

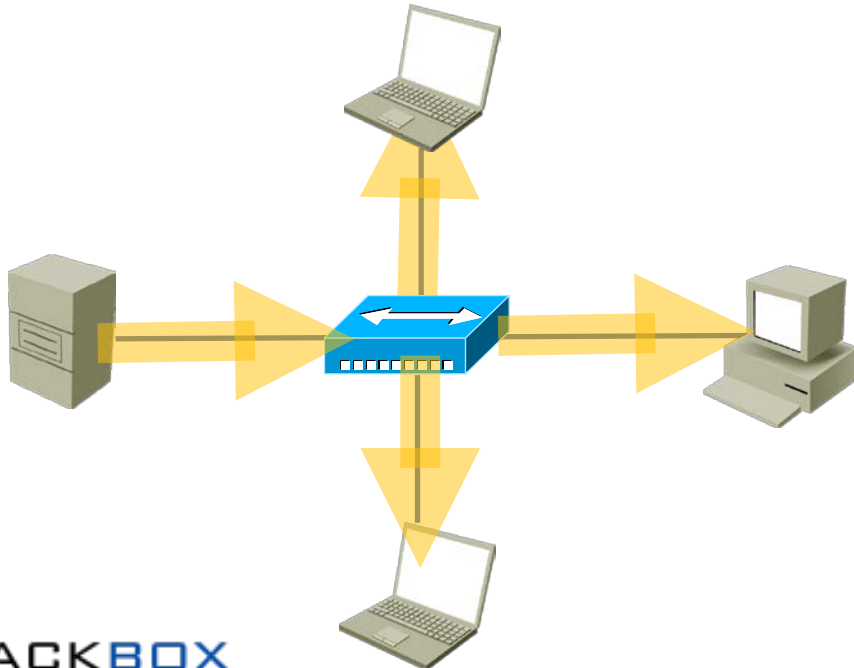
Hubs vs Switches



- Hubs were Layer 1 devices, switches are Layer 2 devices
- When traffic comes in to a hub it is flooded out all other ports
- Switches listen to source MAC addresses and learn which MAC addresses are connected on which port
- When traffic comes in to the switch with a known destination MAC address, it sends it out only the relevant port
- This provides better performance and security

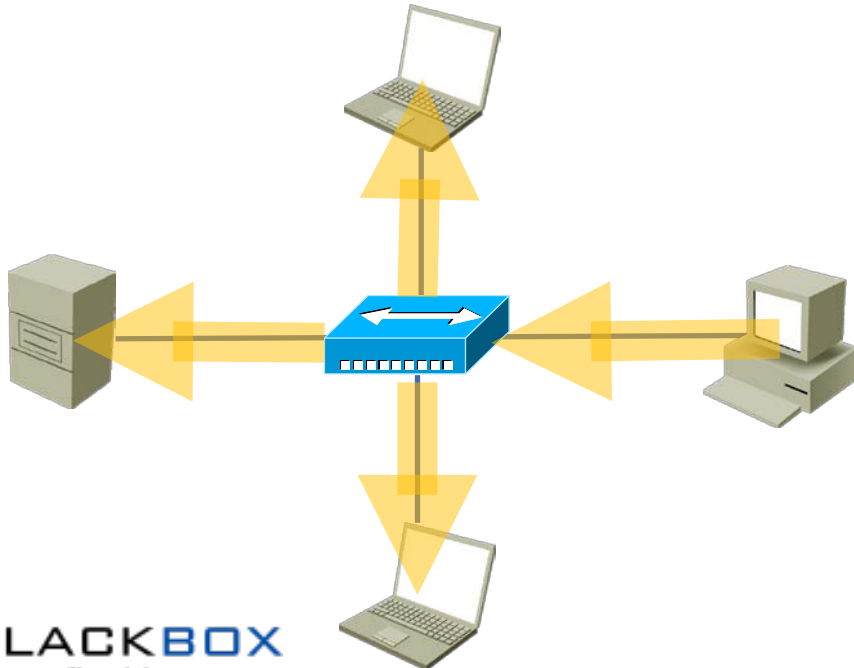
Traffic Monitoring on Hubs

- To monitor the traffic going to and from a host connected to a hub, you can simply plug a device running packet sniffing software (such as Wireshark) in any port on the hub network
- This is useful for doing deep troubleshooting work



Traffic Monitoring on Hubs

- To monitor the traffic going to and from a host connected to a hub, you can simply plug a device running packet sniffing software (such as Wireshark) in any port on the hub network
- This is useful for doing deep troubleshooting work



Wireshark



Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr == 192.168.1.6` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19511	995.233558000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19512	995.233597000	192.168.1.8	192.168.1.6	ICMP	Redirect (Redirect for host)
19513	995.233631000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19514	995.248689000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19515	995.248710000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19516	995.260447000	192.168.1.6	82.192.95.92	TCP	55552 > http [FIN, ACK] Seq=200 Ack=1154 Win=16368 Len=0
19520	995.312985000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521	995.313009000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522	995.314343000	192.168.1.6	82.192.95.92	TCP	55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523	995.314363000	192.168.1.6	82.192.95.92	TCP	[TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524	995.324651000	82.192.95.92	192.168.1.6	TCP	http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525	995.324668000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527	995.325988000	192.168.1.6	82.192.95.92	TCP	[TCP segment of a reassembled PDU]
19528	995.326010000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529	995.326263000	192.168.1.6	82.192.95.92	HTTP	POST /cgi-bin/iavs4stats.cgi HTTP/1.1 (iavs4/stats)
19530	995.326278000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
19531	995.375611000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532	995.375625000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533	995.380658000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534	995.380678000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535	995.382891000	82.192.95.92	192.168.1.6	HTTP	HTTP/1.1 204 No Content
19536	995.382911000	82.192.95.92	192.168.1.6	HTTP	[TCP Retransmission] HTTP/1.1 204 No Content
19539	995.505191000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540	995.505232000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550	996.308269000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551	996.308324000	192.168.1.8	192.168.1.6	ICMP	Redirect (Redirect for host)
19552	996.308363000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)

Ethernet II, Src: HonHaiPr_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewav_43:90:de (00:15:af:43:90:de)

Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)

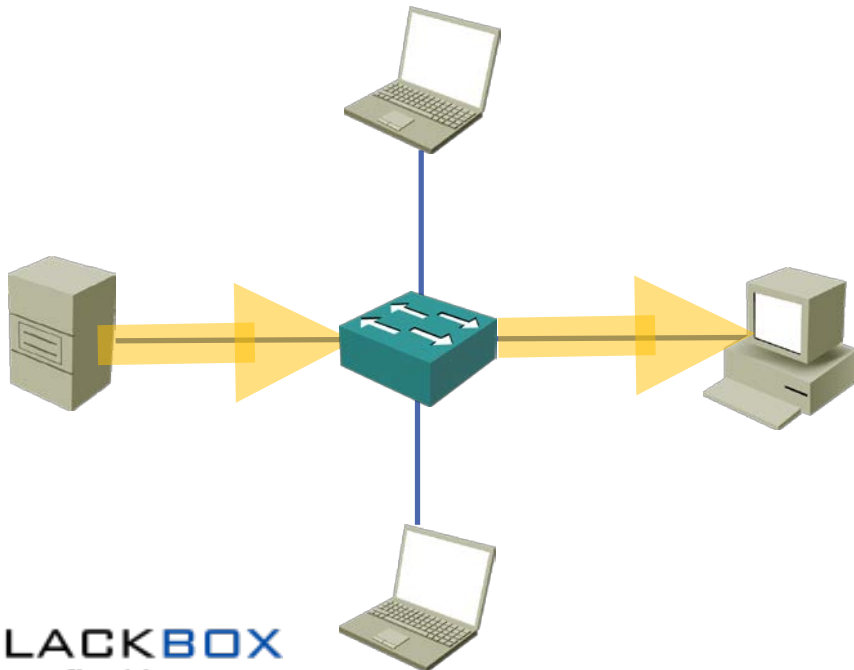
Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23

```
0000  00 15 af 43 90 de c0 cb 38 26 b5 30 08 00 45 00  ...C.... 8&0..E.
0010  00 3f 57 57 40 00 ef 06 26 fa 44 7e 07 3b c0 a8  .7Ww@... &.D-;..
0020  01 06 4b 07 d8 68 00 00 00 00 0f 49 3f 88 50 14  ..K..h... ..I7.P.
0030  00 00 5a f6 00 00 47 6f 20 61 77 61 79 2c 20 77  ..Z...Go away, w
0040  65 27 72 65 20 6e 6f 74 20 68 6f 6d 65         e're not home
```

eth1: <live capture in progress> File: Packets: 19552 Displayed: 5155 Marked: 0 Profile: Default

Traffic Monitoring on Switches

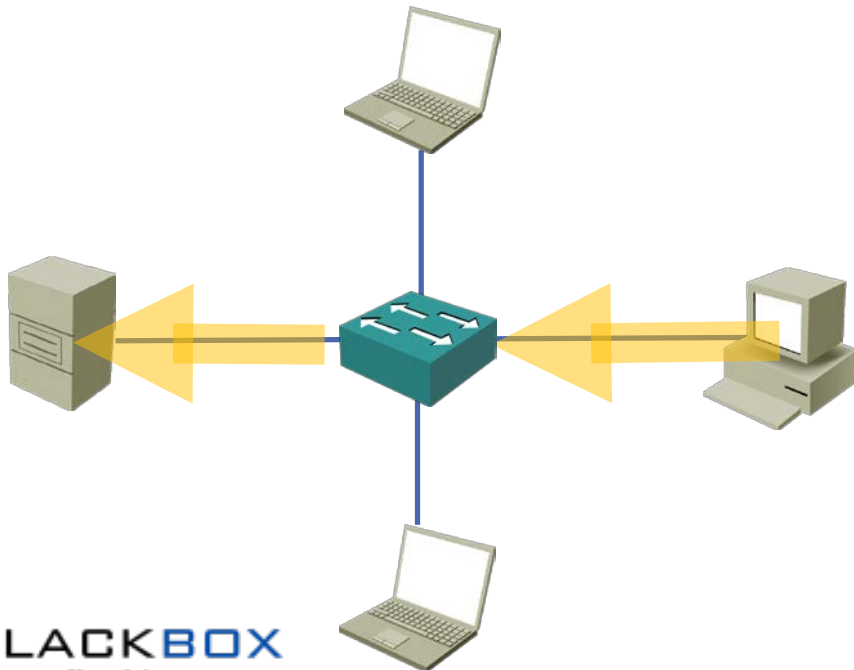
- You can't just plug a device running packet sniffing software (such as Wireshark) in any port on a switch to monitor traffic



Traffic Monitoring on Switches



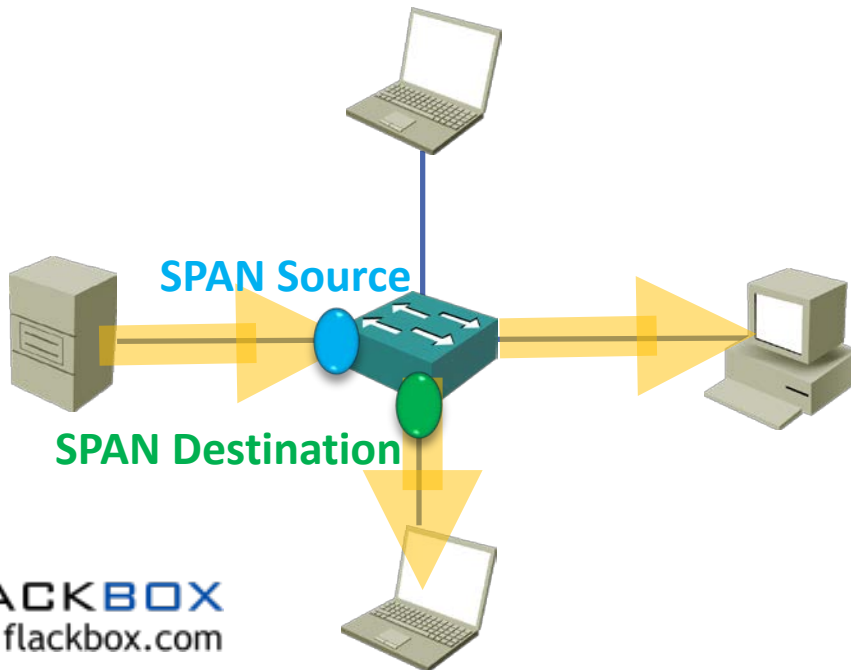
- You can't just plug a device running packet sniffing software (such as Wireshark) in any port on a switch to monitor traffic



SPAN Switched Port Analyzer



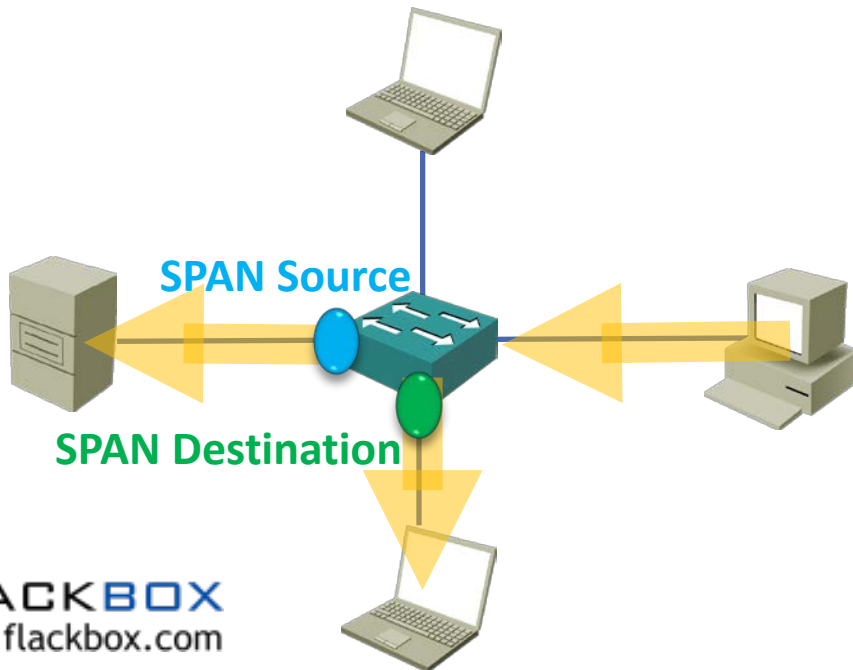
- An administrator can configure SPAN on a switch to send a copy of the traffic sent and/or received on a source to another port
- The source can be a physical port, an EtherChannel, or an entire VLAN
- The destination is a physical port



SPAN Switched Port Analyzer



- An administrator can configure SPAN on a switch to send a copy of the traffic sent and/or received on a source to another port
- The source can be a physical port, an EtherChannel, or an entire VLAN
- The destination is a physical port



SPAN, RSPAN and ERSPAN



- With SPAN the source and destination port must be on the same switch
- With RSPAN (Remote SPAN) the source and destination ports can be on different switches in the same Layer 2 network
- With ERSPAN (Encapsulated RSPAN) the source and destination ports can be on different switches across a Layer 3 network

SPAN Configuration

```
SW1(config)#monitor session 1 source interface FastEthernet0/1  
SW1(config)#monitor session 1 destination interface FastEthernet0/2
```

```
SW1#show monitor
```

```
Session 1
```

```
-----
```

```
Type : Local Session
```

```
Description : -
```

```
Source Ports :
```

```
Both : Fa0/1
```

```
Destination Ports : Fa0/2
```

```
Encapsulation : Native
```

```
Ingress : Disabled
```