00 dynamic
10.253.1.80.2 00-09-0f-83-3b-8a dynamic
```

Source: <https://learningportal.juniper.net/>

Address Resolution Protocol



The process of using layer 3 addresses to determine layer 2 addresses is called ARP or Address Resolution Protocol.

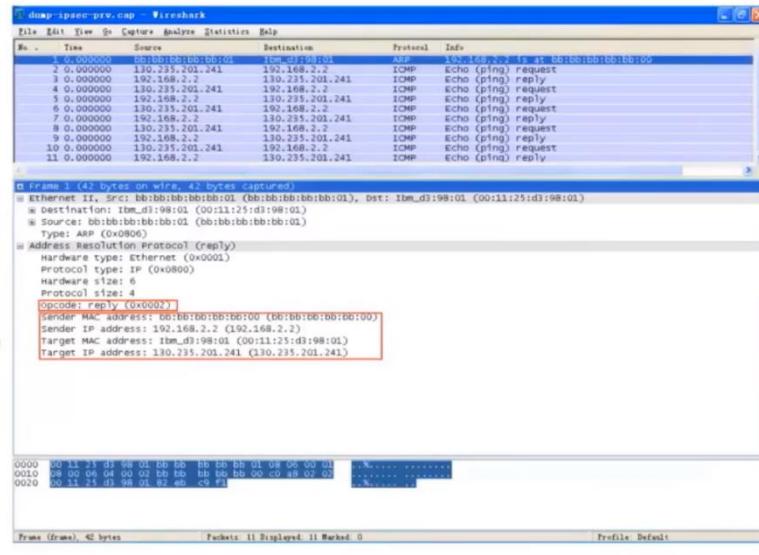
ARP TABLE

```
C:\WINDOWS\system32\cmd.exe
Z:\>arp -a
Interface: 10.253.15.72 --- Bx4
Internet Address Physical Address Type
10.253.1.2 00-12-3f-ed-3f-2c dynamic
10.253.1.6 00-13-72-51-d5-a9 dynamic
10.253.1.10 00-03-ff-1f-7f-e9 dynamic
10.253.1.18 00-03-ff-36-9b-00 dynamic
10.253.1.25 00-11-43-de-91-15 dynamic
10.253.1.26 00-11-43-97-97-fc dynamic
10.253.1.27 00-15-22-17-98-07 dynamic
10.253.1.35 00-14-22-17-98-91 dynamic
10.253.1.80.1 00-15-23-46-50-00 dynamic
10.253.1.80.2 00-09-0f-83-3b-8a dynamic
```

Source: <https://learningportal.juniper.net/>

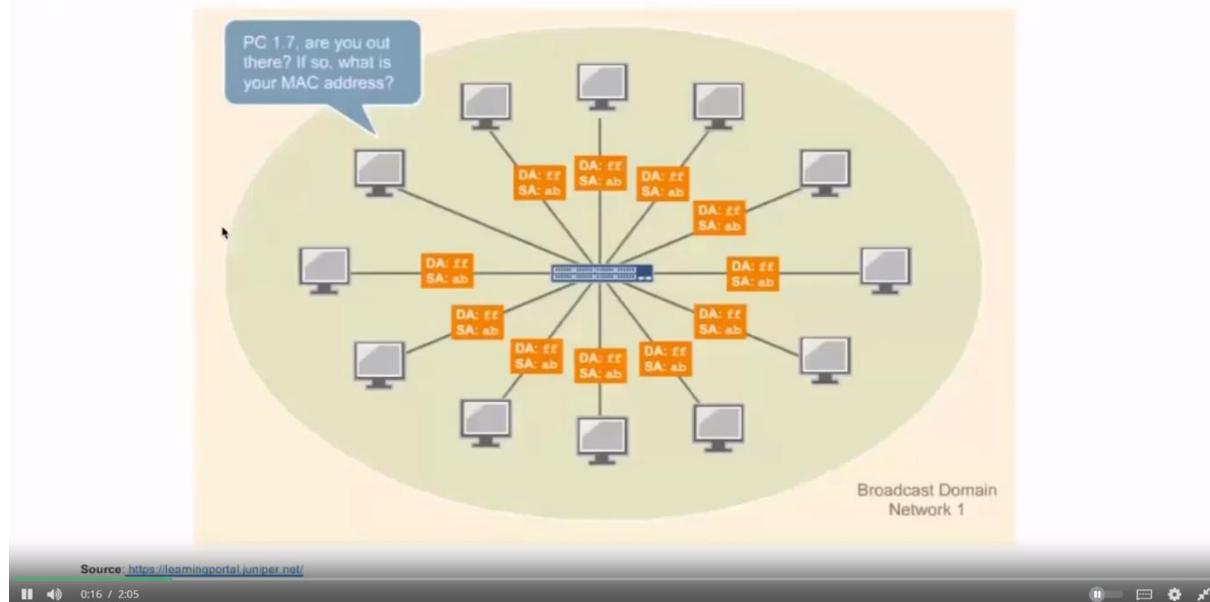
II 4:32 / 6:28

Address Resolution Protocol



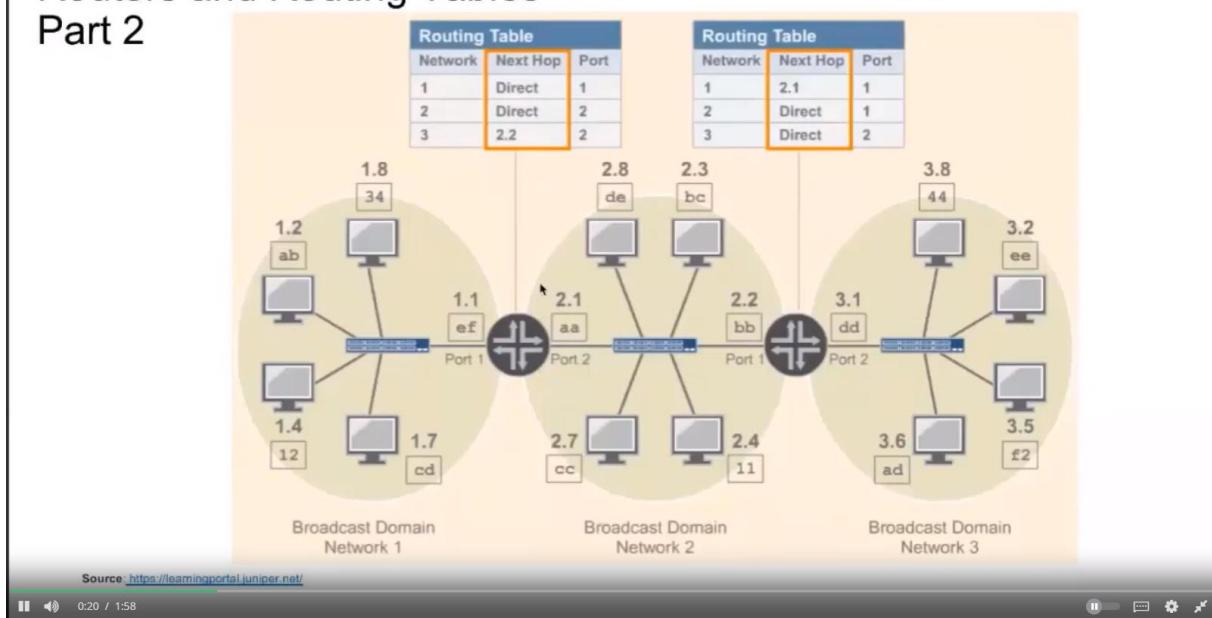
Routers and Routing Tables, Part 1

Houston we have a problem!!!



Routers and Routing Tables, Part 2

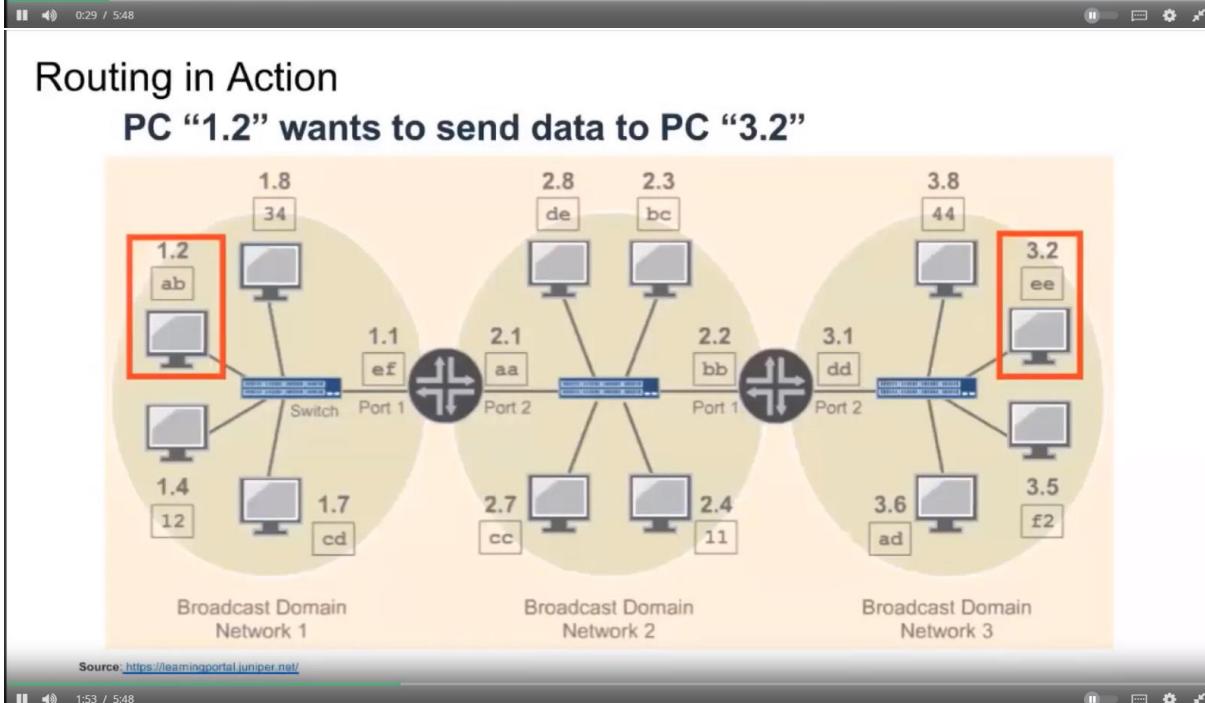
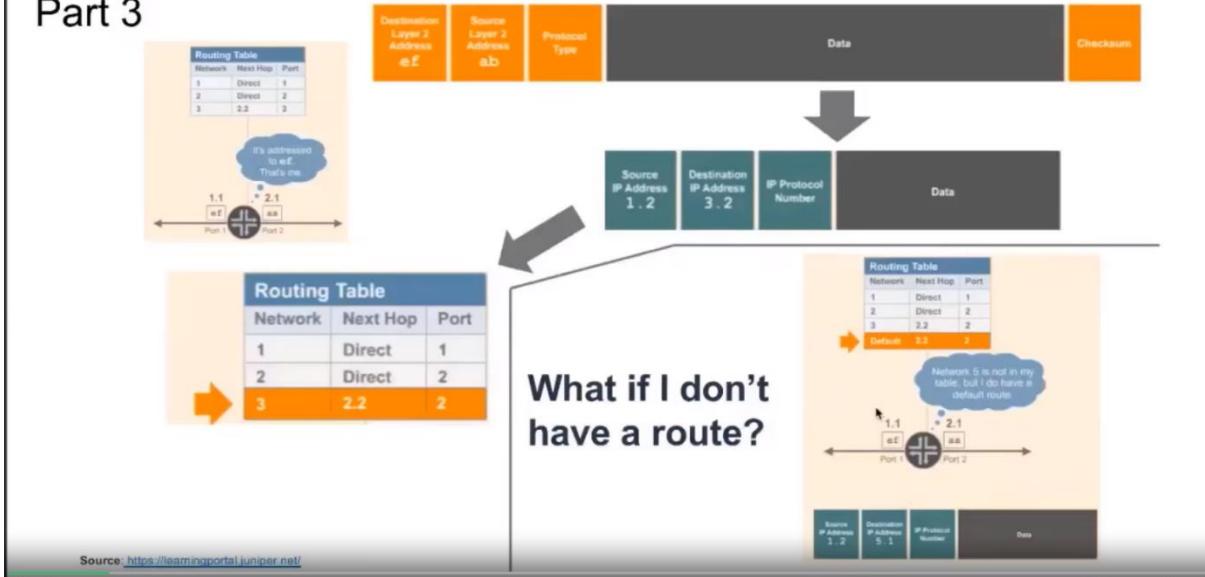
Routers and Routing Tables Part 2

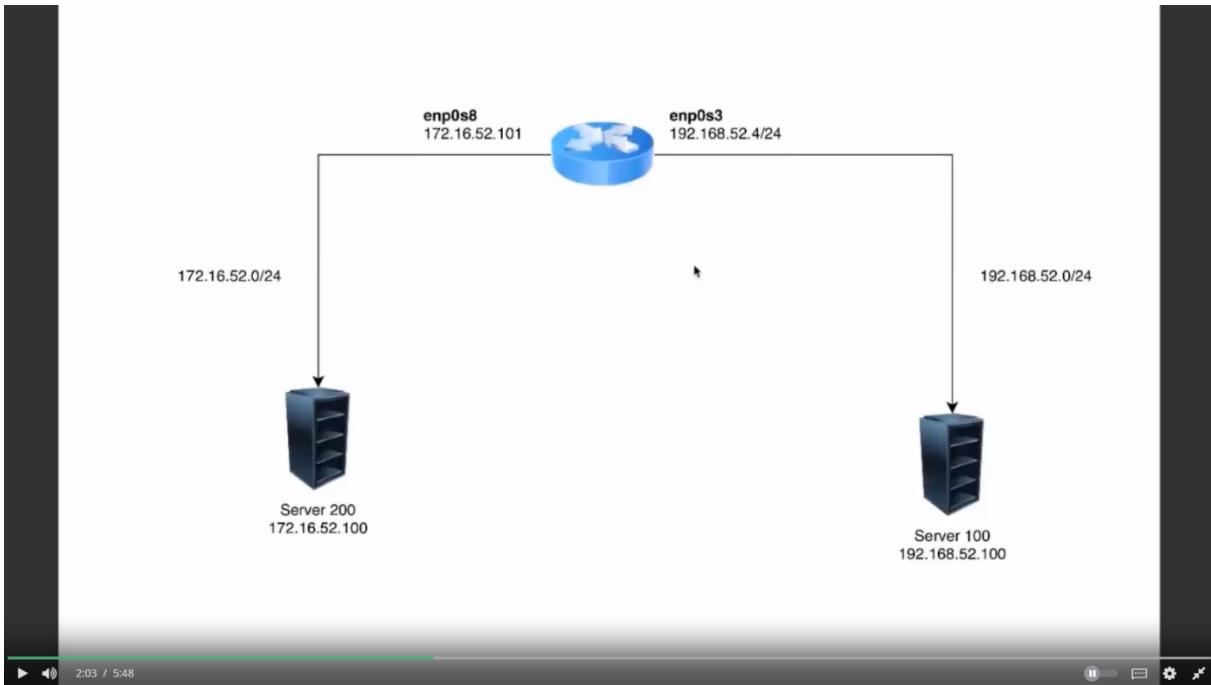


Routers and Routing Tables, Part 3

Routers and Routing Tables

Part 3





Research Network Vendor Training

Check out a few of the online training resources available for the following network vendors.

Cisco

<https://www.cisco.com/c/en/us/training-events/training-certifications/training-catalog/course-selector.html>

Juniper Networks

<https://www.juniper.net/us/en/training/>

Palo Alto Networks

<https://www.paloaltonetworks.com/services/education>

Week 2

IP Addressing - The Basics of Binary

Networking Fundamentals: IP Addressing – The Basics of Binary

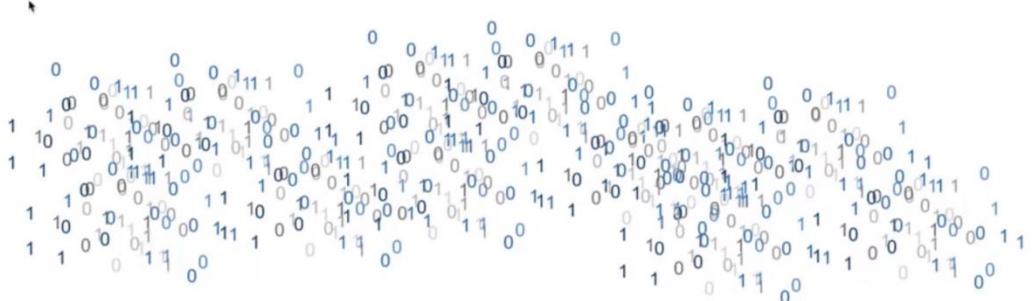
Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security



Binary System

- Human beings think in terms of 10 based (decimal) numbering because we have 10 fingers/toes.
- Computers only know if the power is on (1) or off (0).
- Computers they don't know any other state.



Decimal

Millions	Hundred Thousands	Ten Thousands	Thousands	Hundreds	Tens	Ones
0	9	5	2	7	1	1



Binary

128's Placeholder	64's Placeholder	32's Placeholder	16's Placeholder	8's Placeholder	4's Placeholder	2's Placeholder	1's Placeholder
1	1	0	1	1	0	1	0

- Everyplace holder is twice the value of the previous placeholder.

Convert from binary to decimal

1	1	0	1	1	0	1	0
128	64	32	16	8	4	2	1

- Every placeholder can have only 2 values zero or one.
- We take the value of the placeholders, we multiple it times placeholder and then add up all the placeholders.
- $1 \times 128 + 1 \times 64 + 0 \times 32 + 1 \times 16 + 1 \times 8 + 0 \times 4 + 1 \times 2 + 0 \times 1$
- $128 + 64 + 16 + 8 + 2 = 218$

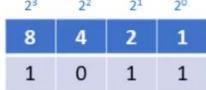
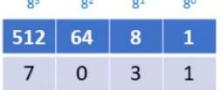
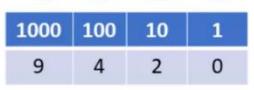
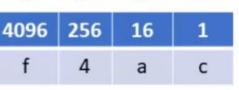
Convert from decimal to binary

235

1	1	1	0	1	0	1	1
128	64	32	16	8	4	2	1

- Can I subtract **128** from 235? Yes $235 - 128 = 107$
- Can I subtract **64** from 107? Yes $107 - 64 = 43$
- Can I subtract **32** from 43? Yes $43 - 32 = 11$
- Can I subtract **16** from 11? No
- Can I subtract **8** from 11? Yes $11 - 8 = 3$
- Can I subtract **4** from 3? No
- Can I subtract **2** from 3? Yes $3 - 2 = 1$
- Can I subtract **1** from 1? Yes $1 - 1 = 0$

11101011

System	Base	Possible values
Binary	2	0, 1
Octal (oct)	8	0 to 7
Decimal (dec)	10	0 to 9
Hexadecimal (hex)	16	0 to f (10-15 are represented by a, b, c, d, e & f)
Binary:  1 0 1 1	= 11	Oct:  7 0 3 1 = 3609
4 digit range 0000 – 1111 (0 – 15)	4 digit range 0000 – 7777 (0 – 4095)	
Dec:  9 4 2 0	= 9420	Hex:  f 4 a c = 62636
4 digit range 0000 – 9999 (0 – 9999)	4 digit range 0000 – ffff (0 – 65535)	

II 🔍 6:53 / 8:52

II 🔍 ⌂ ⚙ ✎

IP Address Structure and Network Classes

IP Protocol

IPv4 is a 32 bits address divided in four octets.

From 0.0.0.0 to 255.255.255.255

IPv4 has 4,294,967,296 possible addresses in its address space.

Decimal	Binary
10.195.121.10	00001010.11000011.01111001.00001010
	00001010.11000011.01111001
Network Portion	Host portion

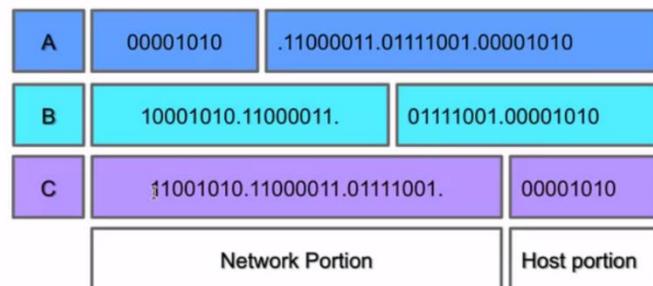
Classful Addressing

When the Internet's address structure was originally defined, every unicast IP address had a *network* portion, to identify the network on which the interface using the IP address was to be found, and a *host* portion, used to identify the particular host on the network given in the network portion.

The partitioning of the address space involved five *classes*. Each class represented a different trade-off in the number of bits of a 32-bit IPv4 address devoted to the network number versus the number of bits devoted to the host number.

Class	Address Range	Use	Default mask
A	0.0.0.0 – 127.255.255.255	Unicast/Special	255.0.0.0
B	128.0.0.0 – 191.255.255.255	Unicast/Special	255.255.0.0
C	192.0.0.0 – 223.0.0.0	Unicast/Special	255.255.255.0
D	224.0.0.0 – 239.255.255.255	Multicast	N/A
E	240.0.0.0 – 255.255.255.255	Reserved	N/A

Classful Addressing



IP Protocol and Traffic Routing

IP Protocol (Internet Protocol)

- Layer 3 devices use the IP address to identify the destination of the traffic, also devices like stateful firewalls use it to identify where traffic has come from.
- IP addresses are represented in quad dotted notation, for example, 10.195.121.10.
- Each of the numbers is a nonnegative integer from 0 to 255 and represents one-quarter of the whole IP address.
- A routable protocol is a protocol whose packets may leave your network, pass through your router, and be delivered to a remote network.



0 - 255 base 10
00000000 - 11111111 base 2



Be familiar with IP addresses, subnet masks and default gateways !!!



IP Protocol

Version	IHL	Service Type	Total Length				
Identification		Flags		Fragment Offset			
TTL	Protocol	Header Checksum					
Source IP Address							
Destination IP Address							
Options		Padding					
Payload							



```

4090 202.b34b90 192.168.1.1 192.168.1.104 ICMP /4 echo (ping) reply ta=
4094 263.633933 192.168.1.104 192.168.1.1 ICMP 74 Echo (ping) request id=
> Frame 3904: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_17:36:85 (4c:34:88:17:36:85), Dst: Cisco-Li_e1:80:b3 (98:fc:11:e1:80:b3)
> Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    & Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x387a (14458)
    & Flags: 0x00
        0.... .... = Reserved bit: Not set
        .0... .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x7e8d [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.104
    Destination: 192.168.1.1

```

II 3:42 / 6:58 | Source GeoIP: Unknown

Network Mask

- The *subnet mask* is an assignment of bits used by a host or router to determine how the network and subnetwork information is partitioned from the host information in a corresponding IP address.
- It is possible to use a shorthand format for expressing masks that simply gives the number of contiguous 1 bits in the mask (starting from the left). This format is now the most common format and is sometimes called the prefix length.
- The number of bits occupied by the network portion.
- Masks are used by routers and hosts to determine where the network/subnetwork portion of an IP address ends and the host part begins.



Network Mask

- The *subnet mask* is an assignment of bits used by a host or router to determine how the network and subnetwork information is partitioned from the host information in a corresponding IP address.
- It is possible to use a shorthand format for expressing masks that simply gives the number of contiguous 1 bits in the mask (starting from the left). This format is now the most common format and is sometimes called the prefix length.
- The number of bits occupied by the network portion.
- Masks are used by routers and hosts to determine where the network/subnetwork portion of an IP address ends and the host part begins.

192.168.52.3/24



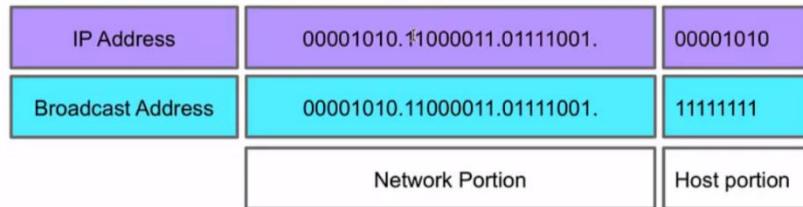
Default Gateway

```
Administrator: C:\windows\system32\cmd.exe
Connection-specific DNS Suffix . :
Wireless LAN adapter Wireless Network Connection 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
Ethernet adapter Bluetooth Network Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
Wireless LAN adapter Wireless Network Connection:
  Connection-specific DNS Suffix . . . tig.co.cr
  Link-local IPv6 Address . . . . . : fe80::45d0:a46c:9315:1c2d%13
  IPv4 Address . . . . . : 192.168.1.104
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . .
```



Broadcast Addresses

In each IPv4 subnet, a special address is reserved to be the subnet broadcast address. The subnet broadcast address is formed by setting the network/subnet portion of an IPv4 address to the appropriate value and all the bits in the Host portion to 1.



```
[[root@server100 ~]# ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:30:f7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.52.3/24 brd 192.168.52.255 scope global noprefixroute dynamic enp0s3
            valid_lft 1140sec preferred_lft 1140sec
        inet 192.168.52.100/24 brd 192.168.52.255 scope global secondary enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::7f98:fcfa:54d3:b511/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[[root@server100 ~]# ip route show
default via 192.168.52.4 dev enp0s3
169.254.0.0/16 dev enp0s3 scope link metric 1002
192.168.52.0/24 dev enp0s3 proto kernel scope link src 192.168.52.3 metric 100
192.168.52.0/24 dev enp0s3 proto kernel scope link src 192.168.52.100 metric 100
[root@server100 ~]# ]]
```

Introduction to the IPv6 Address Schema

IPv4 VS IPv6

In IPv6, addresses are 128 bits in length, four times larger than IPv4 addresses.

An IPv6 address will no longer use four octets. The IPv6 address is divided into eight hexadecimal values (16 bits each) that are separated by a colon (:) as shown in the following example:

65b3:b834:45a3:0000:0000:762e:0270:5224

The IPv6 address is not case-sensitive and you do not need to specify leading zeros in the address. Also, you can use a double colon (::) instead of a group of consecutive zeros when writing out the address.

0:0:0:0:0:0:1

::1

IPv4 VS IPv6

In IPv6, addresses are 128 bits in length, four times larger than IPv4 addresses.

An IPv6 address will no longer use four octets. The IPv6 address is divided into eight hexadecimal values (16 bits each) that are separated by a colon (:) as shown in the following example:

65b3:b834:45a3:0000:0000:762e:0270:5224

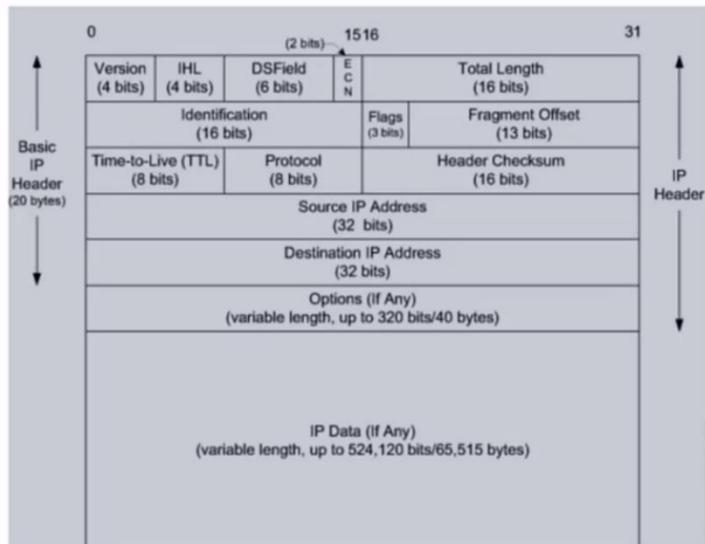
The IPv6 address is not case-sensitive and you do not need to specify leading zeros in the address. Also, you can use a double colon (::) instead of a group of consecutive zeros when writing out the address.

0:0:0:0:0:0:1

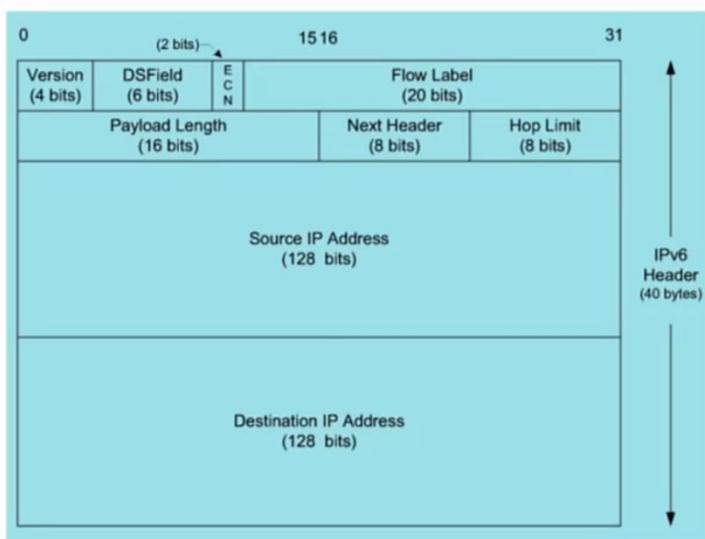
::1

Original: 65b3:b834:45a3:0000:0000:762e:0000:5224
Good abbreviation: 65b3:b834:45a3::762e:0000:5224
Bad abbreviation: 65b3:b834:45a3::762e::5224

IPv4 Header



IPv6 header



IPv4 Addressing Schemes

- **Unicast** Sends information to one system. With the IP protocol this is accomplished by sending data to the IP address of the intended destination system.
- **Broadcast** Sends information to all systems on the network. Data that is destined for all systems is sent by using the broadcast address for the network. An example of a broadcast address for a network is 192.168.2.255. The broadcast address is determined by setting all host bits to 1 and then converting the octet to a decimal number.
- **Multicast** Sends information to a selected group of systems. Typically this is accomplished by having the systems subscribe to a multicast address. Any data that is sent to the multicast address is then received by all systems subscribed to the address. Most multicast addresses start with 224.x.y.z and are considered class D addresses

IPv6 Addressing Schemes

Unicast A unicast address is used for one-on-one communication.

Multicast A multicast address is used to send data to multiple systems at one time.

 **Anycast** Refers to a group of systems providing a service.



Networking Fundamentals

Application and Transport Protocols

Presented by Ben Briggs
IBM Security

Based on a lecture series developed by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security

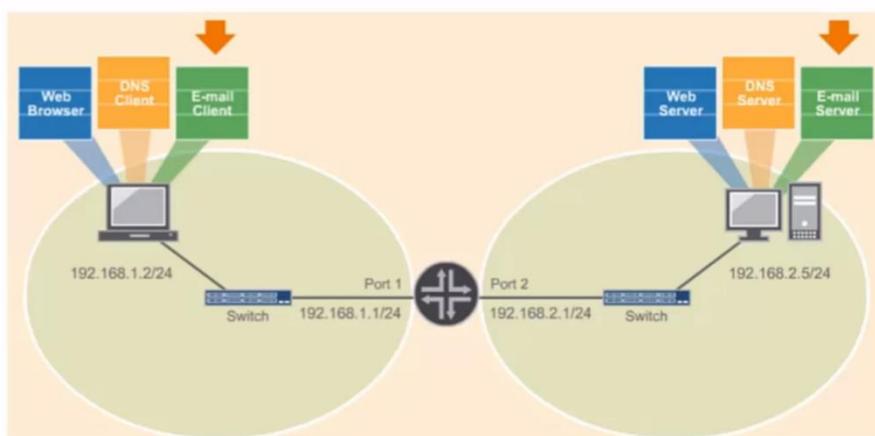
(c) 2020 IBM Corporation

0:21 / 5:03

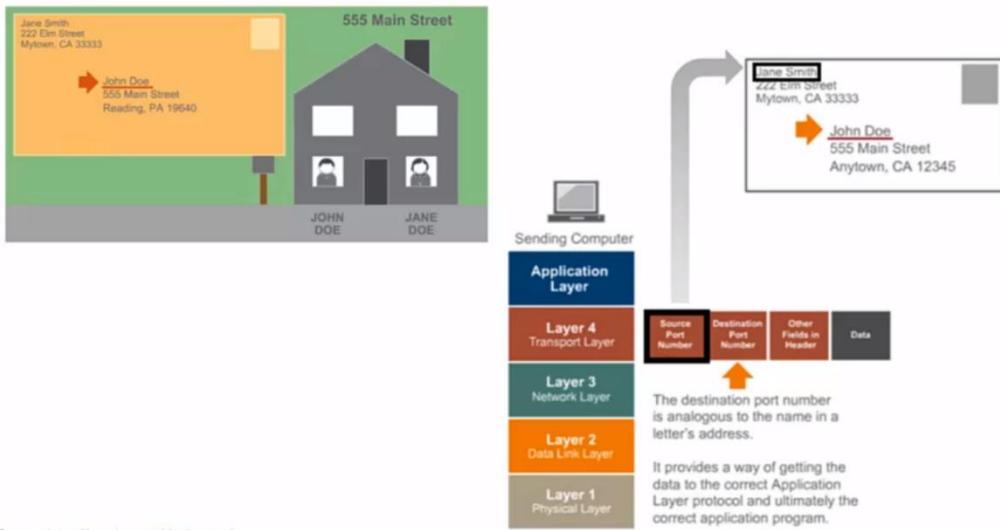
■ ▶ ⏪ ⏹ ⏷ ⏸

Objectives

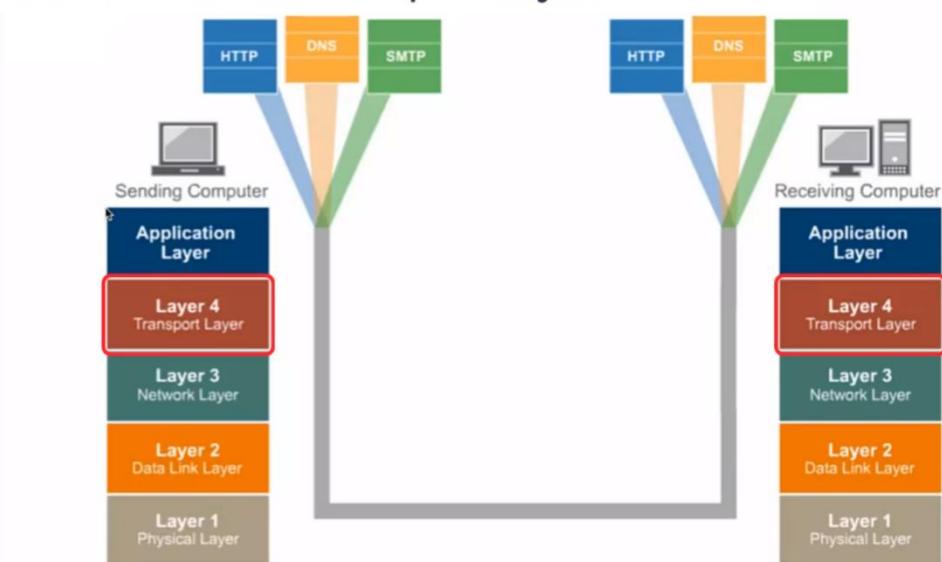
- Understand the differences between TCP and UDP.



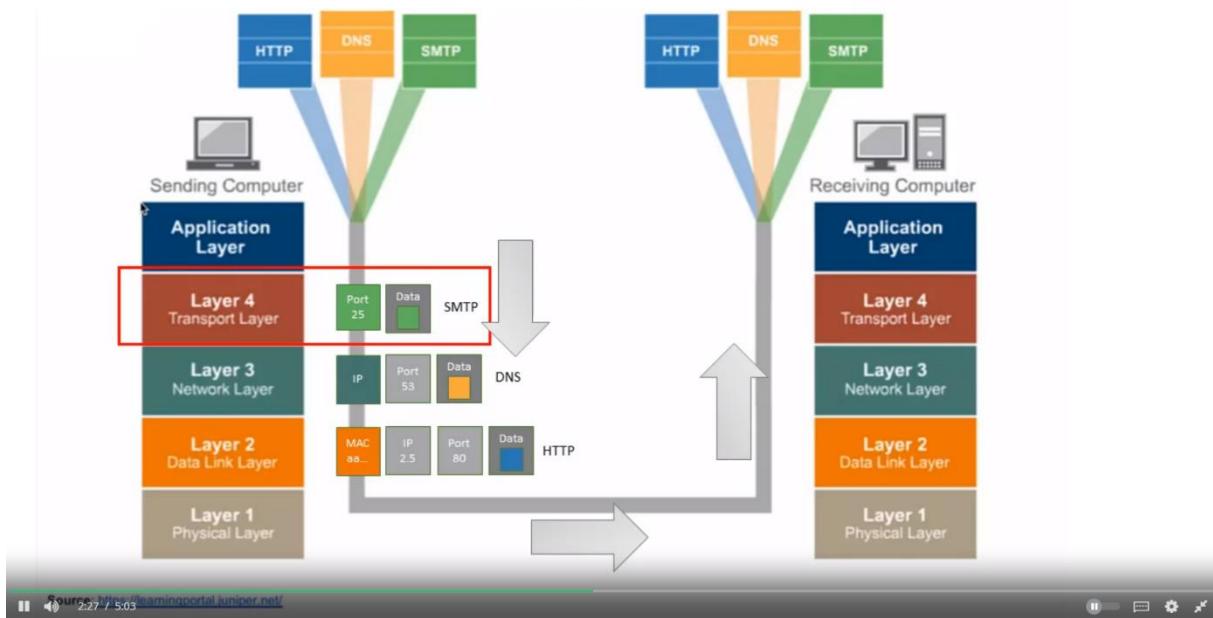
Overview of the Transport Layer Protocols



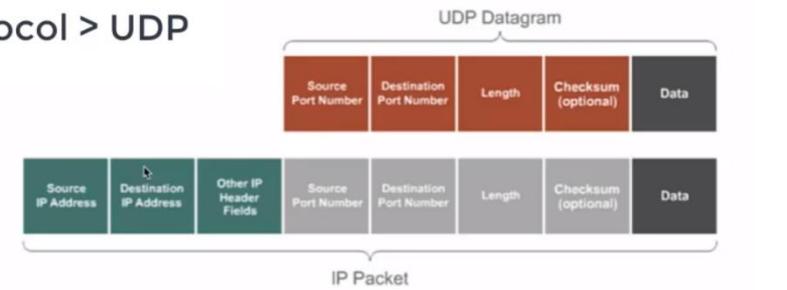
Overview of the Transport Layer Protocols



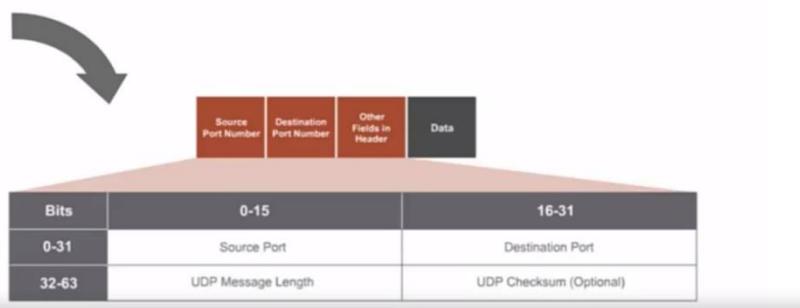
Overview of the Transport Layer Protocols



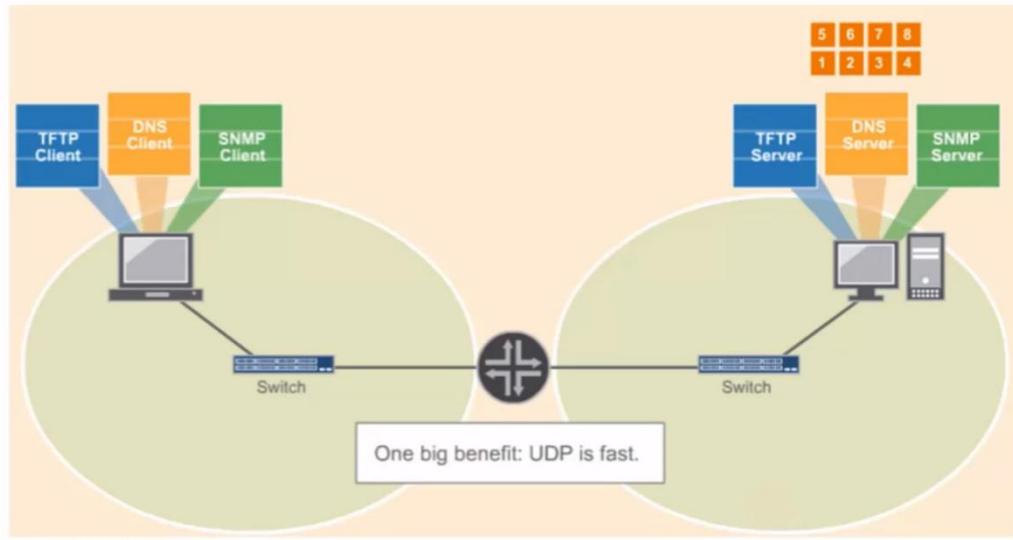
Transport Layer Protocol > UDP



UDP Header Fields

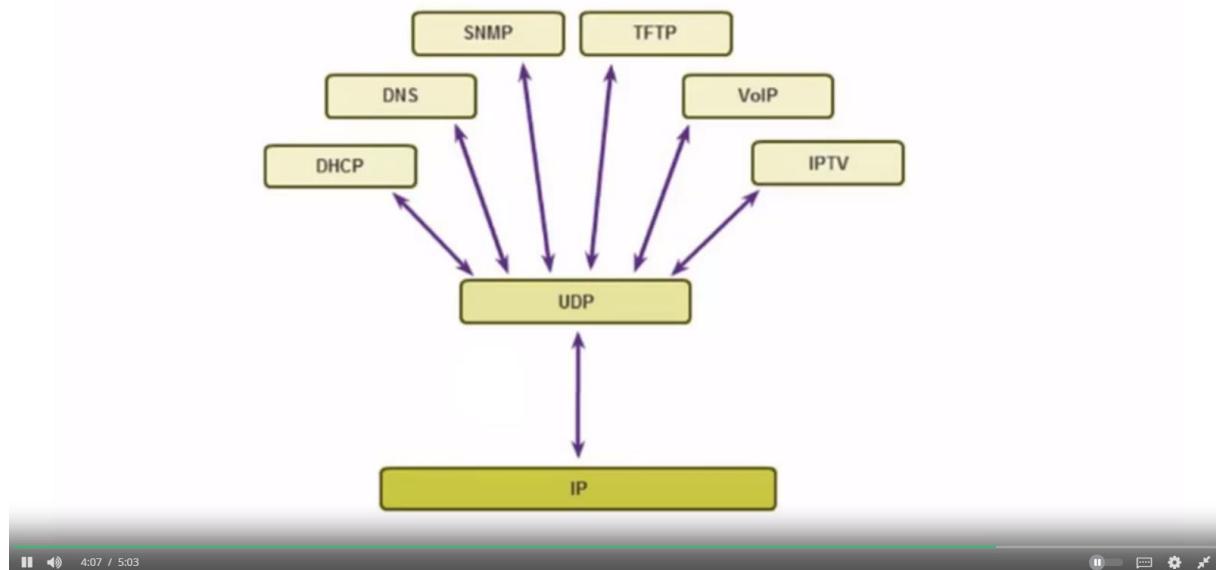


Transport Layer Protocol > UDP



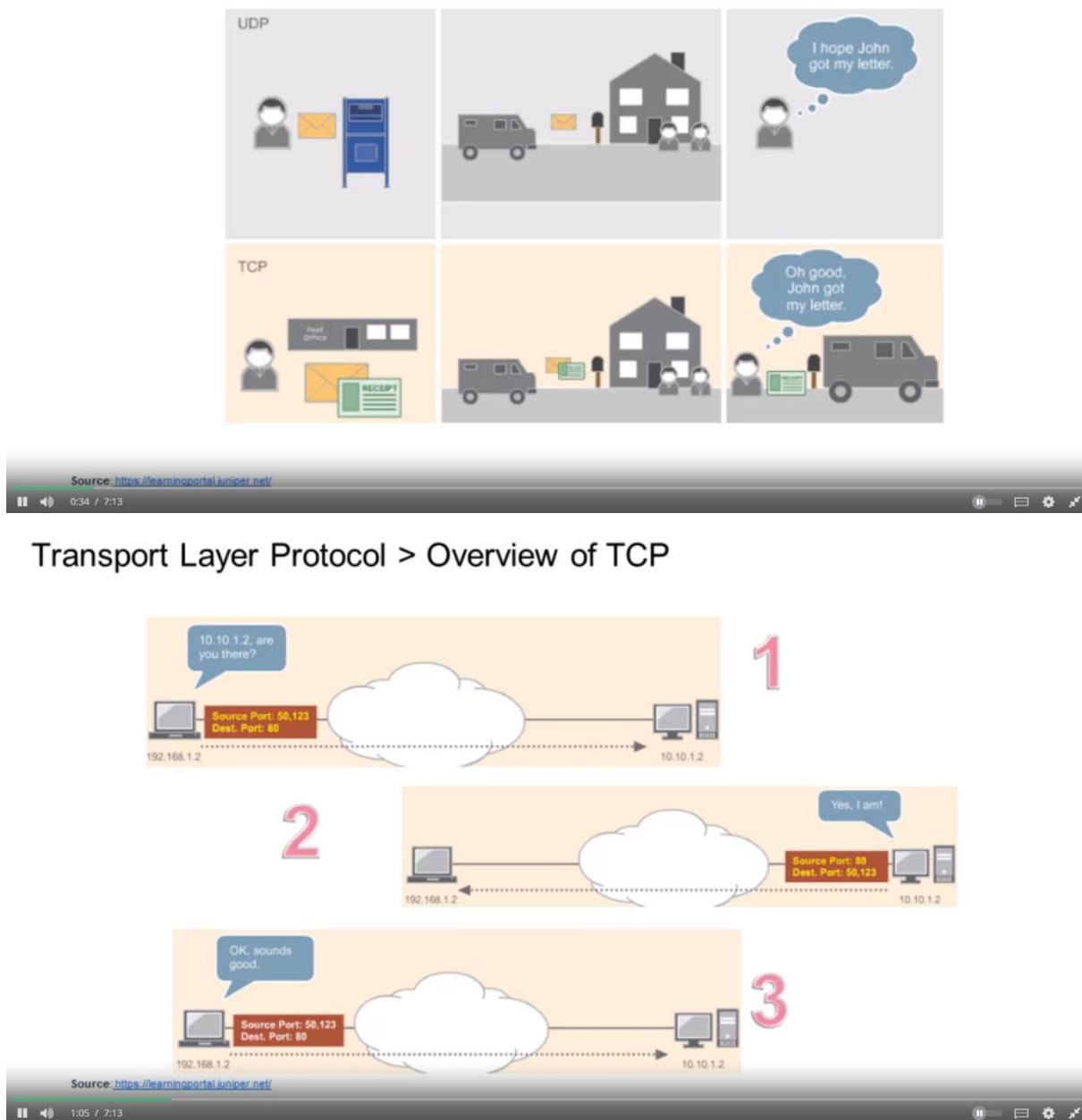
Source: <https://learningportal.juniper.net/>

Transport Layer Protocol > UDP



Application and Transport Protocols UDP and TCP, Part 2

Transport Layer Protocol > Overview of TCP



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.52.1	192.168.52.100	TCP	78	58038 → 22 [SYN]
2	0.000396	192.168.52.100	192.168.52.1	TCP	74	22 → 58038 [SYN]
3	0.000429	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK]
4	0.000824	192.168.52.1	192.168.52.100	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_7.9)
5	0.001085	192.168.52.100	192.168.52.1	TCP	66	22 → 58038 [ACK]
6	0.015550	192.168.52.100	192.168.52.1	SSHv2	87	Server: Protocol (SSH-2.0-OpenSSH_7.9)
7	0.015597	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK]
8	0.016789	192.168.52.1	192.168.52.100	SSHv2	1458	Client: Key Exchange Init
9	0.019329	192.168.52.100	192.168.52.1	SSHv2	1346	Server: Key Exchange Init
10	0.019377	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK]
11	0.022036	192.168.52.1	192.168.52.100	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
12	0.027027	192.168.52.100	192.168.52.1	SSHv2	430	Server: Diffie-Hellman Key Exchange Reply
13	0.027075	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK]
14	0.033606	192.168.52.1	192.168.52.100	SSHv2	82	Client: New Keys
15	0.073519	192.168.52.100	192.168.52.1	TCP	66	22 → 58038 [ACK]
16	0.073672	192.168.52.1	192.168.52.100	SSHv2	110	Client: Encrypted packet (len=44)
17	0.074397	192.168.52.100	192.168.52.1	TCP	66	22 → 58038 [ACK]
18	0.074735	192.168.52.100	192.168.52.1	SSHv2	110	Server: Encrypted packet (len=44)
19	0.074786	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK]
20	0.074874	192.168.52.1	192.168.52.100	SSHv2	126	Client: Encrypted packet (len=60)
21	0.079213	192.168.52.100	192.168.52.1	SSHv2	150	Server: Encrypted packet (len=84)
22	0.079282	192.168.52.1	192.168.52.100	TCP	66	58038 → 22 [ACK]

Destination	Protocol	Length	Info
192.168.52.1	TCP	78	58038 → 22 [SYN, ECN, CWR] Seq=0 Win=65535
192.168.52.100	TCP	74	22 → 58038 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535
192.168.52.1	TCP	66	58038 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len=0
192.168.52.1	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_7.9)
192.168.52.100	TCP	66	22 → 58038 [ACK] Seq=1 Ack=22 Win=29056 Len=0
192.168.52.100	SSHv2	87	Server: Protocol (SSH-2.0-OpenSSH_7.9)
192.168.52.1	TCP	66	58038 → 22 [ACK] Seq=22 Ack=22 Win=131712 Len=0
192.168.52.100	SSHv2	1458	Client: Key Exchange Init
192.168.52.1	SSHv2	1346	Server: Key Exchange Init
192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=1414 Ack=1302 Win=13064
192.168.52.1	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
192.168.52.100	SSHv2	430	Server: Diffie-Hellman Key Exchange Reply
192.168.52.1	TCP	66	58038 → 22 [ACK] Seq=1462 Ack=1666 Win=13064
192.168.52.100	SSHv2	82	Client: New Keys
192.168.52.1	TCP	66	22 → 58038 [ACK] Seq=1666 Ack=1478 Win=31872
192.168.52.100	SSHv2	110	Client: Encrypted packet (len=44)
192.168.52.1	TCP	66	22 → 58038 [ACK] Seq=1666 Ack=1522 Win=31872
192.168.52.100	SSHv2	110	Server: Encrypted packet (len=44)
192.168.52.1	TCP	66	58038 → 22 [ACK] Seq=1522 Ack=1710 Win=131712
192.168.52.100	SSHv2	126	Client: Encrypted packet (len=60)
192.168.52.100	TCP	66	58038 → 22 [ACK] Seq=1582 Ack=1704 Win=31872

```

25 2 537670 102 168 52 1 102 168 52 100 TCP 66 58038 . 22 [AC]
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
▼ Flags: 0x010 (ACK)
  000 ..... = Reserved: Not set
  ....0 ..... =Nonce: Not set
  ....0.... = Congestion Window Reduced (CWR): Not set
  ....0.... = ECN-Echo: Not set
  ....0.... = Urgent: Not set
  ....1.... = Acknowledgment: Set
  ....0... = Push: Not set
  ....0.. = Reset: Not set
  ....0.. = Syn: Not set
  ....0... = Fin: Not set
  [TCP Flags: ....A....]
Window size value: 2058
[Calculated window size: 131712]

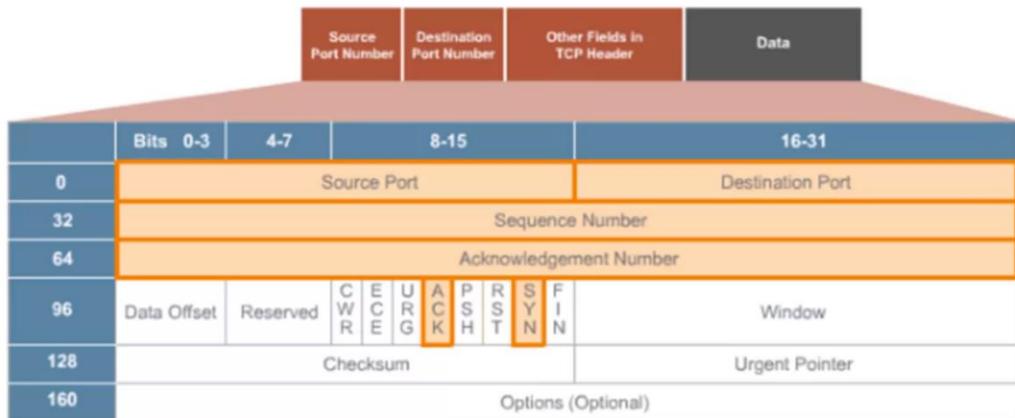
```

Transport Layer Protocol > Overview of TCP

UDP	TCP
Multiplexes data using ports	Multiplexes data using ports
Connectionless	Connection-oriented
Unreliable	Reliable
Unordered data; duplicates possible	Ordered data; duplicate detection
Datagrams	Segments
No flow control	Flow control

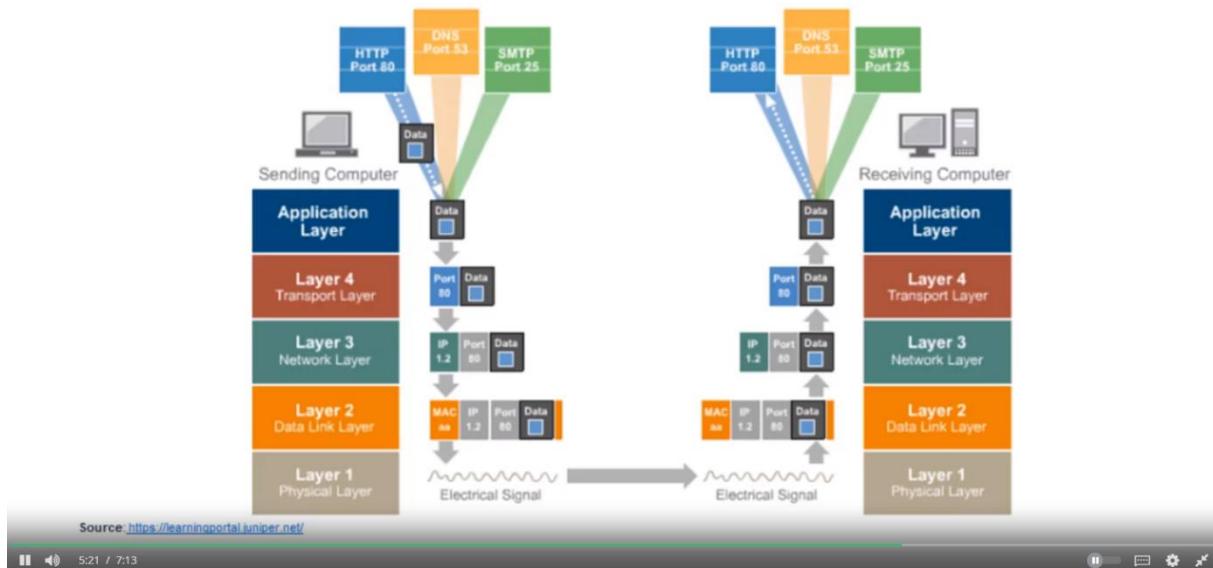
Source: <https://learningportal.juniper.net/>

Transport Layer Protocol > TCP In Action



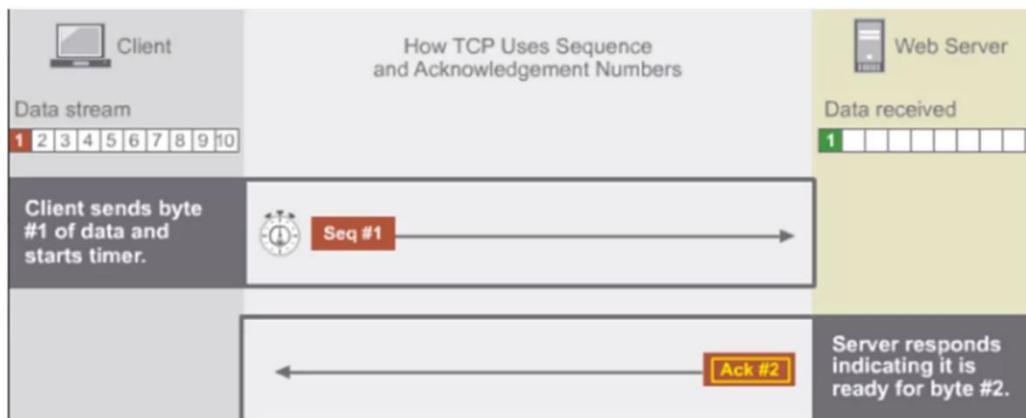
Source: <https://learningportal.juniper.net/>

Transport Layer Protocol > TCP In Action



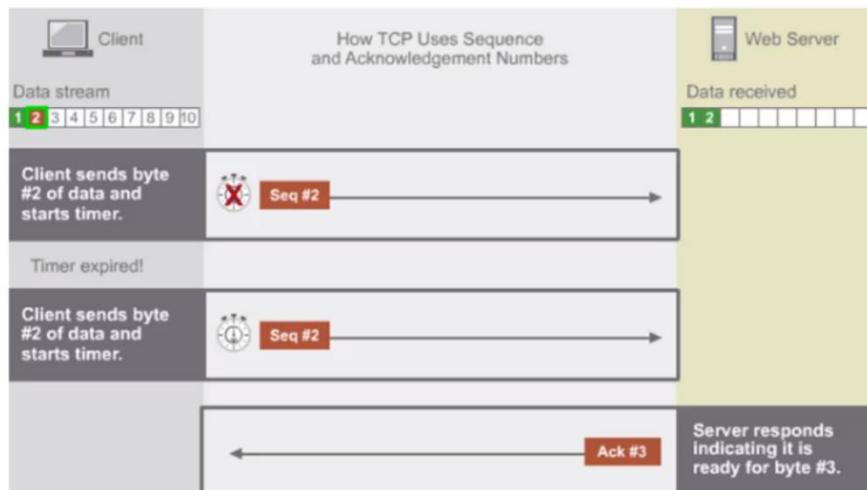
Source: <https://learningportal.juniper.net/>

Transport Layer Protocol > TCP In Action



Source: <https://learningportal.juniper.net/>

Transport Layer Protocol > TCP In Action



Source: <https://learningportal.juniper.net/>

Application Protocols - HTTP



- Developed by Tim Berners Lee.
- HTTP works on a request response cycle; where the client request a web page and the server returns a response.
- It is made of 3 blocks known as the start-line headers and body.
- Not secure.



Application Protocols - HTTPS

- Designed to increase privacy on the internet.
- Make use of SSL certificates.
- It is secured and encrypted.



DNS and DHCP

Networking Fundamentals
Application Protocols
Syslog vs flows

Presented by Ben Briggs
IBM Security

Based on a lecture series by
Moises Mauricio Monge Marin
MSIEM Administrator
IBM Security

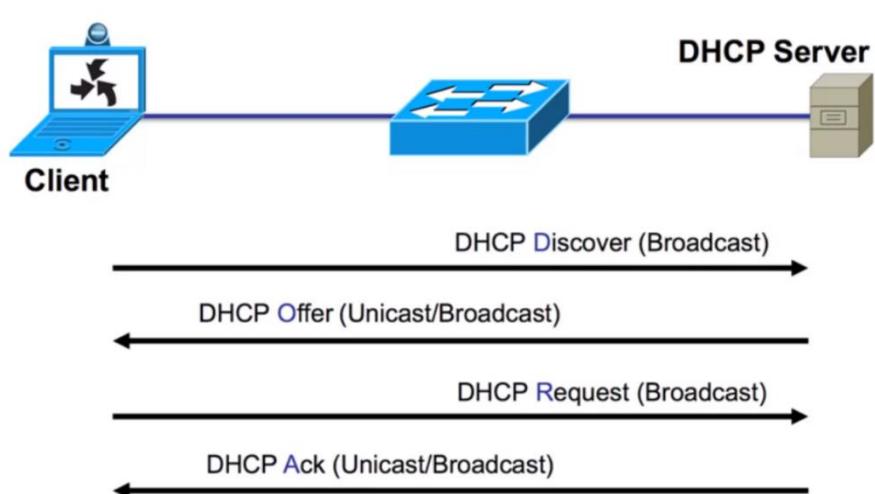


Doman Name System

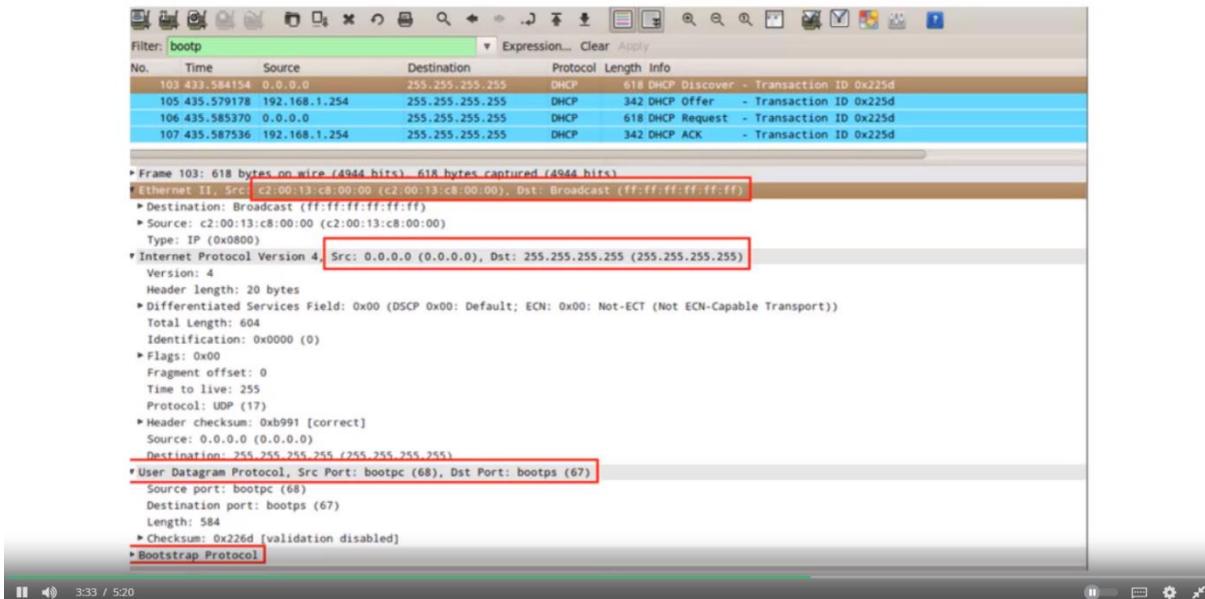


```
, packets transmitted, 0 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 51.109/56.688/65.404/5.211 ms
[Moisess-MacBook:~ MoisesM$ cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
domain hitronhub.home
nameserver 192.168.0.1
Moisess-MacBook:~ MoisesM$
```

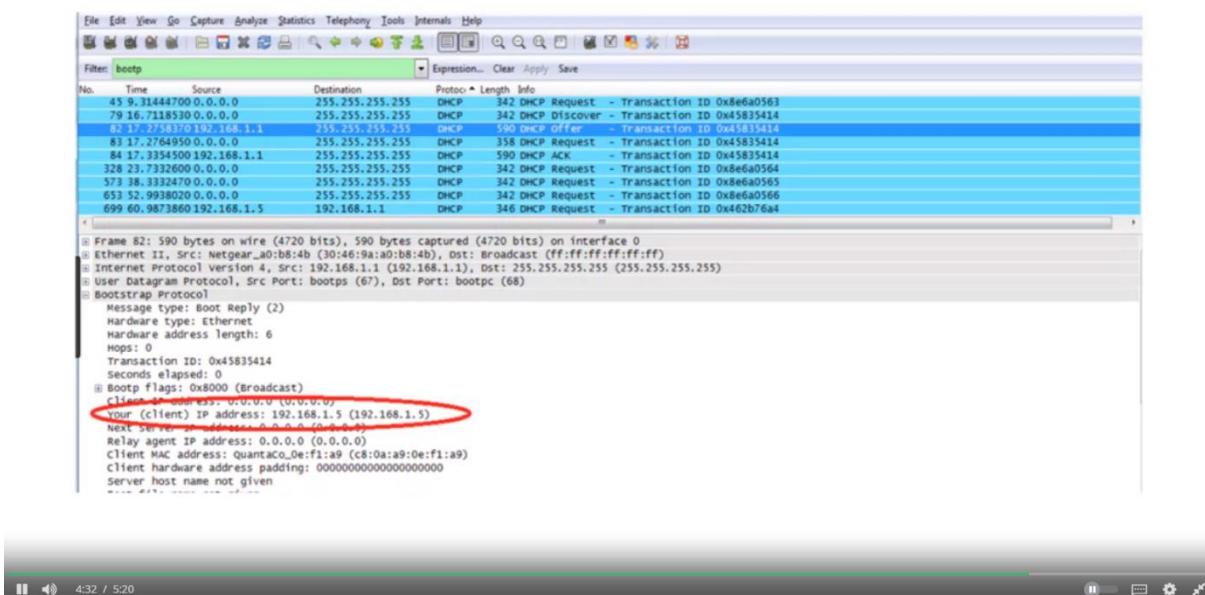
Dynamic Host Configuration Protocol



DHCP Discover



DHCP offer



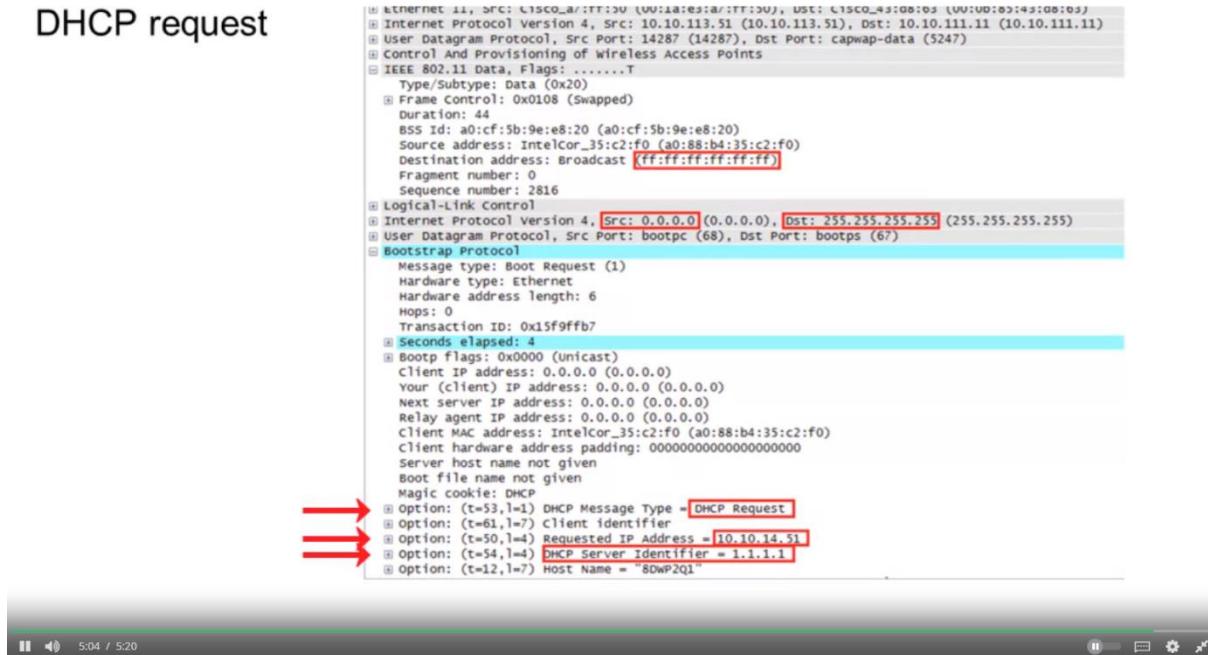
DHCP request

```
[+] Ethernet II, Src: Cisco_43:08:03 (00:1a:e3:a8:ff:03), Dst: Cisco_43:08:03 (00:1a:e3:a8:ff:03)
[+] Internet Protocol Version 4, Src: 10.10.113.51 (10.10.113.51), Dst: 10.10.111.11 (10.10.111.11)
[+] User Datagram Protocol, Src Port: 14287 (14287), Dst Port: capwap-data (5247)
[+] Control And Provisioning of Wireless Access Points
[+] IEEE 802.11 Data, Flags: ....T
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Swapped)
    Duration: 44
    BSS Id: a0:cfc5:b9e:8:20 (a0:cfc5:b9e:8:20)
    Source address: IntelCor_35:c2:f0 (a0:88:b4:35:c2:f0)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Fragment number: 0
    Sequence number: 2816
[+] Logical-Link Control
[+] Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
[+] User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
[+] Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x15f9fffb
[+] Seconds elapsed: 4
[+] Bootp flags: 0x0000 (unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_35:c2:f0 (a0:88:b4:35:c2:f0)
    Client hardware address padding: 000000000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
[+] Option: (t=53,l=1) DHCP Message Type = DHCP Request
[+] Option: (t=61,l=7) Client identifier
[+] Option: (t=50,l=4) Requested IP Address = 10.10.14.51
[+] Option: (t=54,l=4) DHCP Server Identifier = 1.1.1.1
[+] Option: (t=12,l=7) Host Name = "8DWP2Q1"
```

DHCP request

```
[+] Ethernet II, Src: Cisco_43:08:03 (00:1a:e3:a8:ff:03), Dst: Cisco_43:08:03 (00:1a:e3:a8:ff:03)
[+] Internet Protocol Version 4, Src: 10.10.113.51 (10.10.113.51), Dst: 10.10.111.11 (10.10.111.11)
[+] User Datagram Protocol, Src Port: 14287 (14287), Dst Port: capwap-data (5247)
[+] Control And Provisioning of Wireless Access Points
[+] IEEE 802.11 Data, Flags: ....T
    Type/Subtype: Data (0x20)
    Frame Control: 0x0108 (Swapped)
    Duration: 44
    BSS Id: a0:cfc5:b9e:8:20 (a0:cfc5:b9e:8:20)
    Source address: IntelCor_35:c2:f0 (a0:88:b4:35:c2:f0)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Fragment number: 0
    Sequence number: 2816
[+] Logical-Link Control
[+] Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
[+] User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
[+] Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x15f9fffb
[+] Seconds elapsed: 4
[+] Bootp flags: 0x0000 (unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: IntelCor_35:c2:f0 (a0:88:b4:35:c2:f0)
    Client hardware address padding: 000000000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
[+] Option: (t=53,l=1) DHCP Message Type = DHCP Request
[+] Option: (t=61,l=7) Client identifier
[+] Option: (t=50,l=4) Requested IP Address = 10.10.14.51
[+] Option: (t=54,l=4) DHCP Server Identifier = 1.1.1.1
[+] Option: (t=12,l=7) Host Name = "8DWP2Q1"
```

DHCP request



DHCP Ack

No.	Time	Source	Destination	Protocol	Length	Info
1085	18:48:35.553400000	192.168.1.1	192.168.1.110	DHCP	590	DHCP ACK - Transaction ID 0xec3a647a
1193	18:48:49.616543000	192.168.1.110	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x25ac1c9b4
1307	18:49:01.160819000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x53a63280
1328	18:49:02.281295000	192.168.1.1	255.255.255.255	DHCP	590	DHCP Offer - Transaction ID 0x53a63280
1331	18:49:02.281295000	192.168.1.1	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x53a63280
1331	18:49:02.281295000	192.168.1.1	255.255.255.255	DHCP	590	DHCP ACK - Transaction ID 0x53a63280
15	18:48:37.310987000	192.168.1.110	75.75.75.75	DNS	85	Standard query 0x631f A teredo.ipv6.microsoft.com
18	18:48:37.310987000	75.75.75.75	192.168.1.110	DNS	150	Standard query response 0x631f CNAME teredo.ipv6.microsoft.com nsatc.net A 157.56.106.18
86	18:48:18.718330000	192.168.1.110	75.75.75.75	DNS	86	Standard query 0x912f A updatekepalive.mcafee.com
87	18:48:18.737960000	75.75.75.75	192.168.1.110	DNS	136	Standard query response 0x912f CNAME updatekepalive.glb.mcafee.com A 161.69.12.13
166	18:48:19.405230000	192.168.1.110	75.75.75.75	DNS	85	Standard query 0xf001 A teredo.ipv6.microsoft.com
167	18:48:19.451950000	75.75.75.75	192.168.1.110	DNS	150	Standard query response 0xf001 CNAME teredo.ipv6.microsoft.com nsatc.net A 157.56.106.18
252	18:48:20.387890000	192.168.1.110	75.75.75.75	DNS	80	Standard query 0x79f2 A lsatap.easternct.edu
254	18:48:20.407207000	75.75.75.75	192.168.1.110	DNS	135	Standard query response 0x79f2 No such name
745	18:48:26.286885000	192.168.1.110	75.75.75.75	DNS	80	Standard query 0xedc4 A lsatap.easternct.edu

Syslog Message Logging Protocol

The syslog protocol

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

Used for:

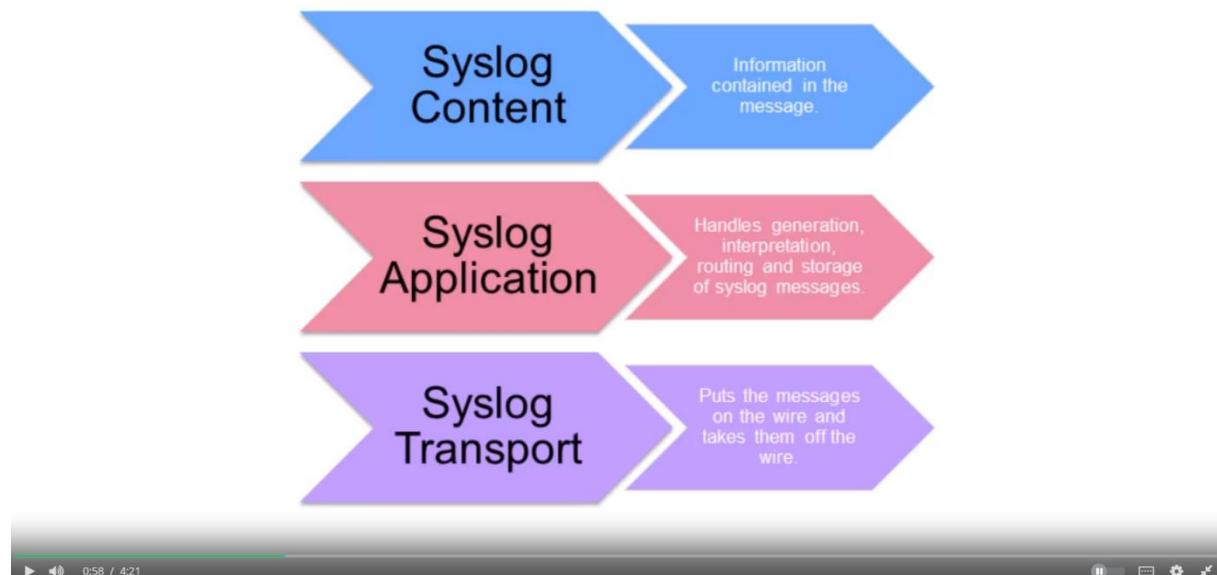
- system management
- security auditing
- general informational
- analysis, and debugging messages.

Used to convey event notification messages.

Provides a message format that allows vendor-specific extensions to be provided in a structured way.



Syslog utilizes three layers:



Functions are performed at each conceptual layer:

- An "**originator**" generates syslog content to be carried in a message. (Router, server, switch, network device, etc)
- A "**collector**" gathers syslog content for further analysis. – Syslog Server.
- A "**relay**" forwards messages, accepting messages from originators or other relays and sending them to collectors or other relays. – Syslog forwarder.
- A "**transport sender**" passes syslog messages to a specific transport protocol. – most common transport protocol is UDP, defined in the RFC5426.
- A "**transport receiver**" takes syslog messages from a specific transport protocol.



Syslog message components

- The information provided by the originator of a syslog message includes the **facility code** and the **severity level**.
- The syslog software adds information to the information header before passing the entry to the syslog receiver:
 - originator process ID
 - a timestamp
 - the hostname or IP address of the device.



Facility codes

- The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons.
- If you are receiving messages from a UNIX system, consider using the User Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

Facility code	Keyword	Description
0 kern	kernel	kernel messages
1 user	user	user-level messages
2 mail	mail	mail system
3 daemon	daemon	system daemons
4 auth	auth	security/authorization messages
5 syslog	syslog	messages generated internally by syslogd
6 lpr	lpr	line printer subsystem
7 news	news	network news subsystem
8 uucp	uucp	UUCP subsystem
9		clock daemon
10 authpriv	authpriv	security/authorization messages
11 ftp	ftp	FTP daemon
12 -		NTP subsystem
13 -		log audit
14 -		log alert
15 cron	cron	scheduling daemon
16 local0	local0	local use 0 (local0)
17 local1	local1	local use 1 (local1)
18 local2	local2	local use 2 (local2)
19 local3	local3	local use 3 (local3)
20 local4	local4	local use 4 (local4)
21 local5	local5	local use 5 (local5)
22 local6	local6	local use 6 (local6)
23 local7	local7	local use 7 (local7)



Syslog Severity Levels

Value	Severity	Keyword	Description	Examples
0	Emergency	emerg	System is unusable	This level should not be used by applications.
1	Alert	alert	Should be corrected immediately	Loss of the primary ISP connection.
2	Critical	crit	Critical conditions	A failure in the system's primary application.
3	Error	err	Error conditions	An application has exceeded its file storage limit and attempts to write are failing.
4	Warning	warning	May indicate that an error will occur if action is not taken.	A non-root file system has only 2GB remaining.
5	Notice	notice	Events that are unusual, but not error conditions.	
6	Informational	info	Normal operational messages that require no action.	An application has started, paused or ended successfully.
7	Debug	debug	Information useful to developers for debugging the application.	



The Syslog Protocol

```
> Internet Protocol Version 4, Src: 192.168.1.111, Dst: 192.168.1.107
> User Datagram Protocol, Src Port: 514, Dst Port: 514
# Syslog message: AUTH.INFO: Jan 23 12:19:59 sshd[2052]: Accepted keyboard-interactive/pam for moimonge from 192.168.1.110 port 62258 ssh2
0010 0... = Facility: AUTH - security/authorization messages (4)
.... 110 = Level: INFO - informational (6)
Message: Jan 23 12:19:59 sshd[2052]: Accepted keyboard-interactive/pam for moimonge from 192.168.1.110 port 62258 ssh2
```

Originator: 192.168.1.111

Collector: 192.168.1.107

Facility: Security/authorization messages (4).

Severity: Information (6).

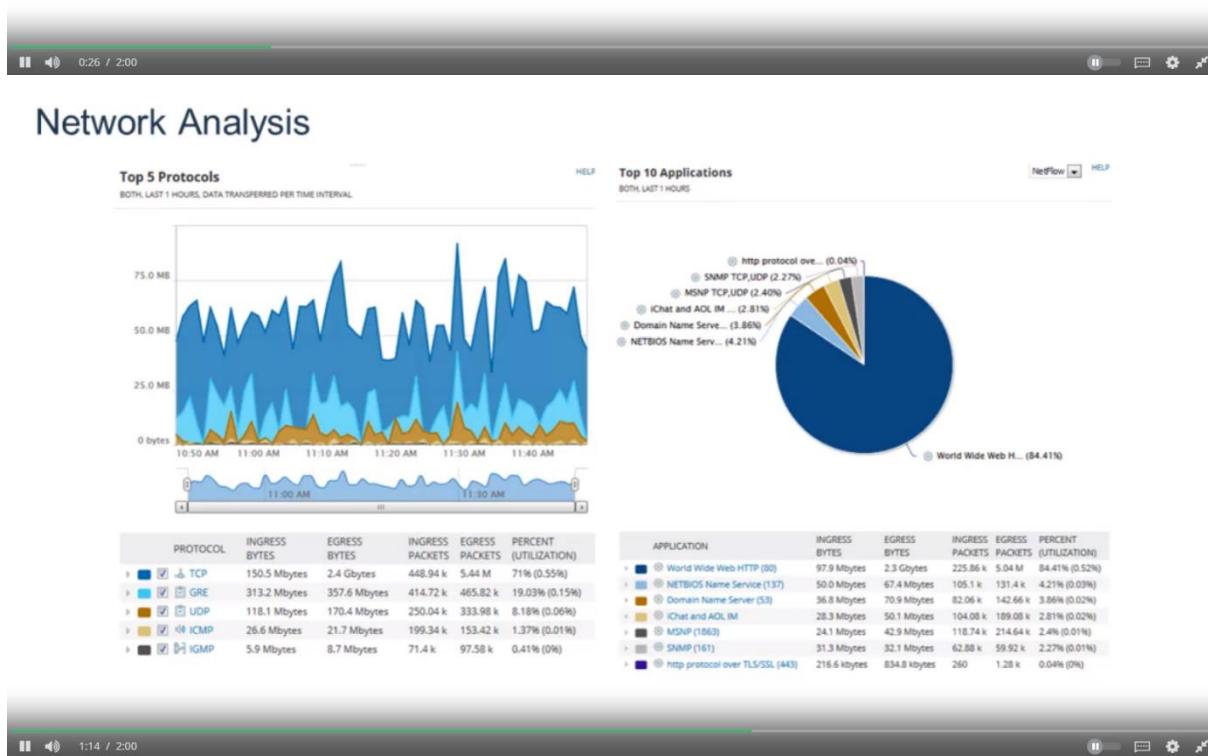
Syslog Content/Message: Jan 23 12:19:59 sshd[2052]: Accepted keyboard-interactive/pam for moimonge from 192.168.1.110 port 62258 ssh2



Flows and Network Analysis

What information is gathered in flows?

Usage	<ul style="list-style-type: none"> • Packet Count • Byte Count 	<ul style="list-style-type: none"> • Source IP Address • Destination IP Address 	To/From
Time of the day	<ul style="list-style-type: none"> • Start sysUpTime • End sysUpTime 	<ul style="list-style-type: none"> • Source TCP/UDP Port • Destination TCP/UDP Port 	Application
Port utilization	<ul style="list-style-type: none"> • Input IfIndex • Output IfIndex 	<ul style="list-style-type: none"> • Type of service • TCP Flags • Protocol 	Routing and peering
QoS	<ul style="list-style-type: none"> • Type of service • TCP Flags • Protocol 		



Port Mirroring and Promiscuous Mode

Port mirroring

- Sends a copy of network packets traversing on one switch port (or an entire VLAN) to a network monitoring connection on another switch port.
- Port mirroring on a Cisco Systems switch is generally referred to as Switched Port Analyzer (SPAN) or Remote Switched Port Analyzer (RSPAN).
- Other vendors have different names for it, such as Roving Analysis Port (RAP) on 3Com switches.
- This data is used to analyze and debug data or diagnose errors on a network.
- Helps administrators keep a close eye on network performance and alerts them when problems occur.
- It can be used to mirror either inbound or outbound traffic (or both) on one or various interfaces.



Promiscuous mode Network Interface Card (NIC)

In computer networking, promiscuous mode (often shortened to "promisc mode" or "promisc. mode") is a mode for a wired network interface controller (NIC) or wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive.



Next Generation Firewalls - Overview

Next Generation Firewalls



Fabian Alfaro Chinchilla
MSIEM Administrator
IBM Security

© 2016 IBM Corporation

0:33 / 4:00

...

What is a NGFW ?

- A Next-Generation Firewall (NGFW) is a part of the third generation of firewall technology. Combines traditional firewall with other network device filtering functionalities.
- Application firewall using in-line deep packet inspection (DPI)
- Intrusion prevention system (IPS).
- Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering.

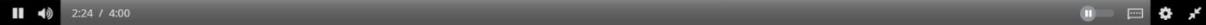
0:47 / 4:00

...

NGFW vs Traditional Firewall

- Inspection over the data payload of network packets.
- NGFW provides the intelligence for distinguish business applications and non-business applications and attacks.

Traditional firewalls don't have the fine-grained intelligence to distinguish one kind of Web traffic from another and enforce business policies, so it's either all or nothing.

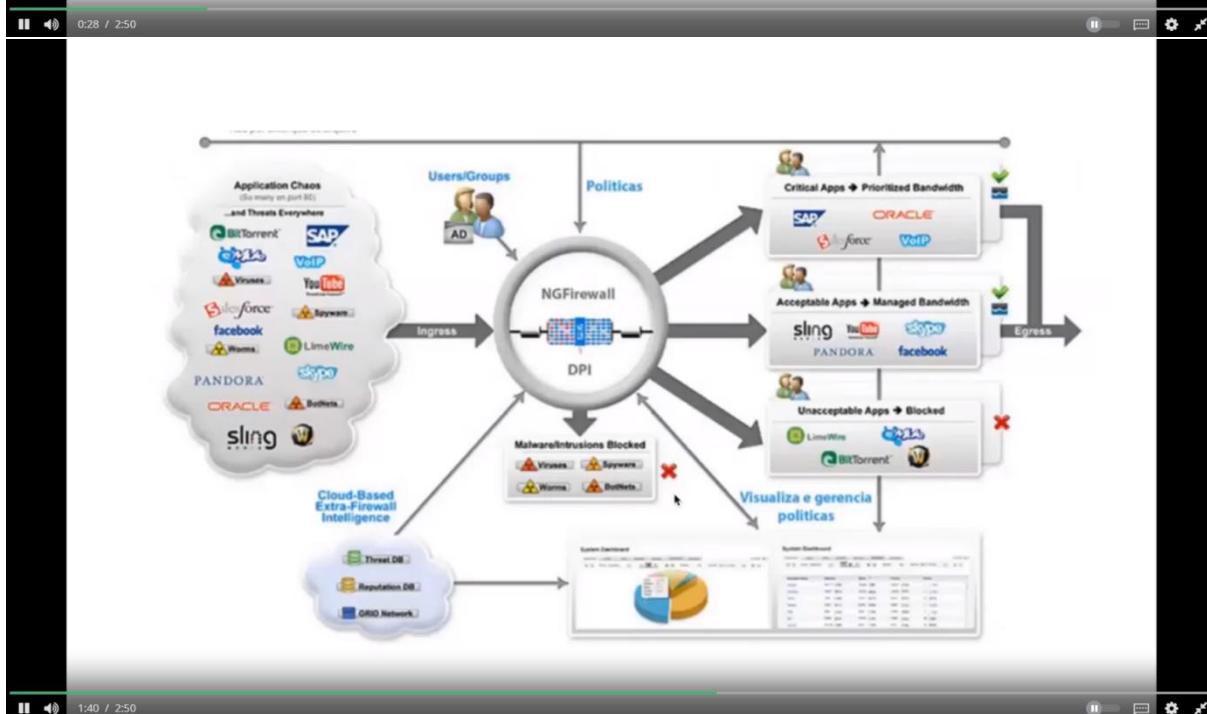
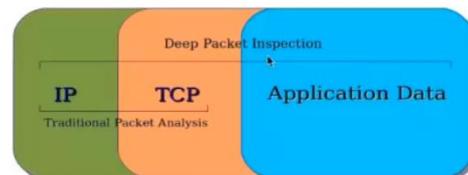


NGFW and the OSI Model

NGFW – OSI Model

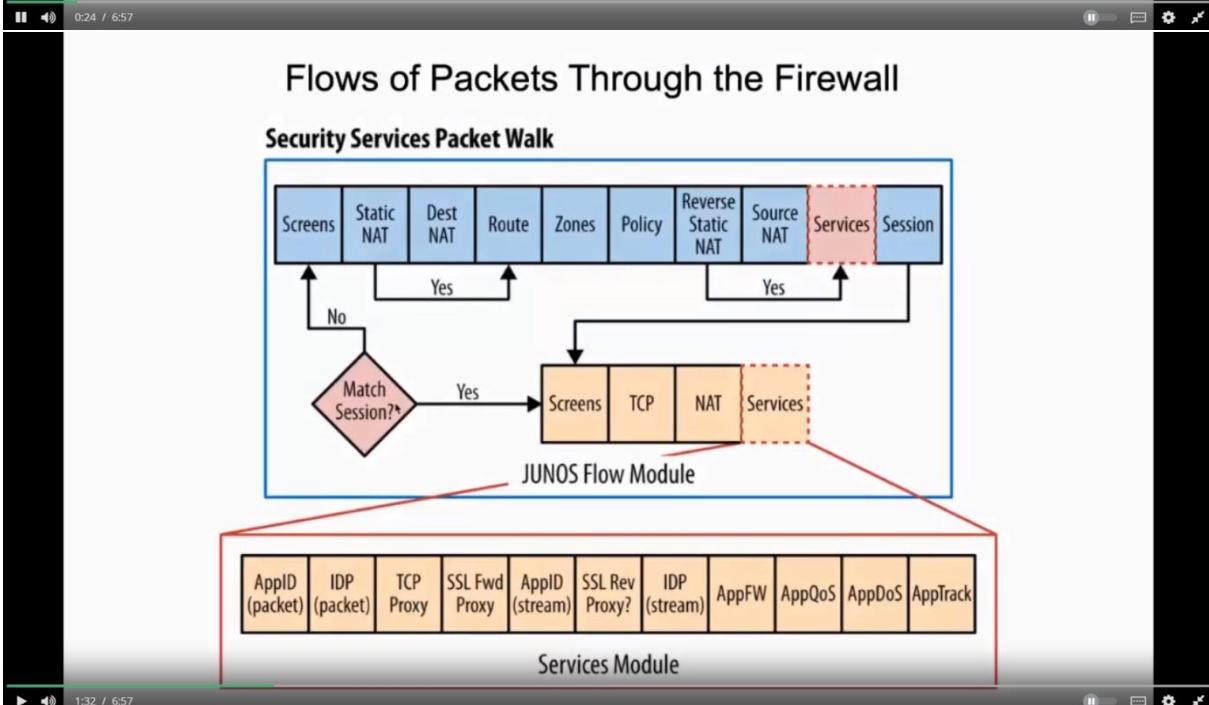
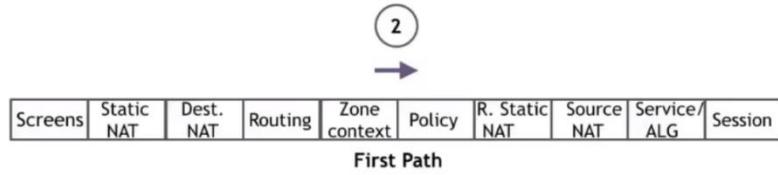
- The firewall itself must be able to monitor the traffic from layers 2 through 7 and make a determination as to what type of traffic is being sent and received.

Deep Packet Inspection



NGFW Packet Flow Example and NGFW Comparisons

Flow of Traffic Between Ingress and Egress Interfaces on a Next Gen FW



NGFW Comparisons:

-Many firewall vendors offer next-generation firewalls, but they argue over whose technique is best.

-A next-generation firewall is application-aware. Unlike traditional stateful firewalls, which deal in ports and protocols, next-generation firewalls drill into traffic to identify the applications traversing the network.

-With current trends pushing applications into the public cloud or to be outsourced to Software as a Service (SaaS) providers, a higher level of granularity is needed to ensure that the proper data is coming into the enterprise network.

NGFW Comparisons:

- **Cisco Systems** has announced plans to add new levels of application visibility into its **Adaptive Security Appliance (ASA)**, as part of its new SecureX security architecture.
- **Palo Alto Networks** says it was the first vendor to deliver next-generation firewalls and the first to replace port-based traffic classification with application awareness. The company's products are based on a classification engine known as **App-ID**. App-ID identifies applications using several techniques, including decryption, detection, decoding, signatures and heuristics
- **Juniper Networks** uses a suite of software products, known as **AppSecure**, to deliver next-generation firewall capabilities to its SRX Services Gateway. The application-aware component, known as AppTrack, provides visibility into the network based on Juniper's signature database as well as custom application signatures created by enterprise administrators

NGFW other vendors:

- McAfee
- Meraki MX Firewalls
- Barracuda
- Sonic Wall
- Fortinet Fortigate
- Check Point
- WatchGuard

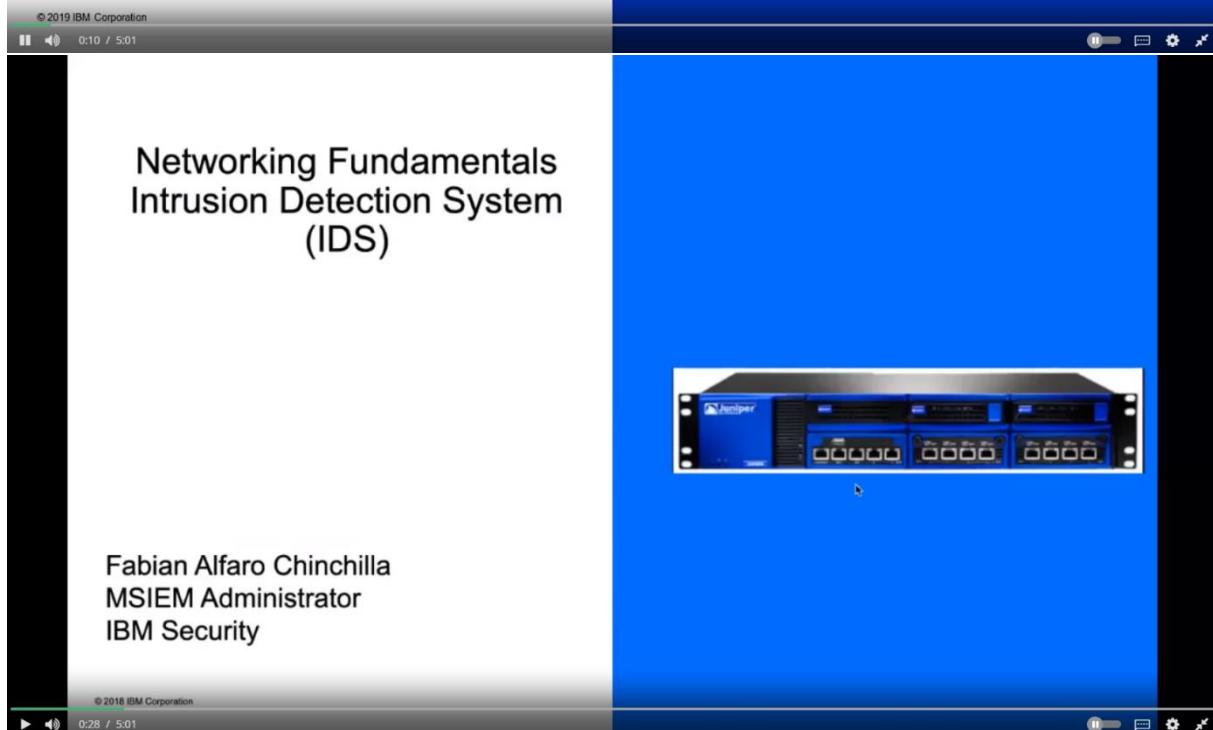
Open Source NGFW:

- **pfSense** is a free and powerful open source firewall used mainly for FreeBSD servers. It is based on stateful packet filtering. It has a wide range of features that are normally only found in very expensive firewalls.
- **ClearOS** is a powerful firewall that provides us the tools we need to run a network, and also gives us the option to scale up as and when required. It is a modular operating system that runs in a virtual environment or on some dedicated hardware in the home, office, etc
- **VyOS** is open source and completely free, and based on Debian GNU/Linux. It can run on both physical and virtual platforms. It provides a firewall, VPN functionality and software based network routing. It also supports paravirtual drivers and integration packages for virtual platforms. Unlike OpenWRT or pfSense, VyOS provides support for advanced routing features such as dynamic routing protocols and command line interfaces.
- **IPCop** is an open source Linux firewall which is secure, user friendly, stable and easily configurable. It provides an easily understandable Web interface to manage the firewall. It is most suitable for small businesses and local PCs.

Intrusion Detection and Intrusion Prevention Systems

In this video, you will learn
to...

- Describe how Intrusion Detection Systems (IDS) work.
- Describe what differentiates an Intrusion Prevention System (IPS) from an IDS.



CLASSIFICATION OF IDS

- Signature based: analyses content of each packet at layer 7 with a set of predefined signatures.
- Anomaly based: monitors network traffic and compares it against an established baseline for normal use and classifying it as either normal or anomalous.



TYPES OF IDS

- Host based IDS (HIDS): anti-threat applications such as firewalls, antivirus software and spyware-detection programs are installed on every network computer that has two-way access to the outside.
- Network based IDS (NIDS): anti-threat software is installed only at specific points such as servers that interface between the outside environment and the network segment to be protected.



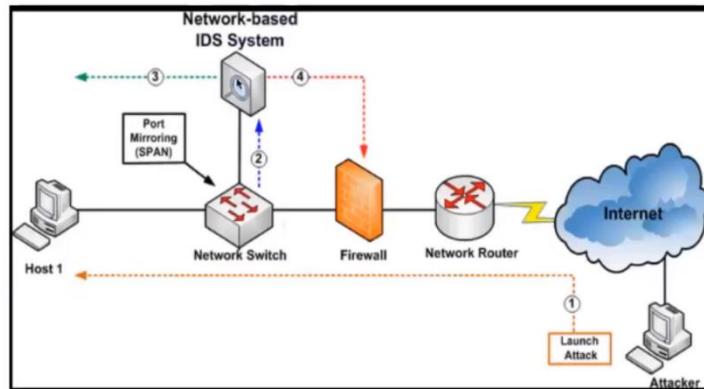
NIDS

- Appliance: IBM RealSecure Server Sensor and Cisco IDS 4200 series

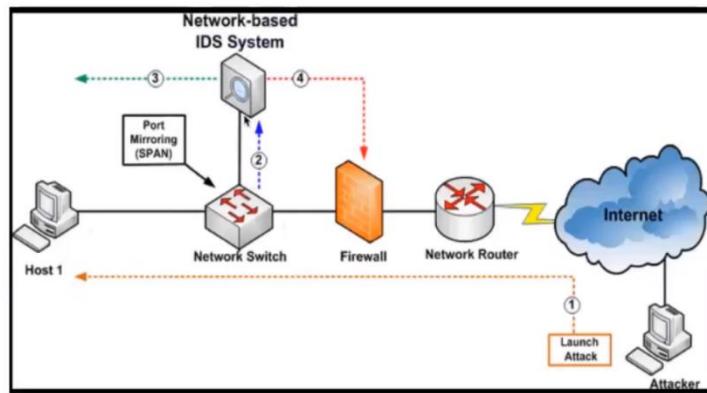


- Software: sensor software installed on server and placed in network to monitor network traffic, such as Snort.

IDS LOCATION ON NETWORK ???



IDS LOCATION ON NETWORK ???



HYBRID IDS IMPLEMENTATIONS

- Combines the features of HIDS and NIDS
- Gains flexibility and increases security
- Combining IDS sensors locations: put sensors on network segments and network hosts and can report attacks aimed at particular segments or the entire network.

Networking Fundamentals

Intrusion Prevention System (IPS)

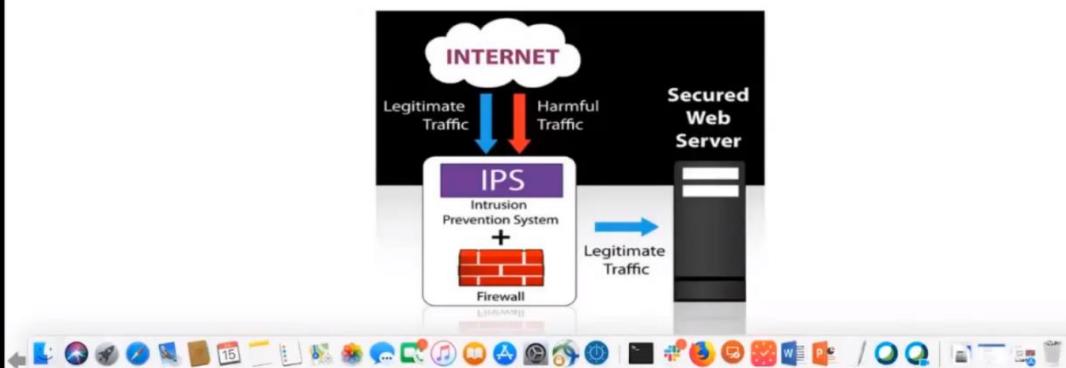
Fabian Alfaro Chinchilla
MSIEM Administrator
IBM Security

© 2016 IBM Corporation



What is an Intrusion Protection System (IPS)?

- Network security/threat prevention technology
- Examines network traffic flows to detect and prevent vulnerability exploits
- Often sits directly behind the firewall



Prevention?

- The IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include
 - Sending an alarm to the administrator (as would be seen in an IDS)
 - Dropping the malicious packets
 - Blocking traffic from the source address
 - Resetting the connection



How does the attack affect me?

- Vulnerability exploits usually come in the form of malicious inputs to a target application or service
- The attackers use those exploits to interrupt and gain control of an application or machine.
- Once successful exploit, the attacker can disable the target application (DoS)
- Also can potentially access to all the rights and permissions available to the compromised application



Signature-based detection

Is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures. Signature detection for IPS breaks down into two types:

1. Exploit-facing signatures identify individual exploits by triggering on the unique patterns of a particular exploit attempt. The IPS can identify specific exploits by finding a match with an exploit-facing signature in the traffic stream
2. Vulnerability-facing signatures are broader signatures that target the underlying vulnerability in the system that is being targeted. These signatures allow networks to be protected from variants of an exploit that may not have been directly observed in the wild, but also raise the risk of false positives.



Statistical anomaly detection

- Takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.
- IPS was originally built and released as a standalone device in the mid-2000s. This however, was in the advent of today's implementations, which are now commonly integrated into Unified Threat Management (UTM) solutions (for small and medium size companies) and next-generation firewalls (at the enterprise level).



High Availability and Clustering

Networking Fundamentals

High Availability and Clustering

Fabian Alfaro Chinchilla
SIEM Administrator
IBM Security

© 2018 IBM Corporation

0:36 / 9:15



0:48 / 9:15



What is HA?

- In information technology, high availability (HA) refers to a system or component that is continuously operational for a desirably long length of time. Availability can be measured relative to "100% operational" or "never failing."
- High availability architecture is an approach of defining the components, modules or implementation of services of a system which ensures optimal operational performance, even at times of high loads.
- Although there are no fixed rules of implementing HA systems, there are generally a few good practices that one must follow so that you gain the most out of the least resources.

What are the requirements for creating an HA cluster?

- Hosts in a virtual server cluster must have access to the same shared storage, and they must have identical network configurations.
- Domain name system (DNS) naming is important too: All hosts must resolve other hosts using DNS names, and if DNS is not set correctly, you won't be able to configure HA settings at all.
- Same OS level.
- Connections between the primary and secondary nodes.

How High Availability Works?

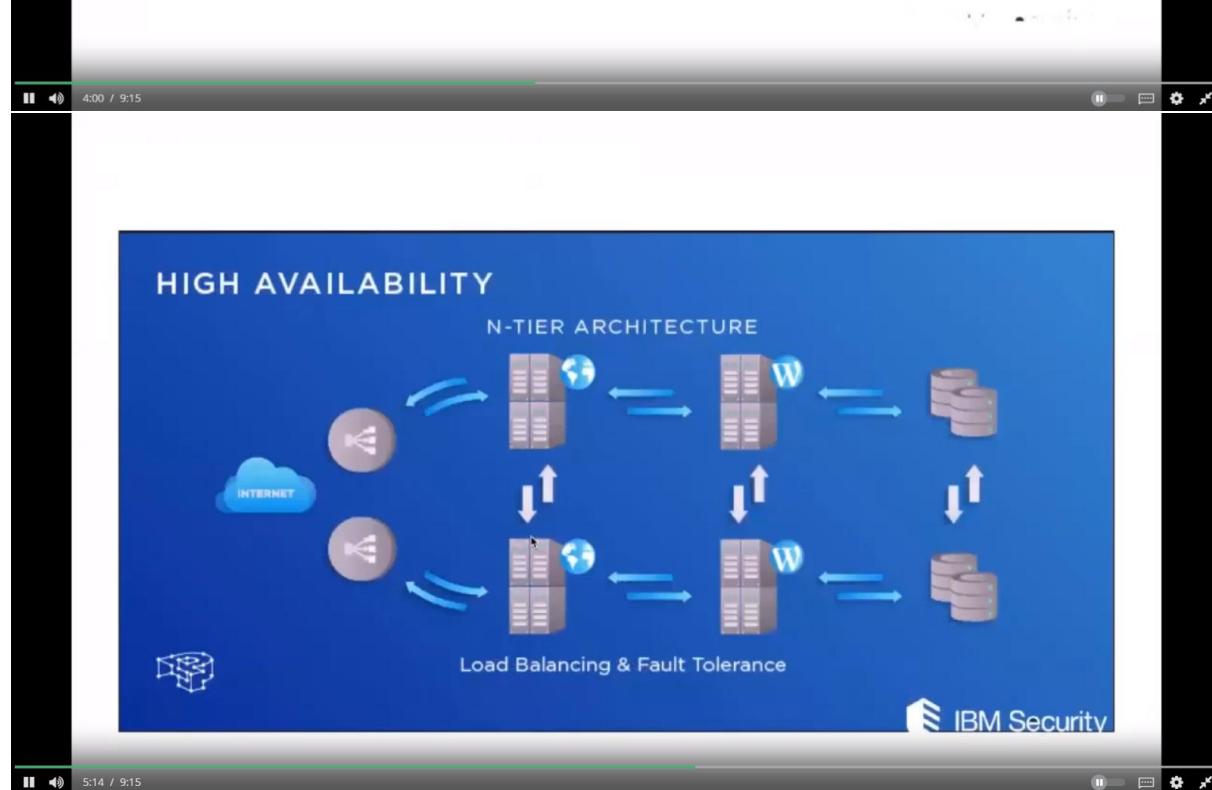
To create a highly available system, three characteristics should be present:

Redundancy:

- Means that there are multiple components that can perform the same task. This eliminates the single point of failure problem by allowing a second server to take over a task if the first one goes down or becomes disabled

Monitoring and Failover

- In a highly available setup, the system needs to be able to monitor itself for failure. This means that there are regular checks to ensure that all components are working properly. Failover is the process by which a secondary component becomes primary when monitoring reveals that a primary component has failed.

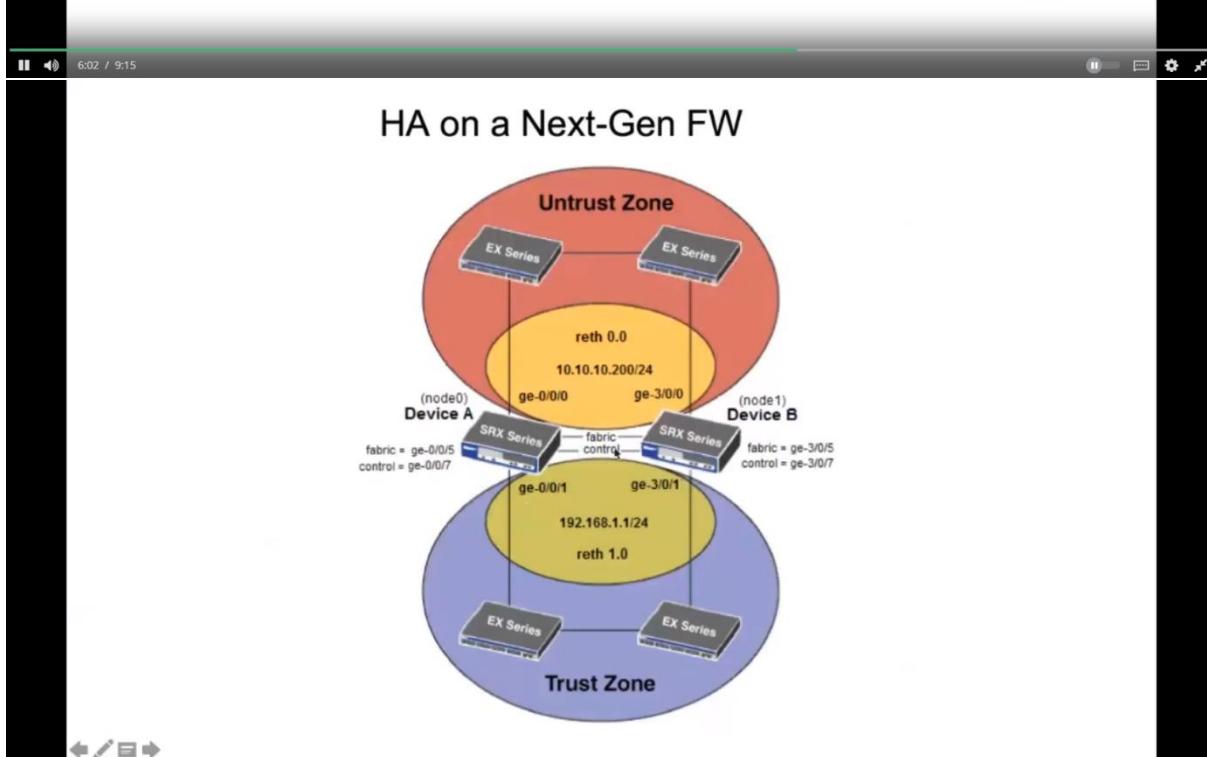


NIC TEAMING

Is a solution commonly employed to solve the network availability and performance challenges and has ability to operate multiple NICs as a single interface from the perspective of the system.

NIC Teaming provides:

- Protection against NIC failures.
- Fault tolerance in the event of a network adapter failure.

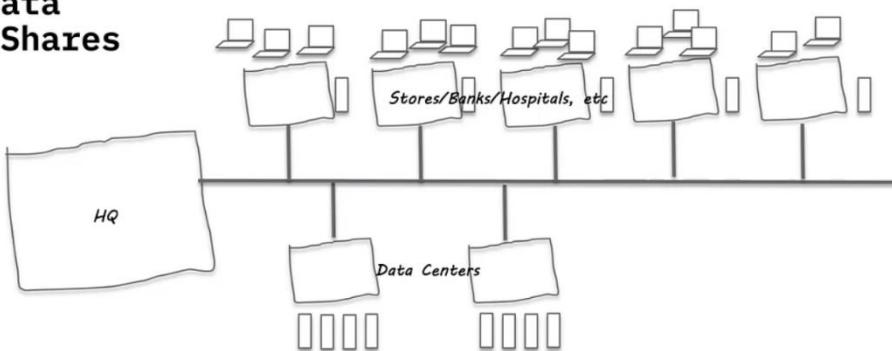


Week 3

Data Source Types Part 1

Data Source Types:

- Distributed Databases
- Data Warehouses
- Big Data
- File Shares



Data Source Types Part 2



Data Source Types:

- Distributed Databases
- Data Warehouses
- Big Data
- File Shares

Distributed Database examples:

Oracle, DB2, Microsoft SQL Server, MySQL

Big Data Database examples:

Hadoop, MongoDB, BigTable

Data Warehouse examples:

Netezza, Exadata, Amazon Redshift, Apache Hive

Fileshare examples:

“NAS” (Network Attached Storage) Network Fileshares such as EMC or NetApp; and Cloud Shares such as Google drive, dropbox.com, box.com, and Amazon’s S3 storage.

Source: <https://en.wikipedia.org/>



Data Source Types:

- Distributed Databases
- Data Warehouses
- Big Data
- File Shares

Distributed Database examples:

Structured Data

Big Data Database examples:

Semi-Structured Data

Data Warehouse examples:

Structured Data

File Share examples:

Unstructured-Data

Source: <https://en.wikipedia.org/>



Data Model Types

Data Model Types:

- Structured Data

Structured data is data that has been organized into a formatted repository, typically a database, so that its elements can be made [addressable](#) for more effective processing and analysis.

A [data structure](#) is a kind of repository that organizes information for that purpose. In a [database](#), for example, each field is discrete and its information can be retrieved either separately or along with data from other fields, in a variety of combinations. The power of the database is its ability to make data comprehensive, so that it yields useful information. A database query language, such as [SQL](#) (standard query language), allows a database administrator to interact with the database.

Structured data contrasts with [unstructured](#) and [semi-structured data](#). The three can be considered to exist on a continuum, with unstructured data being the least formatted and structured data being the most formatted. Data is increasingly amenable to processing as it is increasingly structured.



© 2019 IBM Corporation
0:24 / 4:21

Source: <https://techtarget.com>

Data Model Types:

- Semi-Structured Data

Semi-structured data is data that has not been organized into a specialized repository, such as a database, but that nevertheless has associated information, such as metadata, that makes it more amenable to processing than [raw data](#).

The difference between structured data, unstructured data and semi-structured data:
Unstructured data has not been organized into a format that makes it easier to access and process. In reality, very little data is completely unstructured. Even things that are often considered unstructured data, such as documents and images, are structured to some extent. Structured data is basically the opposite of unstructured: It has been reformatteed and its elements organized into a data structure so that elements can be addressed, organized and accessed in various combinations to make better use of the information. Semi-structured data lies somewhere between the two. It is not organized in a complex manner that makes sophisticated access and analysis possible; however, it may have information associated with it, such as [metadata](#) tagging, that allows elements contained to be addressed.

Here's an example: A Word document is generally considered to be unstructured data. However, you can add metadata tags in the form of keywords and other metadata that represent the document content and make it easier for that document to be found when people search for those terms -- the data is now semi-structured. Nevertheless, the document still lacks the complex organization of the database, so falls short of being fully structured data.



© 2019 IBM Corporation
2:01 / 4:21

Source: <https://techtarget.com>

Data Model Types:

- Unstructured Data

Unstructured data is information, in many different forms, that doesn't hew to conventional data models and thus typically isn't a good fit for a mainstream relational [database](#).

Thanks to the emergence of alternative platforms for storing and managing such data, it is increasingly prevalent in IT systems and is used by organizations in a variety of business intelligence and [analytics](#) applications.

Traditional [structured data](#), such as the transaction data in financial systems and other business applications, conforms to a rigid format to ensure consistency in processing and analyzing it. Sets of unstructured data, on the other hand, can be maintained in formats that aren't uniform, freeing analytics teams to work with all of the available [data](#) without necessarily having to consolidate and standardize it first. That enables more comprehensive analyses than would otherwise be possible.

Types of unstructured data

One of the most common types of unstructured data is text. Unstructured text is generated and collected in a wide range of forms, including Word documents, email messages, PowerPoint presentations, survey responses, transcripts of call center interactions, and posts from blogs and social media sites. Other types of unstructured data include images, audio and video files.

Source: <https://techtarget.com>



Structured Data

Structured Data: Flat File Databases

Flat-file databases take all the information from all the records and store everything in one table. This works fine when you have a small number of records related to a single topic, such as a person's name and phone number, but if you have hundreds or thousands of records, each with a number of fields, the database quickly becomes difficult to use.

SID	SFName	SLName	SteleNumber	CID	Cname	TID	Trainer	TrnTeleNumber
1	Mary	Hinkle	555.123.4567	101	Data Basics	T01	Charles Hill	555.987.6543
2	Paul	Litz	555.258.8963	101	Data Basics	T01	Charles Hill	555.987.6542
1	Mary	Hinkle	555.123.4567	102	Web Design	T02	Glen Barber	555.879.4652
3	Dee	Coleman	555.357.9514	203	Relational Design	T03	Rick Dobson	555.324.2986
4	Don	Charney	555.369.8741	204	VBA Programming	T03	Rick Dobson	555.324.2986

Source: <https://en.wikipedia.org/>

© 2019 IBM Corporation
II 0:36 / 7:15

Structured Data: Relational Databases

Relational databases separate this mass of information into numerous **tables**. All the columns in each table should be about one topic, such as "student information," "class information," or "trainer information."

SID	SFName	SLName	SteleNumber	CID	Cname	TID	Trainer	TrnTeleNumber
1	Mary	Hinkle	555.123.4567	101	Data Basics	T01	Charles Hill	555.987.6543
2	Paul	Litz	555.258.8963	101	Data Basics	T01	Charles Hill	555.987.6542
1	Mary	Hinkle	555.123.4567	102	Web Design	T02	Glen Barber	555.879.4652
3	Dee	Coleman	555.357.9514	203	Relational Design	T03	Rick Dobson	555.324.2986
4	Don	Charney	555.369.8741	204	VBA Programming	T03	Rick Dobson	555.324.2986

Source: <https://en.wikipedia.org/>

© 2019 IBM Corporation
II 2:35 / 7:15

Structured Data: Relational Databases

The tables for a relational database are linked to each other through the use of **keys**. Each table may have one **primary key** and any number of **foreign keys**. A foreign key is simply a primary key from one table that has been placed in another table.

Primary Key			
SID	SFName	SLName	SteleNumber
1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963
1	Mary	Hinkle	555.123.4567
3	Dee	Coleman	555.357.9514
4	Don	Charney	555.369.8741

Primary Key			
SID	CID	Cname	TID
1	101	Data Basics	T01
2	101	Data Basics	T01
1	102	Web Design	T02
3	203	Relational Design	T03
4	204	VBA Programming	T03

Primary Key		
TID	Trainer	TrnTeleNumber
T01	Charles Hill	555.987.6543
T01	Charles Hill	555.987.6542
T02	Glen Barber	555.879.4652
T03	Rick Dobson	555.324.2986
T03	Rick Dobson	555.324.2986

The most important rules for designing relational databases are called **Normal Forms**.

When databases are designed properly, huge amounts of information can be kept under control. This lets you **query** the database (search for information) and quickly get the answer you need.

Query: "What students are taking classes from trainer CHARLES HILL?"

Answer:

1	Mary	Hinkle	555.123.4567
2	Paul	Litz	555.258.8963

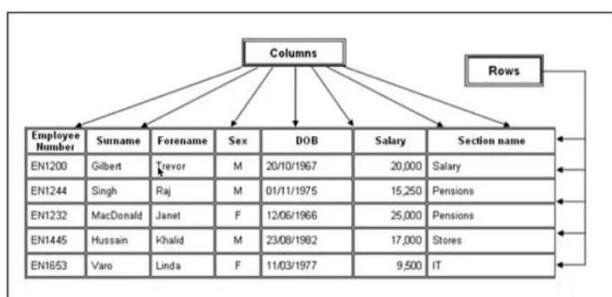
Compiled by Rick Dobson
Graphics & Design by Fred Schneider

© 2019 IBM Corporation

|| 3:33 / 7:15

Structured Data: SQL; "Structured Query Language", the language used to interact with data inside a database.

SQL (S-Q-L, /sɪk'wɛl/ "sequel"; Structured Query Language) is a **domain-specific language** used in programming and designed for managing data held in a **relational database management system** (RDBMS), or for stream processing in a **relational data stream management system** (RDSMS). It is particularly useful in handling **structured data** where there are relations between different entities/variables of the data.



dvrentals> select title, release_year, length, replacement_cost from film	dvrentals> where length > 120 and replacement_cost > 29.99
dvrentals> order by title desc	title release_year length replacement_cost
'West Lion'	2006 159 29.99
'Virgin Daisy'	2006 179 29.99
'Uncut Suicides'	2006 172 29.99
'Tracy Cider'	2006 142 29.99
'Song Hedwig'	2006 165 29.99
'Slacker Sons'	2006 170 29.99
'Soul Packer'	2006 154 29.99
'River Outlaw'	2006 149 29.99
'Right Cranes'	2006 153 29.99
'Quest Mussolini'	2006 177 29.99
'Poseidon Forever'	2006 159 29.99
'Loathing Legally'	2006 140 29.99
'Lawless Vision'	2006 181 29.99
'Jingle Sagebrush'	2006 124 29.99
'Jericho Man'	2006 111 29.99
'Dance Run'	2006 135 29.99
'Gilmore Boiled'	2006 163 29.99
'Floats Garden'	2006 145 29.99
'Fantasia Park'	2006 131 29.99
'Extraordinary Conqueror'	2006 122 29.99
'Everyone Craft'	2006 163 29.99
'Dirty Ace'	2006 147 29.99
'Clyde Theory'	2006 139 29.99
'Clockwork Paradise'	2006 143 29.99
'Ballroom Mockingbird'	2006 173 29.99

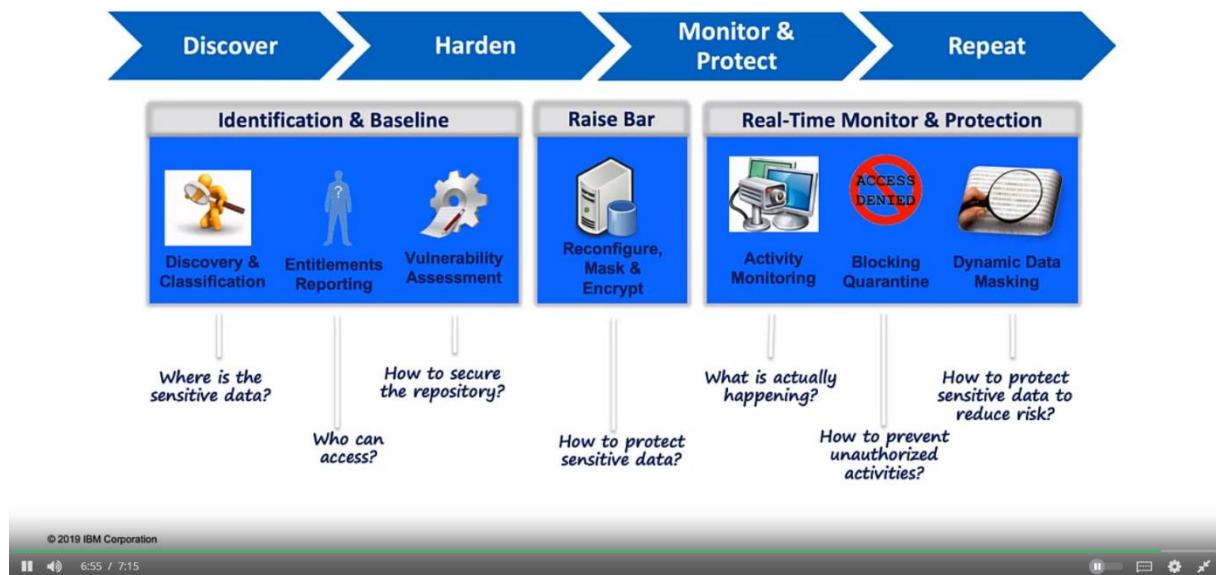
(29 rows)

Source: <https://en.wikipedia.org/>

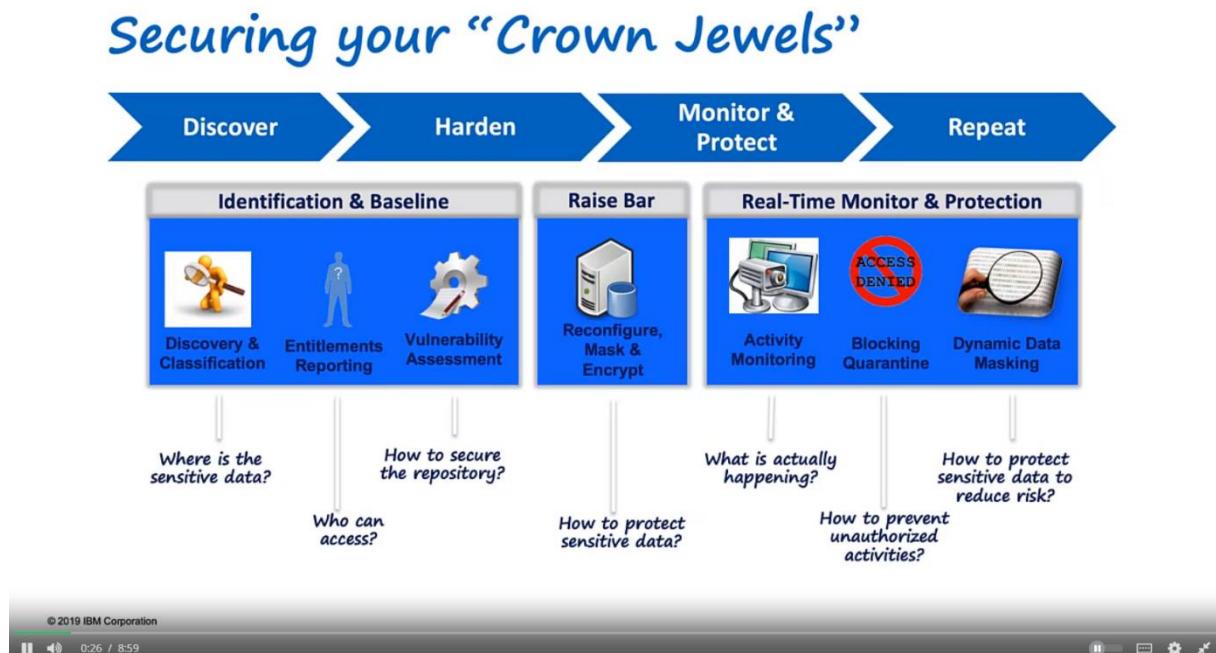
© 2019 IBM Corporation

|| 5:09 / 7:15

Securing your “Crown Jewels”

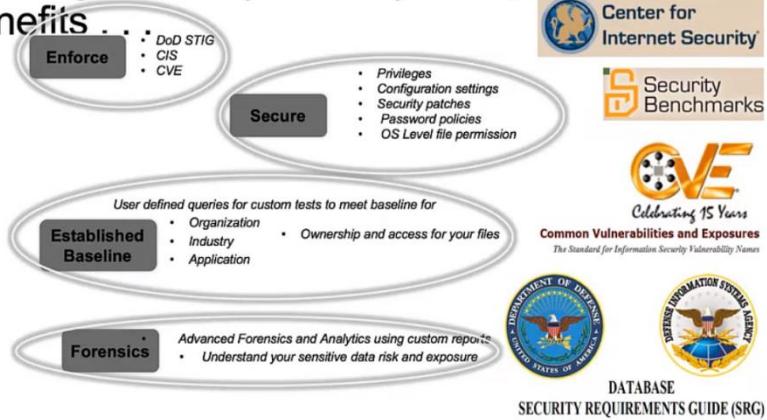


Securing the Crown Jewels



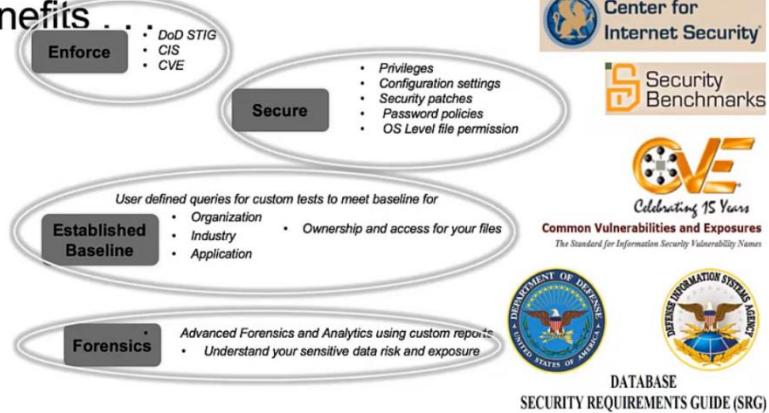
Leveraging Security Industry Best Practices

Leverage security industry best practice and benefits . . .

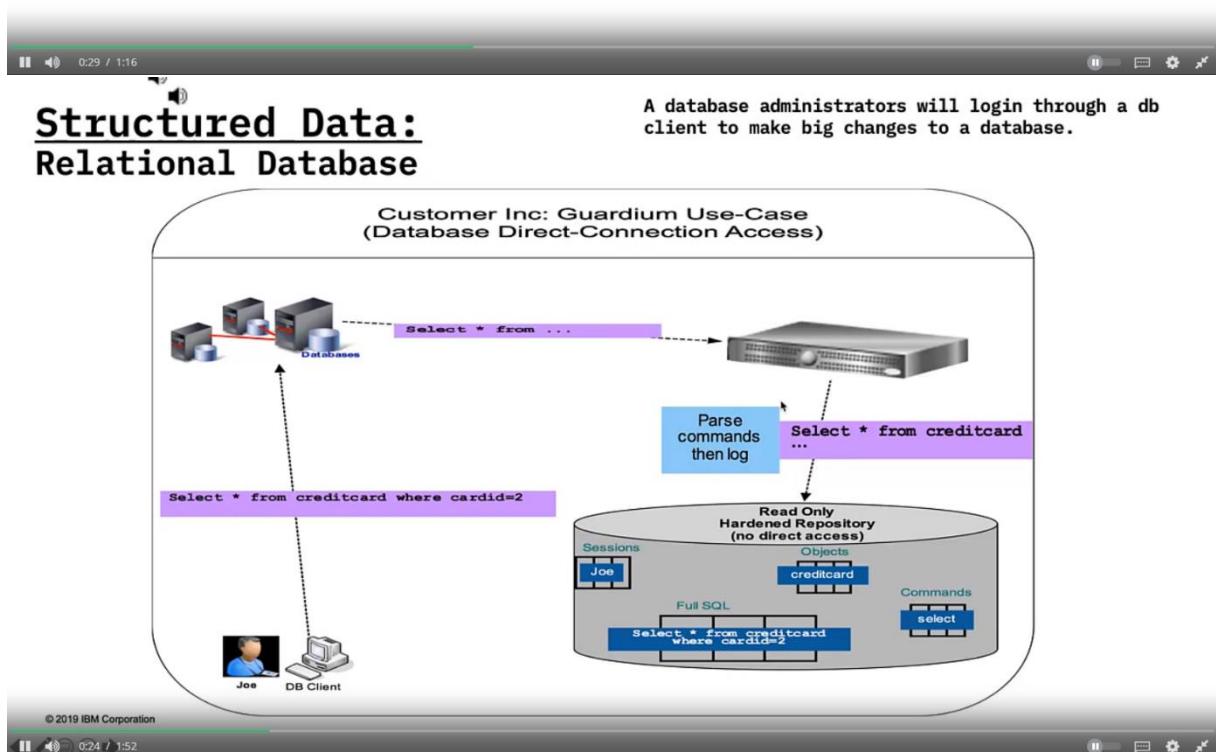


Structured Data and Relational Databases

Leverage security industry best practice and benefits . . .

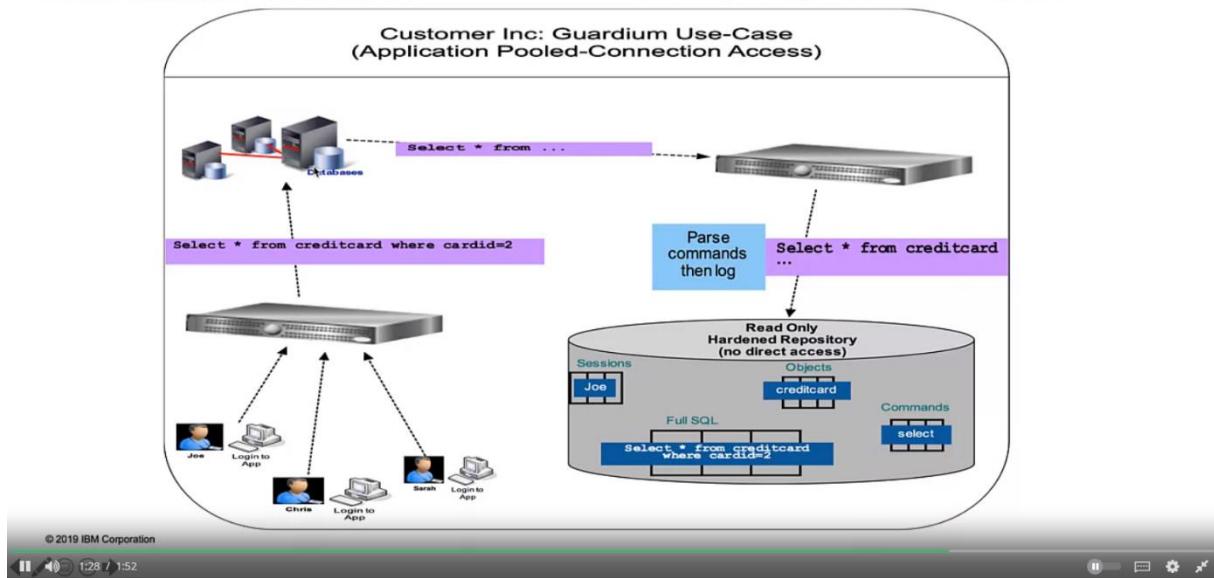


DATABASE SECURITY REQUIREMENTS GUIDE (SRG)



Structured Data: Relational Database

Perhaps the most common day-to-day use case for a database is using it as the backend of an application such as your organizations HR system, or even your organizations email system!



Anatomy of a Vulnerability Assessment Test Report

Anatomy of a VA test report

IBM InfoSphere™ Guardium™

Results for Security Assessment: My demo Assessment

Assessment executed: 2014-04-16 04:35:32.0

From: 2014-04-15 04:35:32.0

To: 2014-04-16 04:35:32.0

Client IP or IP subnet: Any

Server IP or IP subnet: Any

Tests passing: 36%

CG Tests passing: 3679

STG Tests passing: 1535

CVE Tests passing: 820

The above testing passing statistics do not take into account any filtering that may currently be applied, and do not include tests in any status other than passed or failed.

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

View Log | Home to Datasource List

Summary Test Results

Result History Shows Trends

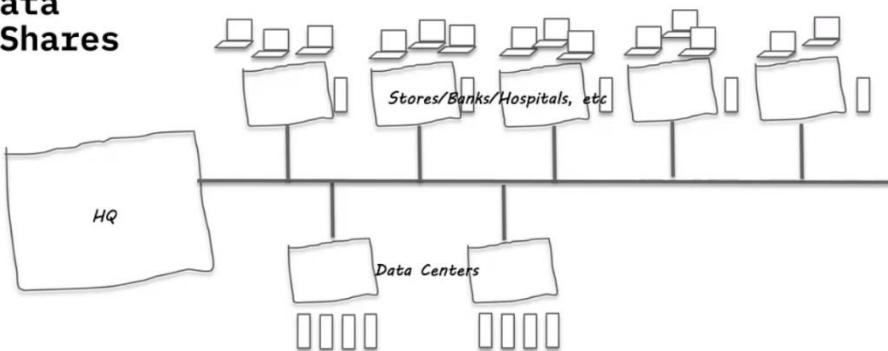
Detailed Test Results

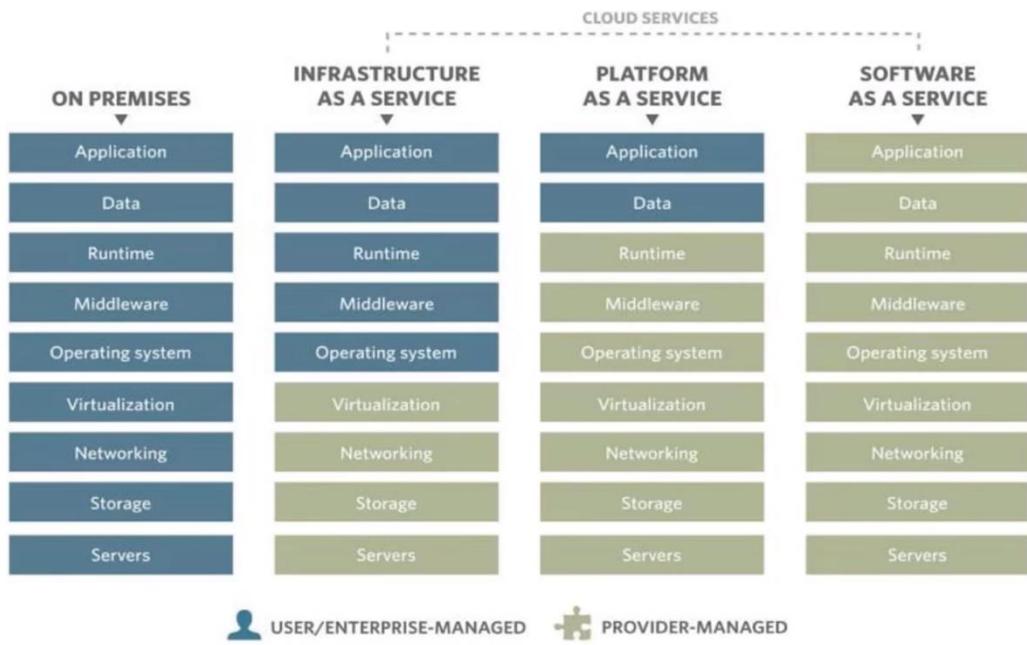
Detailed Remediation Suggestions

Securing Data Sources by Type

Data Source Types:

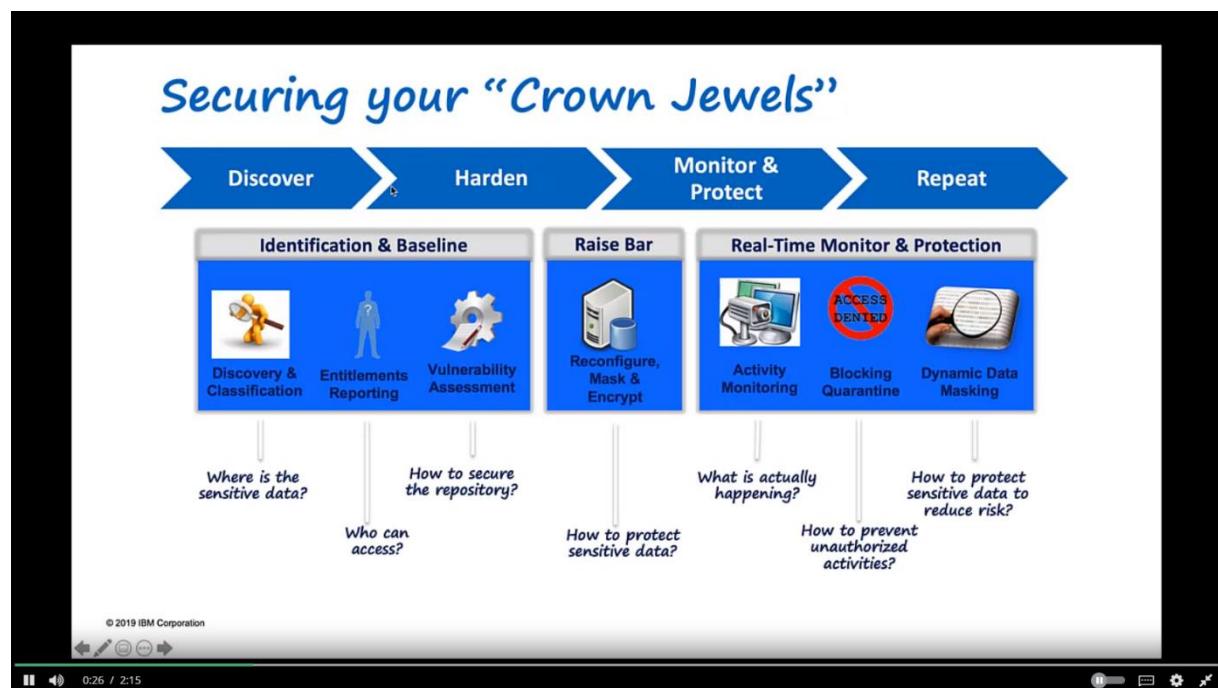
- Distributed Databases
- Data Warehouses
- Big Data
- File Shares





© 2019 IBM Corporation

Securing Databases Wrap Up



Data Monitoring

DATA ACTIVITY MONITORING / AUDITING / LOGGING

1. Does your product log all key activity, including key generation, retrieval/usage, etc.?
2. Demo data access activity monitoring and logging of the activity monitoring?
3. Does your product monitor for unique user identities (including highly privileged users such as administrators and developers) with access to the data?
4. At the storage level, can it detect/identify assess to highly privileged users such as database administrators, system administrators or developers?
5. Does your product generate real time alerts of policy violations while recording activities?
6. Does your product monitor user data access activity in real time with customizable security alerts and blocking unacceptable user behavior, access patterns or geographic access, etc.? If yes please describe.
7. Does your product generate alerts?
8. Demo the capability for reporting and metrics using information logged?
9. Does your product create auditable reports of data access and security events with customizable details that can address defined regulations or standard audit process requirements? If yes please
10. Does your product support the ability to log security events to a centralized security incident and event management (SIEM) system?
11. Demo monitoring of non-Relational Database Management Systems (RDBMS) systems, such as Cognos, Hadoop, Spark, etc.
12. Demo the following event attributes and to what level of granularity?

The screenshot shows a presentation slide with the following details:

Header: IBM Security

Title: DATA ACTIVITY MONITORING / AUDITING / LOGGING

List:

13. Demo when the product provides the following event attributes and to what level of granularity?
 - o Log date and time (international format)
 - o Event date and time - the event time stamp may be different to the time of logging e.g. server logging where the client application is hosted on remote device that is only periodically or intermittently online
 - o Interaction identifier
14. Demo sufficient information in the log record to establish what events occurred and who or what caused them?
15. Demo configurations configured to monitor user account additions and changes?
16. Demo configurations to monitor the following event?
Significant instances of failed password attempts and against multiple accounts within a short time frame which may indicate hacking attempts
17. Demo configurations to monitor the following event?
Significant instances of failed access attempts to the database not authorized to the account ID
18. Demo configurations to monitor the following event?
Attempts to SELECT the list of users and passwords
19. Demo configurations to monitor the following event?
All direct access to the database from accounts which should be limited to access through the application
20. Demo configurations to monitor the following event?
Use of nonstandard tools (i.e. Excel/Access) to directly access DBMS
21. Demo configurations to monitor the following event?
Use of Application ID (ApplID) from a source other than the defined owner Application location (based on host name or IP address)
22. Demo configurations to monitor the following event?
Log failures, manual logging shut down and attempts to purge

IBM Guardian (GT1) https://10.10.9.239:8443/#protect_policy/0

Most Visited Box Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C... Machine Type Standalone

IBM Guardian 11:45 User Interface Search

Policy Rules Allow-All

Expand All Collapse All Select All Unselect All Delete Selected Copy Rules Filter: []

[]	[]	[]	[]	1	Access Rule: Alert - Access to Sensitive Objects (Installed)
[]	[]	[]	[]	2	Exception Rule: Alert on failed logon attempts (Installed)
[]	[]	[]	[]	3	Access Rule: terminate - SSN Access by System (Installed)
[]	[]	[]	[]	4	Access Rule: Exclude Applications (Installed)
[]	[]	[]	[]	5	Access Rule: Ignore objects (Installed)
[]	[]	[]	[]	6	Access Rule: Exclude commands (Installed)
[]	[]	[]	[]	7	Access Rule: Log full details (Installed)

Rule Suggestion Suggest from DB

Rule min. ct. 0 Object Group min. ct. 1 Suggest Rules

Back Add Rules Reinstall Uninstall Policy Simulator

DATA ACTIVITY MONITORING / AUDITING / LOGGING

3. Does your product monitor for unique user identities (including highly privileged users such as administrators and developers) with access to the data?

1:31 / 4:35 32 IBM Security IBM

IBM Guardium (G10) <https://10.10.9.239:8443/guard-00089a0-a-c530-459c-98dc-842778151e3>

User Interface Search [record application demo on mac](#)

Machine Type Standalone

IBM Guardium 11:47 User Interface More Actions ?

Privileged User Activity

Start Date: 2017-05-10 12:28:33 | End Date: 2017-05-11 12:28:33

Export Actions ?

Timestamp Session Start Client IP DB User Name OS User Source Program Server IP Service Name Full Sql Count of FULL SQLs

2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalaryStructure add SalaryMultipleFactor float	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table t1 (i int)	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	drop table t1	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	SELECT 'GuardAppEvent:Released' from dual	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table findat1 add j integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table hrdta add empsn varchar(11)	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalesRegion add ASIAPAC integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	ALTER TABLE t1 ADD j INTEGER	1

Total: 809 [1](#) [2](#) [3](#) ... [41](#) [20](#) | [50](#) | [100](#)

IBM Guardium (G10) https://10.10.9.239:8443/guardrest/report?instanceId=187&rid=435450&id=2004&action=drilldown&mode=full&tabbed=&isAscending=false&sortCol=-6&from=16org.apache.catalina.filters.CSRF_NONCE=1

User Interface Search [record application demo on mac](#)

Machine Type Standalone

IBM Guardium Report Drilldown More Actions ?

Privileged User Activity

Generated by user: date
On: 2017-05-11 12:29:04

REMOTE_SOURCE:
From: NOW-1 DAY
To: NOW
Alias: Off

Timestamp	Session Start	Client IP	DB User Name	OS User	Source Program	Server IP	Service Name	Full Sql	Count of FULL SQLs
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalaryStructure add SalaryMultipleFactor float	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table t1 (i int)	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	drop table t1	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	SELECT 'GuardAppEvent:Released' from dual	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table findat1 add j integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table hrdta add empsn varchar(11)	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalesRegion add ASIAPAC integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	ALTER TABLE t1 ADD j INTEGER	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table findat1 add j integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table hrdta add empsn varchar(11)	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalesRegion add ASIAPAC integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	ALTER TABLE t1 ADD j INTEGER	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table findat1 add j integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add Amount integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add ContractAmount integer	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add PO varchar(5)	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add UnderContract varchar(3)	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table findat1 (i integer, k varchar(50))	1
2017-05-11 10:53:32	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table hrdta (empid integer, empname varchar(20))	1

DATA ACTIVITY MONITORING / AUDITING / LOGGING

- At the storage level, can it detect/identify assess to highly privileged users such as database administrators, system administrators or developers?

The screenshot shows the IBM Guardium interface with the following details:

Header: IBM Security, IBM Guardium (O10), 33, 11:49, User Interface Search, Machine Type Standalone.

Section Title: Admin (Highly Privileged) User Activity

Table Headers: Timestamp, Session Start, Client IP, DB User Name, OS User, Source Program, Server IP, Service Name, Full Sql, Count of FULL SQLs.

Table Data: The table lists six rows of activity from 2017-05-11 10:55:10 to 2017-05-11 10:58:10. The 'Full Sql' column contains complex SQL statements related to table creation and modification.

Timestamp	Session Start	Client IP	DB User Name	OS User	Source Program	Server IP	Service Name	Full Sql	Count of FULL SQLs
2017-05-11 10:55:10	2017-05-11 10:54:54	10.10.9.56	SYSTEM	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add PO varchar(5)	1
2017-05-11 10:55:10	2017-05-11 10:54:54	10.10.9.56	SYSTEM	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add UnderContract varchar(3)	1
2017-05-11 10:55:10	2017-05-11 10:54:54	10.10.9.56	SYSTEM	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table findatt1 (i integer, k varchar(50))	1
2017-05-11 10:55:10	2017-05-11 10:54:54	10.10.9.56	SYSTEM	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table hydata (empid integer, empname varchar(20))	1
2017-05-11 10:55:10	2017-05-11 10:54:54	10.10.9.56	SYSTEM	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table inventors (ProductID integer, Count integer, Cost integer, Description varchar(20))	1
2017-05-11 10:55:10	2017-05-11 10:54:54	10.10.9.56	SYSTEM	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table NewProductSales(ProductID integer, Name varchar(20), cost integer, revenue integer)	1

Data Alerts

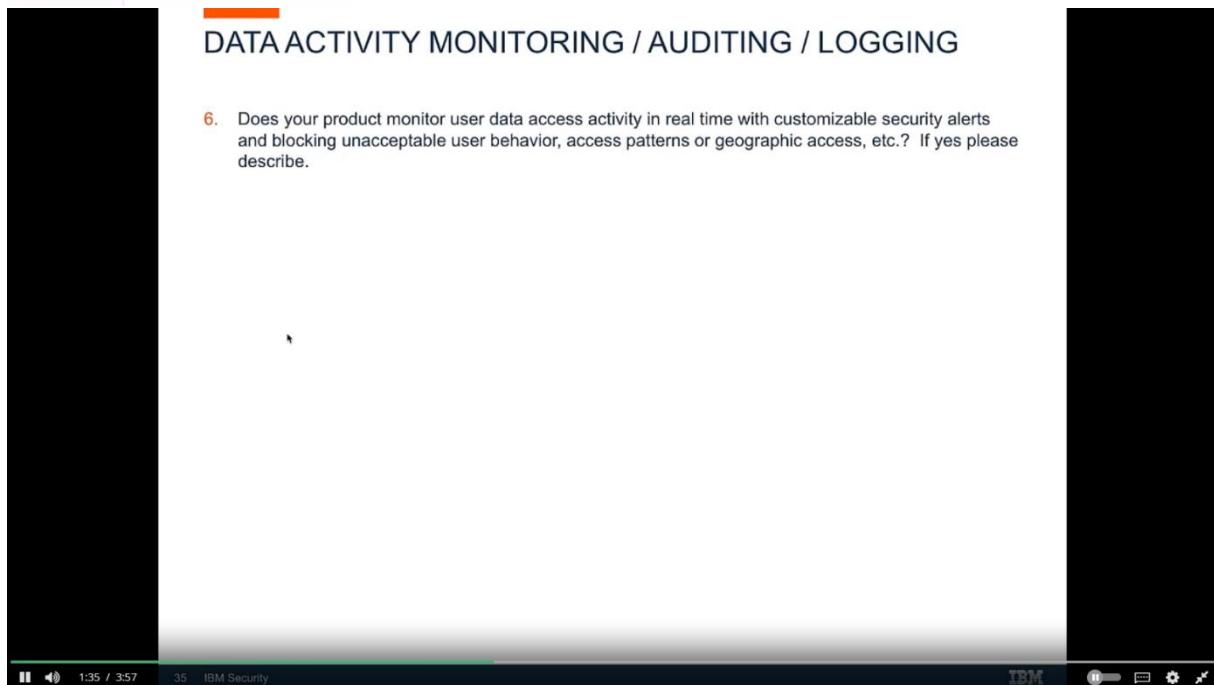
DATA ACTIVITY MONITORING / AUDITING / LOGGING

5. Does your product generate real time alerts of policy violations while recording activities?

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Investigate' section selected, which is highlighted in blue. The main content area displays a table titled 'Policy Violations Details' with the following columns: Timestamp, Category Name, Access Rule Description, Client IP, Server IP, DB User Name, Full SQL String, Severity Description, and Count of Policy Rule Violations. The table lists several rows of policy violations, such as 'Alert - Access to Sensitive Objects' and 'terminate - SSN Access by System'. The bottom of the table shows a total of 114 violations and page navigation links.

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Count of Policy Rule Violations
2017-05-11 12:55:26		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	JOE	select * from creditcard	INFO	1
2017-05-11 12:53:34		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	JOE	select * from creditcard	INFO	1
2017-05-11 12:08:31		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:08:31		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:08:22		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select* from joe.creditcard	INFO	1
2017-05-11 10:54:40		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE CreditCard	INFO	1
2017-05-11 10:54:40		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE SSN	INFO	1
2017-05-11 10:53:56		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE SSN	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	DELETE CREDITCARD WHERE NAME_ON_CARD = 'Abby Wadsworth'	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	DELETE CREDITCARD WHERE NAME_ON_CARD = 'Ken Wadsworth'	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	Select * from Creditcard where name_on_card like '%Patent%'	INFO	1

-Messages Report			
Message Date	Message STATUS	Sent To	Message Text
2017-05-11 12:55:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects 'nCategory: Classification: Severity INFO nRule # 20060 [Alert - Access to Sensitive Objects] nRequest Info: { Session start: 2017-05-11 12:55:57 Session End: 2017-05-11 12:55:57 Session alert: 2017-05-11 12:55:57 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.58 (OSPREY) Client PORT: 50303 Server Port: 273 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE vApplication User Name: v\$source Program: SQLPLUS SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard vNoValues: select * from creditcard InSQL Status: In
2017-05-11 12:53:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects 'nCategory: Classification: Severity INFO nRule # 20060 [Alert - Access to Sensitive Objects] nRequest Info: { Session start: 2017-05-11 12:53:53 Session End: 2017-05-11 12:53:53 Session alert: 2017-05-11 12:53:53 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.58 (OSPREY) Client PORT: 50303 Server Port: 273 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE vApplication User Name: v\$source Program: SQLPLUS SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard vNoValues: select * from creditcard InSQL Status: In
2017-05-11 12:08:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects 'nCategory: Classification: Severity INFO nRule # 20060 [Alert - Access to Sensitive Objects] nRequest Info: { Session start: 2017-05-11 12:08:53 Session End: 2017-05-11 12:08:53 Session alert: 2017-05-11 12:08:53 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.58 (OSPREY) Client PORT: 50303 Server Port: 273 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: SYSTEM vApplication User Name: v\$source Program: SQLPLUS SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard vNoValues: select * from creditcard InSQL Status: In



IBM Guardium (G10) Mail Calendar Service Benefit Plan Guard... + https://10.10.9.239:8443/#/guard-015a7f1d5-af03-404c-ac94-74786507f903

Most Visited Box Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C...

IBM Guardium 12:13 User Interface Search admin.acitl.BeaReRJL.DataPrivacy.datesec-exempt,cbx_id= dateInfosec Machine Type Standalone

-Messages Report

Start Date: 2017-05-10 12:56:33 | End Date: 2017-05-11 12:56:33 More Export Actions

Message Date Message STATUS Sent To Message Text

2017-05-11 12:55:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects InCategory: Classification: Severity INFO InRule # 20060 [Alert - Access to Sensitive Objects] InRequest Info: [Session start: 2017-05-11 12:55:57 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.54 (OSPREY) Client PORT: 50303 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE vApplication User Name: inSQL vSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard vNoValues: select * from creditcard vSQL Status: In
2017-05-11 12:53:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects InCategory: Classification: Severity INFO InRule # 20060 [Alert - Access to Sensitive Objects] InRequest Info: [Session start: 2017-05-11 12:53:53 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.54 (OSPREY) Client PORT: 50303 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE vApplication User Name: inSQL vSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard vNoValues: select * from creditcard vSQL Status: In
2017-05-11 12:08:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects InCategory: Classification: Severity INFO InRule # 20060 [Alert - Access to Sensitive Objects] InRequest Info: [Session start: 2017-05-11 12:08:57 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.54 (OSPREY) Client PORT: 50303 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE vApplication User Name: inSQL vSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard vNoValues: select * from creditcard vSQL Status: In

Report - 1 / 2 / 3 / 6 2015 / 3:57

oracle@osprey:~ — ssh root@10.10.9.56 — 80x24

```
[oracle@osprey ~]$ [oracle@osprey ~]$ [oracle@osprey ~]$ sqlplus

SQL*Plus: Release 11.2.0.2.0 Production on Thu May 11 14:59:14 2017

Copyright (c) 1982, 2011, Oracle. All rights reserved.

Enter user-name: system
Enter password:

Connected to:
Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production

SQL> select * from joe.ssn;
select * from joe.ssn
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel
Process ID: 21501
Session ID: 10 Serial number: 705
I

SQL>
```

2:54 / 3:57

IBM Guardium (G10) | Mail | Calendar | Service Benefit Plan Guard... | +

https://10.10.9.239:8443/investigate_policyViolations

Most Visited | Box | Developer Works | Documentation | Field Technical Co... | FMS | GSA | SFTP | Sales | Security | Support | Verse | getAbstract | G V10 | IBM Bluemix - Netw... | CTP | Skype | IBM Security Guar... | IBM Recognition C...

IBM Guardium 12:14 User Interface Search Machine Type Standalone

Policy Violations Details

Start Date: 2017-05-08 13:00:07 | End Date: 2017-05-14 13:00:07

More Export Actions

Timestamp Category Name Access Rule Description Client IP Server IP DB User Name Full SQL String Severity Description Count of Policy Rule Violations

2017-05-11 12:59:44		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:59:44		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:59:26		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	JOE	select * from creditcard	INFO	1
2017-05-11 12:53:34		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	JOE	select * from creditcard	INFO	1
2017-05-11 12:09:31		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:09:31		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:08:22		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select* from joe.creditcard	INFO	1
2017-05-11 10:54:40		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE CreditCard	INFO	1
2017-05-11 10:54:40		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE SSN	INFO	1
2017-05-11 10:53:56		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE SSN	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	DELETE CREDITCARD WHERE NAME_ON_CARD = 'Abby Wadsworth'	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	DELETE CREDITCARD WHERE	INFO	1

Total: 116 | 1 2 3 ... 6 | 20 | 50 | 100

DATA ACTIVITY MONITORING / AUDITING / LOGGING

- Does your product generate alerts?

IBM Guardium (G10) Mail Calendar Service Benefit Plan Guard... + https://10.10.9.239:443/#!/investigate_policyViolations

Most Visited Box Developer Works Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C...

IBM Guardium 12:15 User Interface User Interface Search admin.acudit.ResultList.DataPrivacyListExempt,dba_id= dateInfosec Machine Type Standalone

Policy Violations Details

Start Date: 2017-05-08 13:00:07 | End Date: 2017-05-14 13:00:07 More

Export Actions

Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Count of Policy Rule Violations
2017-05-11 12:59:44		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:59:44		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:59:26		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	JOE	select * from creditcard	INFO	1
2017-05-11 12:53:34		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	JOE	select * from creditcard	INFO	1
2017-05-11 12:09:31		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:08:31		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	select * from joe.ssn	INFO	1
2017-05-11 12:08:22		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	select* from joe.creditcard	INFO	1
2017-05-11 10:54:40		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE CreditCard	INFO	1
2017-05-11 10:54:40		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE SSN	INFO	1
2017-05-11 10:54:40		terminate - SSN Access by System	10.10.9.56	10.10.9.56	SYSTEM	DROP TABLE SSN	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	DELETE CREDITCARD WHERE NAME_ON_CARD = 'Abby Wadsworth'	INFO	1
2017-05-11 10:53:56		Alert - Access to Sensitive Objects	10.10.9.56	10.10.9.56	LARRY	DELETE CREDITCARD WHERE	INFO	1

Total: 116 1 2 3 ... 6 20 | 50 | 100

Data Activity Reporting

DATA ACTIVITY MONITORING / AUDITING / LOGGING

8. Demo the capability for reporting and metrics using information logged?

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Investigate' section selected, containing links for Database Activities, Database Administration, Detailed Activities, Exceptions, Hadoop, Schema Changes, and Query Builder. The main content area displays a log entry from May 11, 2017, at 13:01:23. The log table has columns for Message ID, STATUS, Sent To, and Message Text. The first log entry shows an alert based on rule ID 10, with the message text detailing an access to sensitive objects via SQL*Plus. The second log entry is similar, also from May 11, 2017, at 13:01:23, with the same alert details.

Message ID	STATUS	Sent To	Message Text
I-05-11 13:01:23	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects InCategory: Classification: Severity INFO InRule # 2060 [Alert - Access to Sensitive Objects] InSession [Session start: 2017-05-11 12:59:20 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 21875 Service Name: 134 Database Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: SYSTEM InApplication User Name: inSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from joe.jssn InNoValues: select * from joe.sar InSql Status: In
I-05-11 13:01:23	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects InCategory: Classification: Severity INFO InRule # 2060 [Alert - Access to Sensitive Objects] InSession [Session start: 2017-05-11 12:59:20 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 50309 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE InApplication User Name: inSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard InNoValues: select * from creditcard InSql Status: In
I-05-11 13:01:23	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects InCategory: Classification: Severity INFO InRule # 2060 [Alert - Access to Sensitive Objects] InSession [Session start: 2017-05-11 12:59:20 Server Type: ORACLE Client: 10.10.9.56 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 50309 Server Port: 278 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE InApplication User Name: inSource Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard InNoValues: select * from creditcard InSql Status: In

DATA ACTIVITY MONITORING / AUDITING / LOGGING

9. Does your product create auditable reports of data access and security events with customizable details that can address defined regulations or standard audit process requirements? If yes please

The screenshot shows the IBM Guardium Audit Process Builder interface. On the left, a sidebar menu includes options like Welcome, Setup, Manage, Discover, Harden, Investigate, Protect, Comply (which is selected), Accelerators, Reports, and My Dashboards. The main panel is titled "Audit Process Builder" and displays the "User Activity" audit process. It shows the following configuration details:

Details for: User Activity	
Name and archive	User Activity
Add tasks	1 Task
Send results	2 Receivers
Schedule audit process	Schedule when the audit process will be repeated
Run audit process	Optional: Run audit process

At the bottom of the main panel, there are "Run Once Now", "Save", "Reset", and "View Results" buttons.

DATA ACTIVITY MONITORING / AUDITING / LOGGING

10. Does your product support the ability to log security events to a centralized security incident and event management (SIEM) system?

```
35 / 1 8:16 39 IBM Security Terminal Shell Edit View Window Help root@osprey: ~ ssh root@10.10.9.86 -- 101+24
May 11 15:55:59 osprey Trace: Level: Error, Trace ID: 62598-1769#012 Listener->gSoap worker(0): Client received an error: [300] Failed to execute GetProgramActualStatus. Running Program content is invalid
May 11 15:55:59 osprey Trace: Level: Error, Trace ID: 2049-572#012 Listener->gSoap worker(0): Raising server error: [300] Failed to execute Ge
tProgramActualStatus. Running Program content is invalid
May 11 15:56:00 osprey Trace: Level: Error, Trace ID: 2049-572#012 bnsAdmin->gSoap worker(0): Raising server error: [300] Failed to execute Get
ProgramActualStatus. Running Program content is invalid
May 11 15:56:00 osprey Trace: Level: Error, Trace ID: 2049-572#012 Listener->gSoap worker(0): Client received an error: [300] Failed to execute Ge
tProgramActualStatus. Running Program content is invalid. Specific error: 300. GSoap error: #2
May 11 15:56:00 osprey Trace: Level: Error, Trace ID: 2049-572#012 Listener->gSoap worker(0): Raising server error: [300] Failed to execute Ge
tProgramActualStatus. Running Program content is invalid
May 11 15:56:00 osprey Trace: Level: Error, Trace ID: 2049-572#012 bnsAdmin->gSoap worker(0): Raising server error: [300] Failed to execute Del
eteDecisionPlan. Running Program content is invalid
May 11 15:56:00 osprey Trace: Level: Error, Trace ID: 62598-1769#012 Listener->gSoap worker(0): Client received an error: [300] Failed to execute Ge
tDeleteDecisionPlan. Running Program content is invalid. Specific error: 300. GSoap error: #2
May 11 15:56:00 osprey Trace: Level: Error, Trace ID: 2049-572#012 Listener->gSoap worker(0): Raising server error: [300] Failed to execute Delete
DecisionPlan. Running Program content is invalid
May 11 15:56:27 osprey Trace: Level: Error, Trace ID: 2049-572#012 Listener->gSoap worker(0): Raising server error: [322] Failed to execute bns
GetAllDecisionPlans. Service unavailable. Classification: Adminstration. Severity INFO #015#Rule #20868 [Alert - Access to Sensitive Objects]#015#nCategory: Classification: Severity INFO #015#Rule #20868 [Alert - Access to Sensitive Objects]#015#nRequest Infos [ Session start: 2017-05-11 13:56:02 Server Type: ORACLE Client: 10.10.9.55 (OSPREY) Server: 10.10.9.56 (OSPREY) Client PORT: 47553 Server Port: 465 Service Type: ORACLE Database Name: XE@XE Net Protocol: BEQUEATH DB Proto
col: TNS DB Protocol Version: 3.0 DB User: JOE#015#nApplication User Name: #015#nSource Program: SQLPLUS/OSPREY Authorization Code: #0 Request Type: 50L_Listener_Error From: Oracle Database Listener [From Application User Name: #015#nSource Program: SQLPLUS/OSPREY Authorization Code: #015#n
Last Error: #015#nSQL: select * from creditcard#015#nValueUsers: select * from creditcard#015#nSQL Status: #015#n
*** 294 Cal Anthony 3294 341-5678-9812-6294
Cal Anthony 15-JUN-33
*** 295 Cal Thomas 341-5678-9812-6295
CARDID FIRSTNAME LASTNAME CARDNUMBER
PIN TXN_ID TXN_DATE SECU
NAME_ON_CARD EXP
*** 3295 Cal Thomas 05-JUL-33
*** 296 Cal Smith 341-5678-9812-6296
Cal Smith 25-JUL-33
441 rows selected.
SQL> 
```

IBM Guardian (GT0) +

https://10.10.9.239:8443/#/guard-0f5a7f40-af03-404c-ac94-74786507f905

Most Visited ▾ Box Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C...

IBM Guardian 13:15 Data Search More Machine Type Standalone

-Messages Report

Start Date: 2017-05-10 14:05:13 | End Date: 2017-05-11 14:05:13

Message Date Message STATUS Sent To Message Text

2017-05-11 13:56:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects >Category: Classification: Severity INFO >Rule # 20050 [Alert - Access to Sensitive Objects] >Request Info: { Session start: 2017-05-11 13:56:02 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.58 (OSPREY) Client PORT: 47553 Server Port: 465 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE >Application User Name: joe >Source Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard >NoValues: select * from creditcard INSQL Status: In
2017-05-11 12:59:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects >Category: Classification: Severity INFO >Rule # 20050 [Alert - Access to Sensitive Objects] >Request Info: { Session start: 2017-05-11 12:59:02 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.58 (OSPREY) Client PORT: 21501 Server Port: 136 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: SYSTEM >Application User Name: SYSTEM >Source Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from joe.ssn >NoValues: select * from joe.ssn INSQL Status: In
2017-05-11 12:55:57	SENT	SYSLOG	Alert based on rule ID Alert - Access to Sensitive Objects >Category: Classification: Severity INFO >Rule # 20050 [Alert - Access to Sensitive Objects] >Request Info: { Session start: 2017-05-11 12:53:10 Server Type: ORACLE Client IP: 10.10.9.58 (OSPREY) Server: 10.10.9.58 (OSPREY) Client PORT: 50304 Server Port: 276 Service Name: ORACLEXE Database Name: XE@XE Net Protocol: BEQUEATH DB Protocol: TNS DB Protocol Version: 3.14 DB User: JOE >Application User Name: v\$source_program >Source Program: SQLPLUS@OSPREY Authorization Code: 0 Request Type: SQL_LANG Last Error: InSQL: select * from creditcard >NoValues: select * from creditcard INSQL Status: In

More Export Actions

Report

My Dashboards

DATA ACTIVITY MONITORING / AUDITING / LOGGING

11. Demo monitoring of non-Relational Database Management Systems (RDBMS) systems, such as Cognos, Hadoop, Spark, etc.

6:28 / 8:16 40 IBM Security

IBM Guardium (G10)

https://10.10.9.239:8443/investigate_bigsins

Most Visited Box Developer Works Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C...

Machine Type Standalone

IBM Guardium

13:19 Data Search

Report

05-11 14:08:25

No data found for current runtime parameters

Server IP Message Details DB User Name Source Program Application User BI Job ID BI User Name BI Job Name BI Jar Name Count of Message Details

Hadoop

Hadoop - BigInsights MapReduce Report

Hadoop - Exception Report

Hadoop - Full Message Details report

Hadoop - HBase Report

Hadoop - HDFS Report

Hadoop - Hus/Beeswax Exception Report

Hadoop - MapReduce Report

Hadoop - Unauthorized MapReduce Jobs

hadoop Hue/Beeswax Report

Schema Changes

Guardium Data Protection Dashboard

QueryBuilder

Report Builder

Search for Data Activity

Return to File Activity

6:45 / 8:16

Attributes to Include in Logging

DATA ACTIVITY MONITORING / AUDITING / LOGGING

12. Demo the following event attributes and to what level of granularity?

The screenshot shows a presentation slide with the title 'DATA ACTIVITY MONITORING / AUDITING / LOGGING' at the top. Below the title, there is a question: '13. Demo when the product provides the following event attributes and to what level of granularity?'. Underneath this question, there is a bulleted list of four items:

- o Log date and time (international format)
- o Event date and time - the event time stamp may be different to the time of logging e.g. server logging where the client application is hosted on remote device that is only periodically or intermittently online
- o Interaction identifier

The slide has a dark background with white text. The navigation bar at the bottom includes icons for back, forward, search, and other presentation controls.

IBM Guardium (G10)

https://10.10.9.239:8443/#/reports_tracking

Most Visited Box Developer Works Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C...

Machine Type Standalone

IBM Guardium 13:23 Data Search

Query Builder

Entity List

Activity Attributes Main Entity: FULL SQL

Query Fields

Add Count Add District Sort by count Partition optimization

Entity Attribute Field Mode Order-by Sort Rank Descend

Additional mode AND OR HAVING

Query Conditions Entity App. Attribute Operator Runtime Param.

All reports can be accessed through My Dashboard selection.

Delete Clone Roles Save Back

Data Mart Create Report Regenerate Add to My Custom Reports

1:03 / 6:01

IBM Guardium (G10)

https://10.10.9.239:8443/#/investigate_sqlbyusr

Most Visited Box Developer Works Documentation Field Technical Co... FMS GSA SFTP Sales Security Support Verse getAbstract G V10 IBM Bluemix - Netw... CTP Skype IBM Security Guar... IBM Recognition C...

Machine Type Standalone

IBM Guardium 13:24 Data Search

Full SQL By DB User

Start Date: 2017-05-11 13:14:43 | End Date: 2017-05-11 18:14:43 More

Export Actions

Timestamp Client IP DB User Name Session Start Source Program Full Sql Count of FULL SQLs

2017-05-11 13:55:02	10.10.9.56	JOE	2017-05-11 13:56:02	SQLPLUS@OSPREY	SELECT USER FROM DUAL	1
2017-05-11 13:58:02	10.10.9.56	JOE	2017-05-11 13:58:02	SQLPLUS@OSPREY	SELECT DECODE(A'A';'1';'2') FROM DUAL	1
2017-05-11 13:56:40	10.10.9.56	JOE	2017-05-11 13:56:02	SQLPLUS@OSPREY	select * from creditcard	1

20 / 50 / 100

DATA ACTIVITY MONITORING / AUDITING / LOGGING

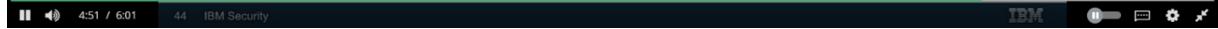
14. Demo sufficient information in the log record to establish what events occurred and who or what caused them?

The screenshot shows the IBM Guardium web interface. On the left, there's a sidebar with various navigation options: Welcome, Setup, Manage, Discover, Harden, Investigate, Protect, Comply, Accelerators, Reports, and My Dashboards. The 'Reports' option is currently selected and highlighted in blue. The main content area is titled 'Privileged User Activity' and displays a table of audit logs. The table has columns for Timestamp, Session Start, Client IP, DB User Name, OS User, Source Program, Server IP, Service Name, Full SQL, and Count of FULL SQLs. The table contains 10 rows of data, each representing a database session and its corresponding SQL statements. The SQL statements include various DDL and DML operations like creating tables, dropping tables, selecting data, and altering tables.

Timestamp	Session Start	Client IP	DB User Name	OS User	Source Program	Server IP	Service Name	Full SQL	Count of FULL SQLs
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	create table t1 (i int)	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	drop table t1	1
2017-05-11 10:54:04	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	SELECT * FROM "GuardAppEvent" WHERE event_type = 'Rel ease' and event_time > now() - 1 hour	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table hrdata add i integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table hrdata add empno varchar(11)	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add SalesRegion integer	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	ALTER TABLE t1 ADD j INTEGER	1
2017-05-11 10:54:03	2017-05-11 10:53:32	10.10.9.56	LARRY	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table test1 add j integer	1

DATA ACTIVITY MONITORING / AUDITING / LOGGING

15. Demo configurations configured to monitor user account additions and changes?



Failed Access Monitoring

DATA ACTIVITY MONITORING / AUDITING / LOGGING

16. Demo configurations to monitor the following event?

Significant instances of failed password attempts and against multiple accounts within a short time frame which may indicate hacking attempts

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Investigate' section selected, containing icons for Protect, Comply, Accelerators, Reports, and My Dashboards. The main content area displays a table titled 'Failed Login Attempts' with the following data:

DB User Name	Source Address	Destination Address	Database Protocol	Count of Exceptions
APPUSER	10.10.9.56	10.10.9.56	ORACLE	1
BOBBY	10.10.9.56	10.10.9.56	ORACLE	3
DALE	10.10.9.56	10.10.9.56	ORACLE	5
SAM	10.10.9.56	10.10.9.56	ORACLE	3
TEST	10.10.9.56	10.10.9.56	ORACLE	3

At the bottom of the table, it says 'Total: 5'. The top right of the interface shows 'Machine Type Standalone'.

DATA ACTIVITY MONITORING / AUDITING / LOGGING

17. Demo configurations to monitor the following event?

Significant instances of failed access attempts to the database not authorized to the account ID

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Reports' item selected. The main content area displays a table titled 'SQL Unauthorized Access'. The table has columns: Client IP, Server IP, Server Type, DB User Name, Database Error Text, Error Code, and Count of Exceptions. One row is shown:

Client IP	Server IP	Server Type	DB User Name	Database Error Text	Error Code	Count of Exceptions
10.10.9.56	10.10.9.56	ORACLE	LARRY	Insufficient privileges	ORA-01031	6

Failed Access Monitoring

DATA ACTIVITY MONITORING / AUDITING / LOGGING

16. Demo configurations to monitor the following event?

Significant instances of failed password attempts and against multiple accounts within a short time frame which may indicate hacking attempts

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Investigate' section selected, containing icons for Protect, Comply, Accelerators, Reports, and My Dashboards. The main content area displays a table titled 'Failed Login Attempts' with the following data:

DB User Name	Source Address	Destination Address	Database Protocol	Count of Exceptions
APPUSER	10.10.9.56	10.10.9.56	ORACLE	1
BOBBY	10.10.9.56	10.10.9.56	ORACLE	3
DALE	10.10.9.56	10.10.9.56	ORACLE	5
SAM	10.10.9.56	10.10.9.56	ORACLE	3
TEST	10.10.9.56	10.10.9.56	ORACLE	3

At the bottom of the table, it says 'Total: 5'. The top right of the interface shows 'Machine Type Standalone'.

DATA ACTIVITY MONITORING / AUDITING / LOGGING

17. Demo configurations to monitor the following event?

Significant instances of failed access attempts to the database not authorized to the account ID

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Reports' section selected. The main content area displays a table titled 'SQL Unauthorized Access' with the following data:

Client IP	Server IP	Server Type	DB User Name	Database Error Text	Error Code	Count of Exceptions
10.10.9.56	10.10.9.56	ORACLE	LARRY	Insufficient privileges	ORA-01031	6

Suspicious Access Events, Part 1

DATA ACTIVITY MONITORING / AUDITING / LOGGING

18. Demo configurations to monitor the following event?

Attempts to SELECT the list of users and passwords

The screenshot shows the IBM Guardium web interface. On the left is a navigation sidebar with icons for Welcome, Setup, Manage, Discover, Harden, Investigate, Protect, Comply, Accelerators, Reports, and My Dashboards. The main content area has a title "Access to List of Users". It displays a table with the following data:

Timestamp	Session Start	Client IP	DB User Name	OS User	Source Program	Server IP	Service Name	Full SQL	Count of FULL SQLs
2017-05-11 10:34:14	2017-05-11 10:34:02	10.10.9.239	SYSTEM	TOMCAT	JDBC THIN CLIENT	10.10.9.56	XE	<pre>pwd d, dba_users u where u.username=d.username and u.account_status = 'OPEN'</pre> <pre>SELECT SUM (COL1) FROM (SELECT COUNT(*) COL1 FROM DBA_PROFILES P1, DBA_PROFILES P2 WHERE P1.PROFILE = P2.PROFILE AND P1.RESOURCE_NAME = ME + '@' + PASSWORD_REUSE_E_MAX AND P2.RESOURCE_NAME = ME + '@' + PASSWORD_REUSE_E_MAX AND P1.LIMIT = P2.LIMIT IN (SELECT DISTINCT PROFILE FROM DBA_USERS WHERE ACCOUNT_STATUS = 'OPEN') AND (P2.LIMIT IS NULL OR P2.LIMIT = 'UNLIMITED') OR (P2.LIMIT = 'DEFAULT' AND EXISTS (SELECT</pre>	2

At the bottom of the table, there are navigation links for page numbers 1, 2, 3, ..., 59, ... and a total count of 201.

DATA ACTIVITY MONITORING / AUDITING / LOGGING

19. Demo configurations to monitor the following event?

All direct access to the database from accounts which should be limited to access through the application

The screenshot shows the IBM Guardium web interface. The left sidebar has a 'Reports' tab selected. The main area displays a table titled 'Unauthorized Use of Application ID' with the following data:

Timestamp	Session Start	Client IP	DB User Name	OS User	Source Program	Server IP	Service Name	Full Sql	Count of FULL SQLs
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table findat1 add j integer	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table hrdta add empsize varchar(11)	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add NetSales integer	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table NewProductSales add RollupByRegions integer	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalaryStructure add SalaryMultipleFactor float	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table SalesRegion add ASIA PAC Integer	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	alter table test1 add j integer	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add Amount integer	1
2017-05-11 10:52:15	2017-05-11 10:51:28	10.10.9.56	APPUSER	ORACLE	SQLPLUS@OSPREY	10.10.9.56	ORACLEXE	Alter table VendorMgt add ContractAmount integer	1

All reports can be accessed through My Dashboard selection.

Entity List

Main Entity: FULL SQL

Seq.	Entity	Attribute	Field Mode	Order-by	Sort Rank	Descend
1	FULL SQL	Timestamp	Value	Value	1	Value
2	Session	Session Start	Value	Value		Value
3	Client/Server	Client IP	Value	Value		Value
4	Client/Server	DB User Name	Value	Value		Value
5	Client/Server	OS User	Value	Value		Value
6	Client/Server	Source Program	Value	Value		Value
7	Client/Server	Server IP	Value	Value		Value
8	Client/Server	Service Name	Value	Value		Value
9	FULL SQL	Full Sql	Value	Value		Value

Additional mode: AND OR HAVING

Entity	Asp.	Attribute	Operator	Runtime Param.
WHERE	Client/Server	DB User Name	IN GROUP	Application DB User
AND	Client/Server	Source Program	NOT IN GROUP	Application Source Program

20. Demo configurations to monitor the following event?
Use of nonstandard tools (i.e. Excel/Access) to directly access DBMS

DATA ACTIVITY MONITORING / AUDITING / LOGGING

IBM

Data Breach Feeds

Data Breach Feeds

In today's environment there are multiple data breaches that occur every day. As an analyst you will want to keep track of what is going on in the world every day.

Data Breaches reports on current breaches from Malware to Data exposures

[DataBreaches.net](https://www.databreaches.net/)

Read the very latest data breach news: <https://www.databreaches.net/news/>

Search among many thousands of data breach cases by breach type, industry, etc.:
<https://www.databreaches.net/?s=case+studies>

Learn about data breach notification laws: <https://www.databreaches.net/state-breach-notification-laws/>

Bleeping Computer reports news on current breaches and threats

BleepingComputer.com

Think using a VPN will guaranty your security? This article from 2021 might have you thinking again.

<https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/>

IBM X-Force Exchange current, real-time world threat map

<https://exchange.xforce.ibmcloud.com/activity/map>

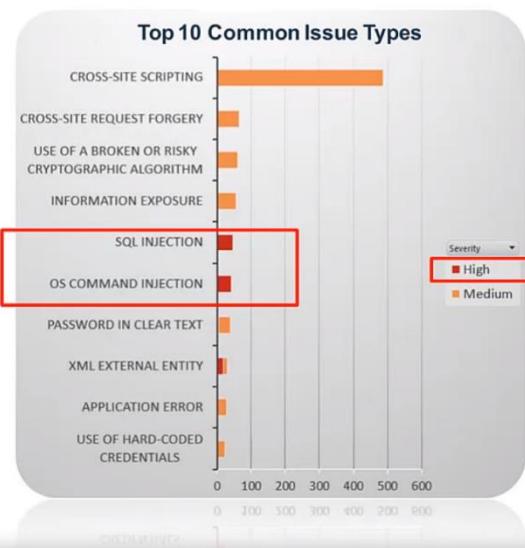
Click on any IP address at the top of the map and you will see details of the threat.

Week 4

Introduction to Injection Flaws

What are injection flaws?

- **Injection flaws** allow attackers to relay malicious code through the vulnerable application to another system (OS, Database server, LDAP server, etc.)
- They are extremely dangerous, and may allow full takeover of the vulnerable system
- Injection flaws appear internally & externally as a Top Issue



OWASP Top 10

- Injection vulnerabilities are consistently considered to be #1 on OWASP Top 10 list

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↗	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↗	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW, Comm.]

SANS Top 25

- Injection vulnerabilities are at the top of SANS Top 25 list

Rank	ID	Name
[1]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	CWE-306	Missing Authentication for Critical Function
[6]	CWE-862	Missing Authorization
[7]	CWE-798	Use of Hard-coded Credentials
[8]	CWE-311	Missing Encryption of Sensitive Data
[9]	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	CWE-807	Reliance on Untrusted Inputs in a Security Decision

Injection Vulnerabilities in the News

- Injection vulnerabilities made possible some of the most dramatic hacks in recent history
- Equifax OS Command Injection vulnerability leads to leak of data of millions of people in US and Canada*
<https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/>
- Personal data of 157K customers stolen from British telecom company TalkTalk through exploitation of SQL Injection*
<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/>



OS Command Injection Part 1

What is OS Command Injection?

- Abuse of vulnerable application functionality that causes execution of attacker-specified OS commands
- Applies to all operating systems – Linux, Windows, MacOS
- Made possible by lack of sufficient input sanitization, and by unsafe execution of OS commands

Example

- Consider a usecase where application allows user to delete log files:

auditlog8.log	
auditlog9.log	
auditlog10.log	

- The deletion command sent as a POST request that may look like this:

```
action=delete&file=auditlog9.log
```

- On the server the following code is executed (assume Java is the implementation language):

```
Runtime.getRuntime().exec("/bin/sh -c \" /bin/rm  
/var/app/logs/" +logFile+ "\"");
```

- Which translates to the following command:

```
/bin/sh -c "/bin/rm /var/app/logs/auditlog9.log"
```

Example

- Consider a usecase where application allows user to delete log files:

auditlog8.log	
auditlog9.log	
auditlog10.log	

- The deletion command sent as a POST request that may look like this:

```
action=delete&file=auditlog9.log
```

- On the server the following code is executed (assume Java is the implementation language):

```
Runtime.getRuntime().exec("/bin/sh -c \"bin/rm  
/var/app/logs/"+logFile+"\"");
```

- Which translates to the following command:

```
/bin/sh -c "/bin/rm /var/app/logs/auditlog9.log"
```

What is the Worst That Could Happen?

- Attacker can replace file to be deleted -BAD:

```
/bin/sh -c "/bin/rm /var/app/logs/../../../../lib/libc.so.6"
```

- Attacker can inject **arbitrary malicious OS command** – MUCHWORSE:

```
/bin/sh -c "/bin/rm /var/app/logs/x;rm -rf /"
```

- OS Command Injection can lead to:

- Full system takeover
- Denial of service
- Stolen sensitive information (passwords, crypto keys, sensitive personal info, business confidential data)
- Lateral movement on the network, launching pad for attacks on other systems
- Use of system for botnets or cryptomining

- This is as bad as it gets, a “GAME OVER” event

How To Prevent OS Command Injection?

- **Recommendation #1 – Do not execute OS commands 😊**
- Sometimes OS command execution is introduced as a quick fix, to let the command or group of commands do the heavy lifting
- This is dangerous, because insufficient input checks may let a destructive OS command slip in
- Resist the temptation to run OS commands and use built-in or 3rd party libraries instead:
 - Instead of `rm` use `java.nio.file.Files.deleteIfExists(file)`
 - Instead of `cp` use `java.nio.file.Files.copy(source, destination)`
 - ...and so on
- Use of library functions significantly reduces the *attack surface*

The screenshot shows a presentation slide with the following content:

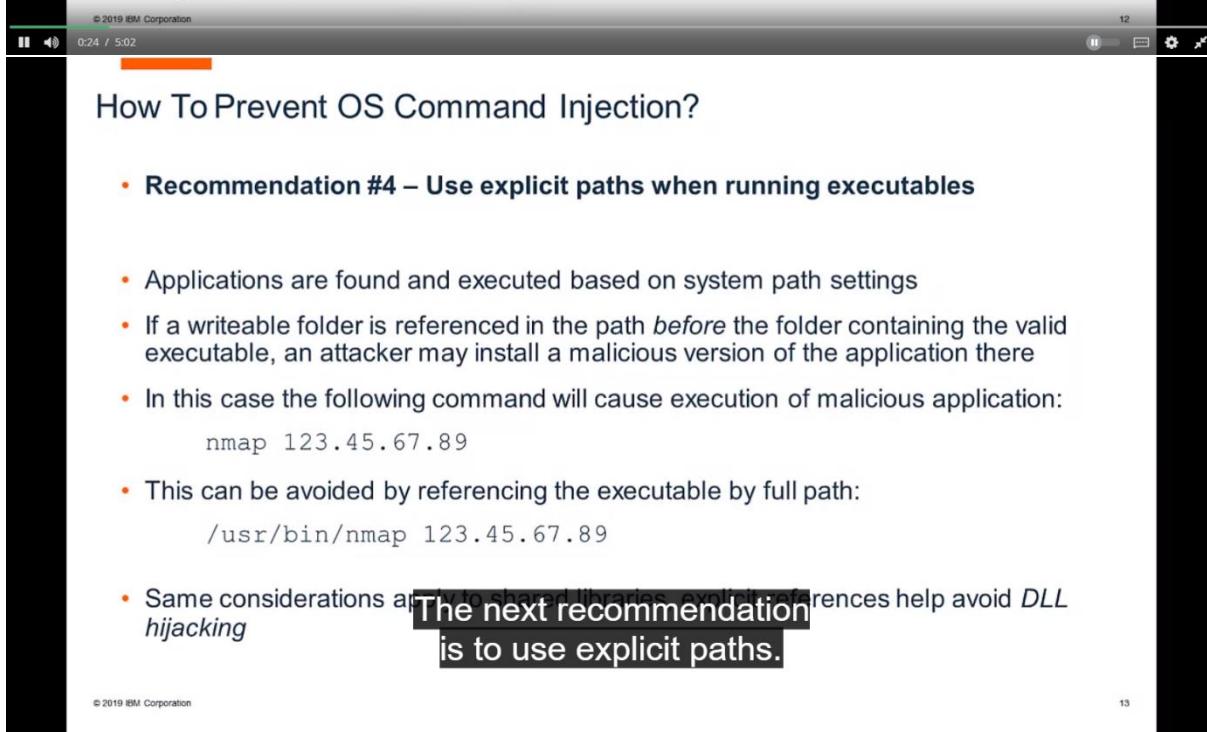
How To Prevent OS Command Injection?

- **Recommendation #2 – Run at the least possible privilege level**
- It is a good idea to run under a user account with the least required rights
- The more restricted the privilege level is the less damage can be done
- If an attacker is able to sneak in an OS command (e.g. `rm -rf /`) he can do much less damage when the application is running as `tomcat` user vs. running as `root` user
- This helps in case of many vulnerabilities, not just injection

OS Command Injection Part 2

How To Prevent OS Command Injection?

- **Recommendation #3 – Do not run commands through shell interpreters**
- When you run shell interpreters like `sh`, `bash`, `cmd.exe`, `powershell.exe` it is much easier to inject commands
- The following command will allow injection of an extra `rm`:
`/bin/sh -c "/bin/rm /var/app/logs/x;rm -rf /"`
- ...but in this case injection will not work, the whole command will fail:
`/bin/rm /var/app/logs/x;rm -rf /`
- Running a single command directly executes just that command
- Note that it is still possible to influence behavior of a single command (e.g. for `nmap` the part in red, when injected, could overwrite a vital system file):
`/usr/bin/nmap 1.2.3.4 -oX /lib/libc.so.6`
- Also note that the parameters that you pass to a script may still result in command injection:
`processFile.sh "x;rm -rf /"`



The screenshot shows a video player interface with a presentation slide. The slide has a black background with white text. At the top, there is a horizontal bar with orange and grey segments. Below the bar, the title 'How To Prevent OS Command Injection?' is displayed. A list of recommendations follows, with some text highlighted in red. A large callout box at the bottom right contains a bold statement. The video player interface includes a progress bar, a timestamp (0:24 / 5:02), and a copyright notice ('© 2019 IBM Corporation').

How To Prevent OS Command Injection?

- **Recommendation #4 – Use explicit paths when running executables**
- Applications are found and executed based on system path settings
- If a writeable folder is referenced in the path *before* the folder containing the valid executable, an attacker may install a malicious version of the application there
- In this case the following command will cause execution of malicious application:
`nmap 123.45.67.89`
- This can be avoided by referencing the executable by full path:
`/usr/bin/nmap 123.45.67.89`
- Same considerations apply to shared libraries. Explicit references help avoid *DLL hijacking*

**The next recommendation
is to use explicit paths.**

© 2019 IBM Corporation

OS Command Injection Part 3

How To Prevent OS Command Injection?

- **Recommendation #5 – Use safer functions when running system commands**
- If available, use functionality that helps prevent command injection
- For example, the following function call is vulnerable to new parameter injection (one could include more parameters, separated by spaces, in ipAddress):

```
Runtime.getRuntime().exec("/usr/bin/nmap " + ipAddress);
```
- ... but this call is not vulnerable:

```
Runtime.getRuntime().exec(new String[] {"./usr/bin/nmap", ipAddress});
```

© 2019 IBM Corporation
0:44 / 7:32

How To Prevent OS Command Injection?

- **Recommendation #6 – If possible, do not let user input reach command execution unchanged**
- Modifying user input, or replacing user-specified values with others (e.g. using translation tables) helps protect against injection
- For example, instead of allowing user to specify file to delete, let her select a unique file ID:

```
action=delete&file=457
```
- When submitted, translate that ID into a real file name:

```
realName = getRealFileName(fileID);  
Runtime.getRuntime().exec(new String[]{"./bin/rm", "/var/app/logs/" + realName});
```

© 2019 IBM Corporation
2:03 / 7:32

How To Prevent OS Command Injection?

- **Recommendation #7 – Sanitize user input with strict whitelists (not blacklists!)**
- In our products we often see blacklists used for parameter sanitization; some of them are incorrect
- It is **hard** to build a successful blacklist – hackers are very inventive ([some examples](#))!
- Suppose we want to blacklist characters used in a file name for command `rm /var/app/logs/file`

Mitigation	Evasion
Blacklist ; &	<code>/bin/rm /var/app/logs/x`rm -rf `/</code>
Blacklist ; & `	<code>/bin/rm /var/app/logs/x\$(rm -rf /)</code>
Blacklist spaces	<code>/bin/rm /var/app/logs/x;rm\${IFS:0:1}-rf\${IFS:0:1}/</code>
Enclose value in double quotes, escape them in value	<code>/bin/rm "/var/app/logs/x\\\";rm -rf /;echo \\"</code>

- A more robust and simpler solution is to whitelist file name as **[A-Za-z0-9.]+**

Key Takeaways

- **DO NOT** use OS commands
 - If possible, use built in or secure/approved 3rd party libraries instead
- **DO** run your code with least possible privilege
- **DO NOT** run commands with shell interpreters
 - Instead, run commands directly
- **DO** use explicit paths when running applications and using shared libraries
- **DO** use safe library functions when running OS commands
- **DO NOT** let user input reach OS command unchanged
 - If possible, replace user input with generated IDs
- **DO** sanitize all user input
 - ONLY use whitelists for sanitization; blacklists are unsafe

SQL Injection Part 1

What is SQL Injection?

- Abuse of vulnerable application functionality that causes execution of attacker-specified SQL queries
- Is possible in any SQL database
- Made possible by lack of sufficient input sanitization

Example

- Suppose our application has a login dialog:



- On the back end the code may be as follows:

```
stmt.executeQuery("SELECT * FROM users WHERE user='"+user+"' AND  
pass='"+pass+"'")
```

- With regular input the query would be as follows, selecting a record only if the match is found:

```
SELECT * FROM users WHERE user='bob' AND pass='secret'
```

- In case of malicious input hacker can login without valid credentials:

```
SELECT * FROM users WHERE user=' OR 1=1;--' AND pass=''
```

Dangers of SQL Injection

Appuyez sur Échap pour quitter le mode plein écran.

- Consequences of SQL injection:

- Bypassing of authentication mechanisms
- Data exfiltration
- Execution of OS commands, e.g. in Postgres:

```
COPY (SELECT 1) TO PROGRAM 'rm -rf /'
```

- Vandalism / DoS (e.g. DROP TABLE sales) – injected statements may sometimes be chained:

```
SELECT * FROM users WHERE user='';DROP TABLE sales;--' AND pass=''
```

Common Types of SQL injection

- Error-based

- Attacker may tailor his actions based on the database errors the application displays

- UNION-based

- May be used for data exfiltration, for example:

```
SELECT name, text FROM log WHERE date='2018-04-01' UNION SELECT user,  
password FROM users --'
```

- Blind injection

- The query may not return the data directly, but it can be inferred by executing many queries whose behavior presents one of two outcomes
- Can be *Boolean-based* (one of two possible responses) and *Time-based* (immediate vs delayed execution)
- For example the following expression, when injected, indicates if the first letter of password is 'a':

```
IF(password LIKE 'a%', sleep(10), 'false')
```

- Out of Band

- Data exfiltration is done through a separate channel (e.g. by sending an HTTP request)

SQL Injection Part 2

How to Prevent SQL Injection?

- **Recommendation #1 – Use prepared statements**
- Most SQL injection happens because queries are pieced together as text
- Use of prepared statements separates the query structure from query parameters.
- Instead of this pattern:

```
stmt.executeQuery("SELECT * FROM users WHERE user='"+user+"' AND  
pass='"+pass+"'")
```
- ...use this:

```
PreparedStatement ps = conn.prepareStatement("SELECT * FROM users  
WHERE user = ? AND pass = ?"); ps.setString(1, user);  
ps.setString(2, pass);
```
- SQL injection risk is now mitigated
- Note that prepared statements must be used properly, we occasionally see bad examples like this:

```
conn.prepareStatement("SELECT * FROM users WHERE user = ? AND pass = ?  
ORDER BY "+column);
```

How to Prevent SQL Injection?

- **Recommendation #2 – Sanitize user input**
- Just like for OS command injection, input sanitization is important
- Only restrictive whitelists should be used, not blacklists
- Where appropriate, do not allow user input to reach the database, and instead use mapping tables to translate it

How to Prevent SQL Injection?

- **Recommendation #3 – Do not expose native database errors to the user**
- Application errors should not expose internal information to the user
- Details belong in an internal log file
- Exposed details can be abused for tailoring SQL injection commands
- For example, the following error message exposes both the internal query structure and the database type, helping attackers in their efforts:

If you have an error in your SQL syntax, check the manual that corresponds to your MySQL server version for the right syntax to use near "x" GROUP BY username ORDER BY username ASC' at line 1

The screenshot shows a video player interface. At the top, there is a navigation bar with icons for back, forward, search, and settings. The main content area displays the title 'How to Prevent SQL Injection?' followed by a bulleted list of recommendations. At the bottom, there is another navigation bar with similar icons.

© 2019 IBM Corporation
2:47 / 6:07
25

How to Prevent SQL Injection?

- **Recommendation #4 – Limit database user permissions**
- When user queries are executed under a restricted user less damage is possible if SQL injection happens
- Consider using user with read-only permissions when database updates are not required, or use different users for different operations

© 2019 IBM Corporation
3:58 / 6:07
26

How to Prevent SQL Injection?

- **Recommendation #5 – Use stored procedures**
- Use of stored procedures mitigates the risk by moving SQL queries into the database engine
- Fewer SQL queries will be under direct control of the application, reducing likelihood of abuse

How to Prevent SQL Injection?

- **Recommendation #6 – Use ORM libraries**
- Object-relational mapping (ORM) libraries help mitigate SQL injection
 - Example: Java Persistence API (JPA) implementations like Hibernate
- ORM helps reduce or eliminate the need for direct SQL composition
- However, if ORM is used improperly SQL Injection may still be possible:

```
Query hqlQuery = session.createQuery("SELECT * FROM users WHERE user='"+user+"'AND pass='"+pass+"'")
```

Key Takeaways

- DO use prepared statements (and do it correctly)
- DO sanitize user input
- DO NOT expose native database errors to the user
- DO limit database user permissions
- DO use stored procedures
- DO use ORM libraries correctly

Other Types of Injection

Other Types of Injection

© 2019 IBM Corporation

30



0:21 / 4:49

Other types of Injection

- Injection flaws exist in many other technologies”

NoSQL Injection

- In MongoDB `$where` query parameter is interpreted as JavaScript
- Suppose we take an expression parameter as input:

```
$where: "$expression"
```

- In simple cases it is harmless:

```
$where: "this.userType==3"
```

- However an attacker can perform a DoS attack:

```
$where: "d = new Date; do {c = new Date;} while (c - d < 100000;"
```

© 2019 IBM Corporation

31

Other types of Injection

XPath Injection

- Suppose we use XPath expressions to select user on login:
`//Employee[UserName/text()=' + Request ("Username") + '' AND Password/text()=' + Request ("Password") + '']`
- In the benign case it will select only the user whose name and password match:
`//Employee[UserName/text()='bob' AND Password/text()='secret']`
- In the malicious case it will select any user:
`//Employee[UserName/text()=' or 1=1 or '1='1 And Password/text()=']`

Other types of Injection

LDAP Injection

- LDAP is a common mechanism for managing user identity information. The following expression will find the user with the specified username and password.
`find("(&(cn=" + user +") (password=" + pass +"))")`
- In the regular case the LDAP expression will work only if the username and password match:
`find("(&(cn=bob) (password=secret))")`
- Malicious users may tweak the username to foce expression to find any user:
`find("(&(cn=*) (cn=*)) (|cn=*) (password=any)")`

Other types of Injection

- Injection flaws also exist in Templating engines
- ...and many other technologies
- Recommendations for avoiding all of them are similar to what is proposed for OS and SQL injection

© 2019 IBM Corporation

34

Overall Recommendations for Preventing Injection

- **DO** use functionality with reduced scope (e.g. specific library functions instead of arbitrary OS command execution)
- **DO** execute with least privilege
- **DO** use safe functionality that prevents injection
- **DO NOT** let user input reach critical resource unchanged (as much as possible)
- **DO** sanitize user input with strict whitelists (not blacklists!)

© 2019 IBM Corporation

35

Additional Resources

Additional Resources

This course is the beginning of your journey. In Cybersecurity there is no way to know everything about Databases or Networking and their vulnerabilities. You need to know where to find additional information and detailed steps to safeguard data. Here are some additional resources that are important to be aware of and explore as you are developing your Cybersecurity skills.

OWASP Cheat Sheets

Injection Flaws https://owasp.org/www-community/Injection_Flaws

OS Command Injection https://owasp.org/www-community/attacks/Command_Injection

SQL Injection https://owasp.org/www-community/attacks/SQL_Injection

LDAP Injection

https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html

pentestmonkey

MSSQL injection cheat sheet: <http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet>

Oracle injection cheat sheet: <http://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet>

DB2 injection cheat sheet: <http://pentestmonkey.net/cheat-sheet/sql-injection/db2-sql-injection-cheat-sheet>

Postgres injection cheat sheet: <http://pentestmonkey.net/cheat-sheet/sql-injection/postgres-sql-injection-cheat-sheet>

MySQL injection cheat sheet: <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Database Hacker's Handbook: Defending Database Servers

You can find this book at different retailers such as Amazon.com.

Software Vulnerabilities

A *vulnerability* is a potential weakness that someone can exploit in a system, network, or application. When targeting applications, attackers commonly exploit the following vulnerabilities:

- Broken access control or authentication
- Unencrypted data
- Use of default passwords or configurations
- Unpatched flaws
- Unused pages

By exploiting these vulnerabilities, attackers can circumvent an application's security to steal protected information, damage systems, or disable services.

Common Attacks

The following list describes some of the most common attacks on applications:

- *SQL injection* involves placing malicious code into a Structured Query Language (SQL) statement through a web page. The attacker typically uses a user input request, such as a username, to enter an SQL statement that will run on your database.
- *Cross-site scripting (XSS)* is an injection in which the attacker uses a web application to send a browser-side script to another user. Because the user's browser recognizes the script as coming from a trusted site, the script runs.

- *File inclusion* targets poorly written web applications that allow users to upload files without appropriate validation. The attacker tricks the web application into showing or running files that should not be publicly visible or available.
- *Buffer overflow* occurs when the amount of data sent exceeds what the memory buffer can handle. If the application is not properly secured, a knowledgeable attacker can use a buffer overflow attack to crash the system. The attacker could even overwrite existing executable code with their own to take control of the system.

Prevention Measures

To defend against common attacks, developers should build security into each step of the *software development life cycle (SDLC)*. They should consider and plan for potential security threats early on and test, scan, audit, and review code throughout development. Plus, various tools can automate security checks through nearly every stage of development, freeing developers to focus on other tasks.

Developers should also limit the number of applications and pages the product has. Extra pages, documentation, and features can increase the attack surface for attackers to target.

Security monitoring and logging practices help teams identify login, validation, and access control errors before a potential attacker can do damage. Personnel can respond quickly to patch the application if needed.

Another critical defense against common attacks is vulnerability scans. These scans identify vulnerabilities in the application and from libraries (collections of reusable code) on which the application depends. A standard type of vulnerability scan is a penetration test. A *penetration test (pentest)* simulates real hacking techniques to find application or system vulnerabilities that attackers can exploit. Organizations should perform pentesting regularly. Some useful pentesting tools for identifying web applications include OWASP ZAP, Comodo, and Vega.