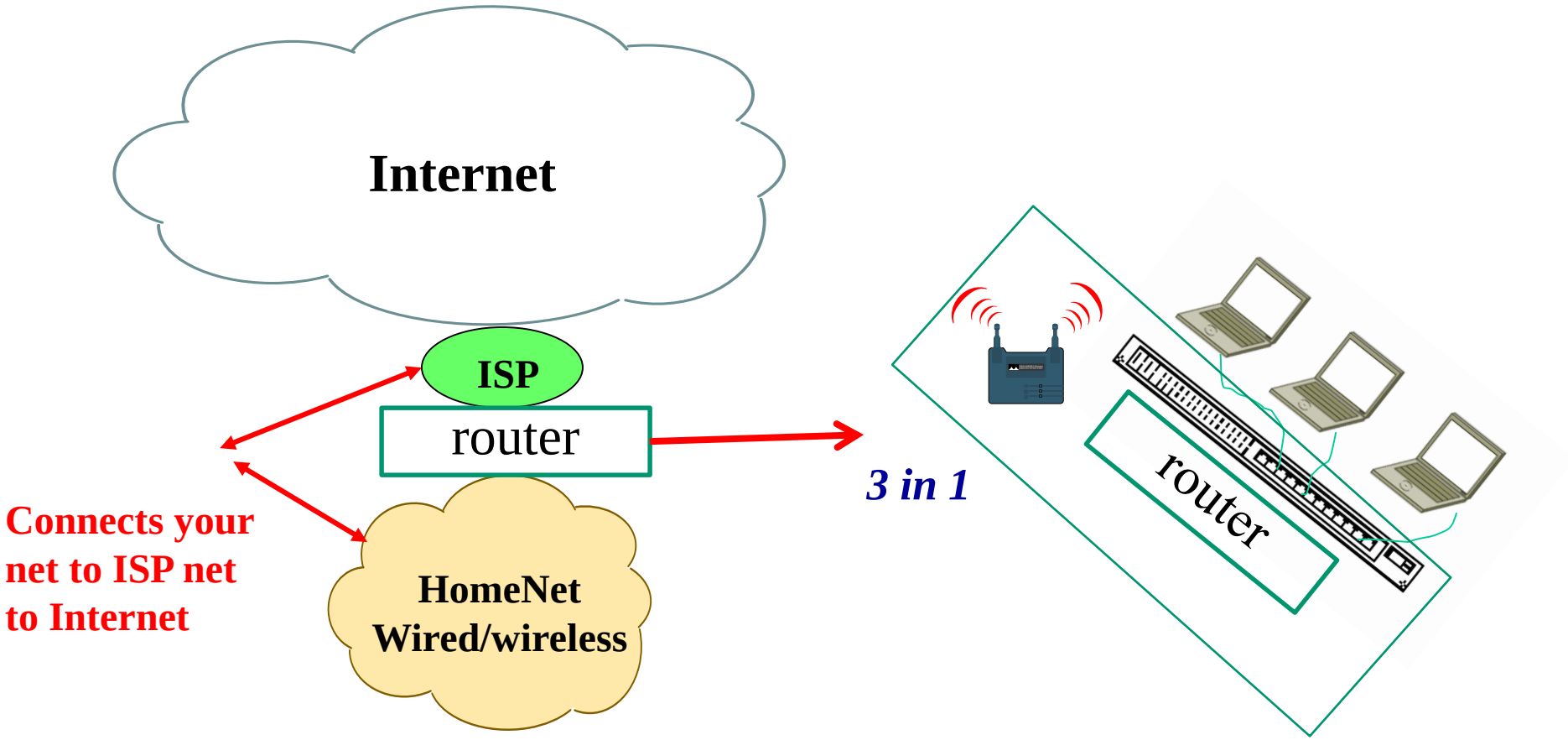
Network Security Summary

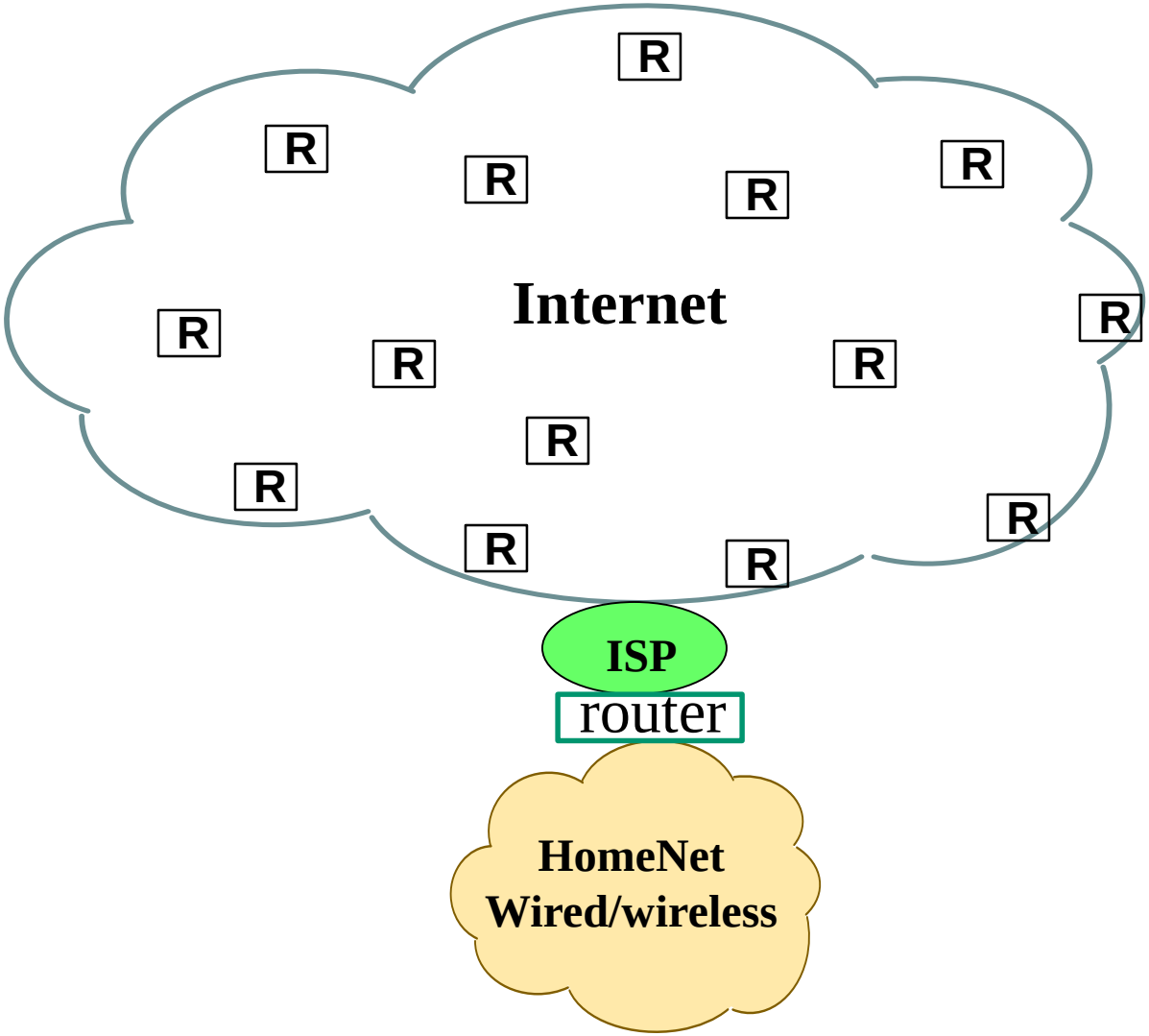
UW i310– 2016

Typical Home – Small Office Scenario



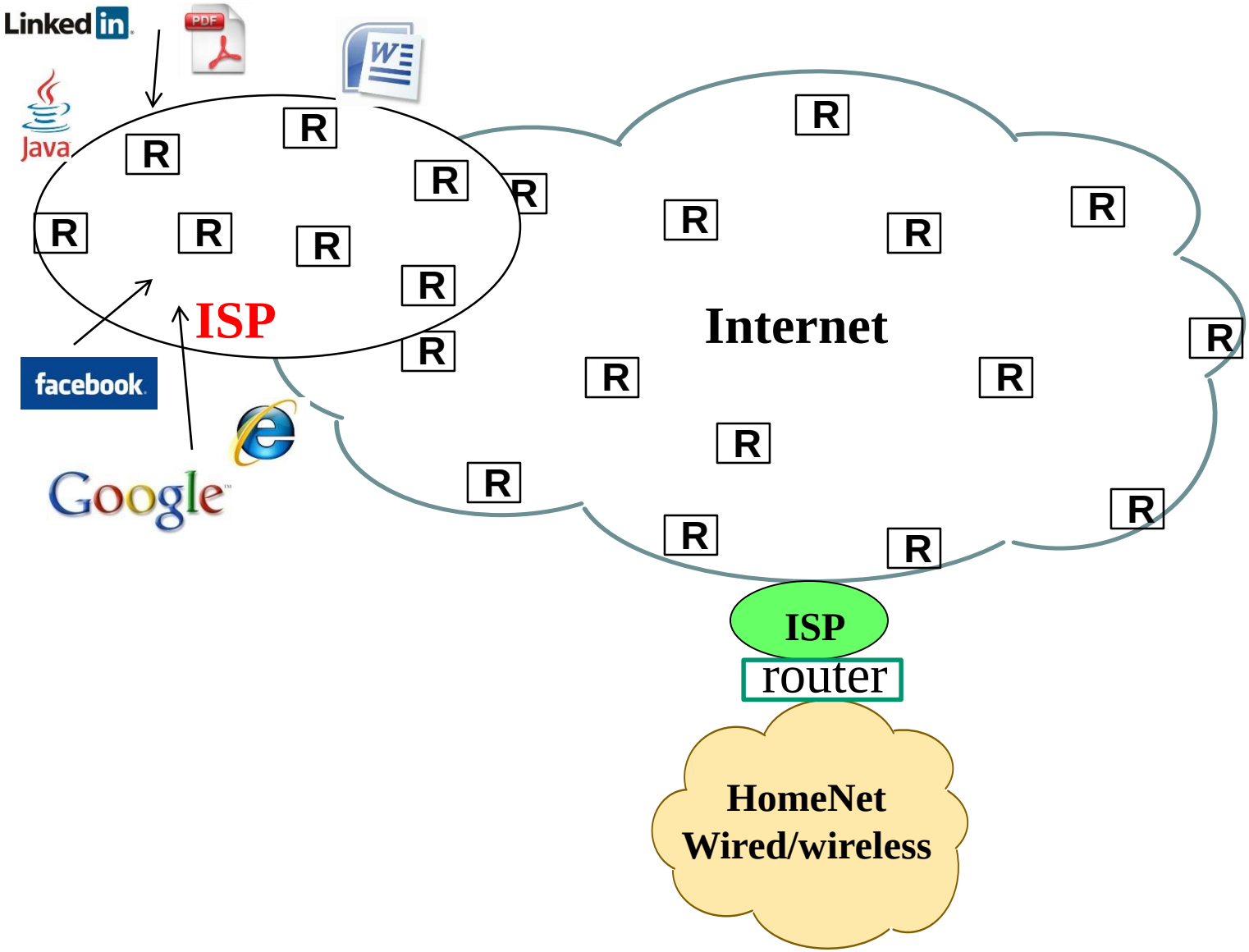
What is job of router - Interconnect Networks (at TCP/IP Net Layer)

Routers – Masters of Internet Domain

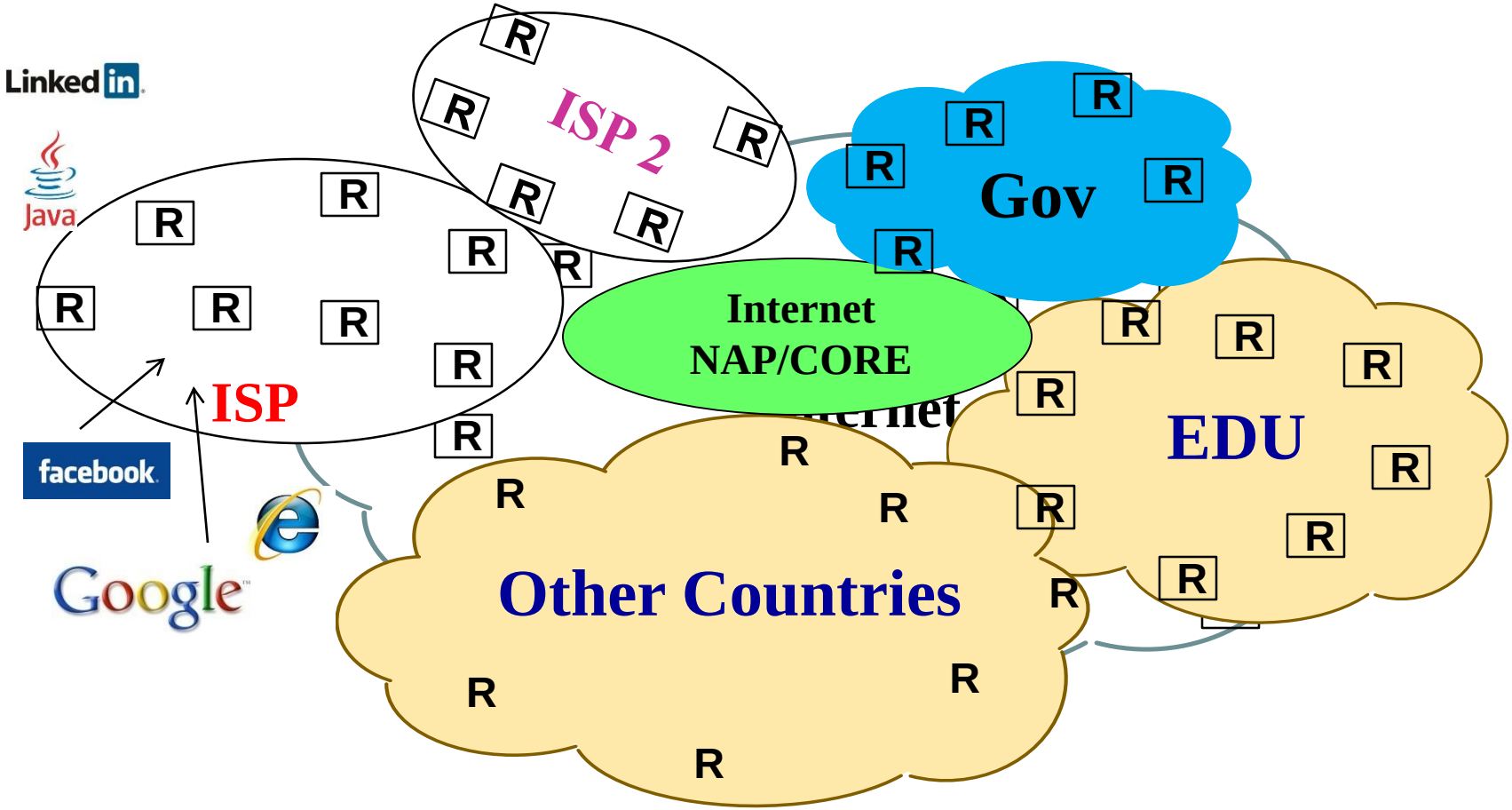


Routers – Masters of Internet Domain

What is job of a router - Interconnect Networks (at TCP/IP Net Layer)

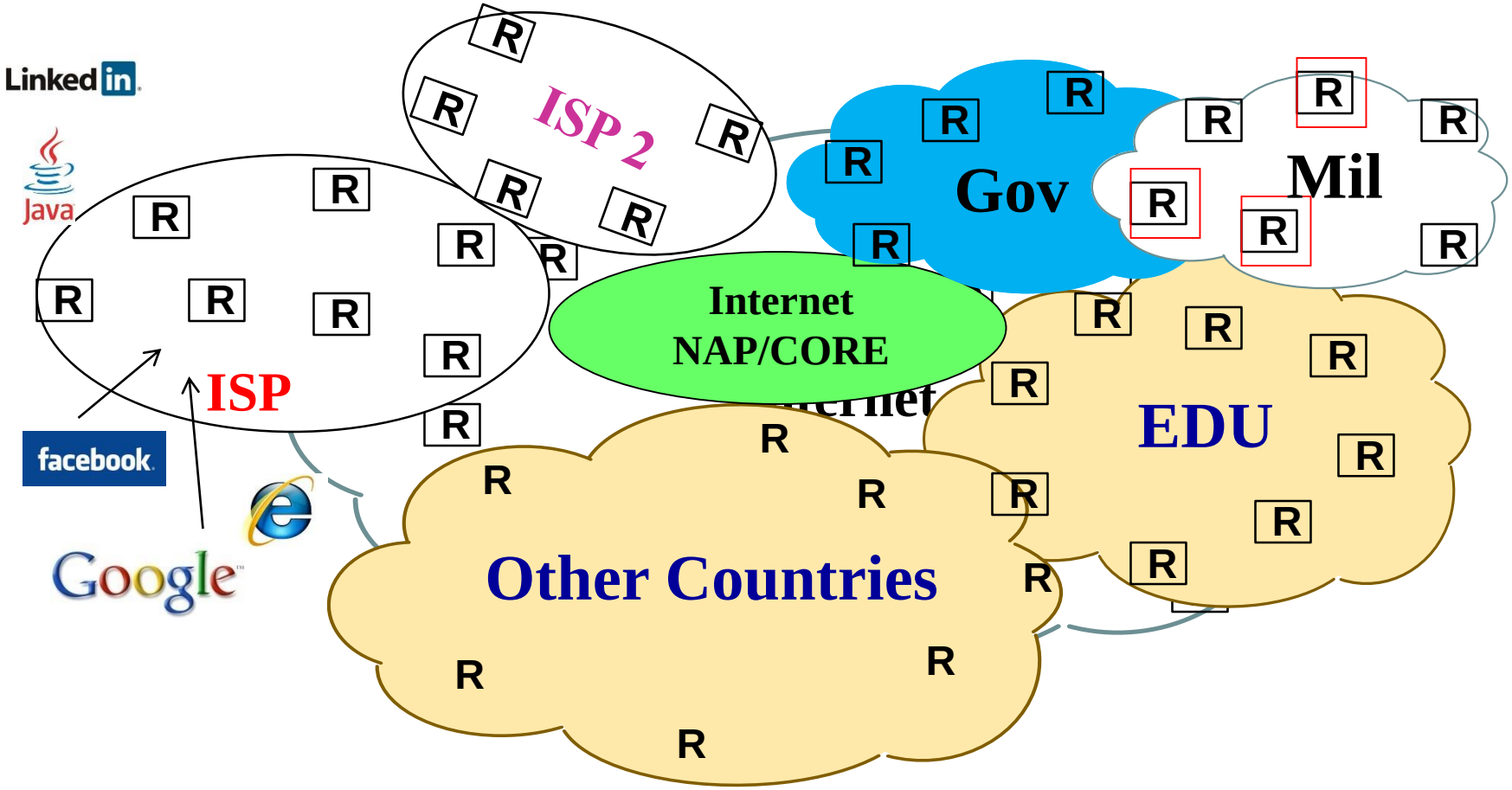


Routers – Greater Internet Domain



What is job of a router - Interconnect Networks (at TCP/IP Net Layer)

What Enables the Net Capability ? ?



TCP/IP Network drivers/apps (voice,video,music,www/browser)

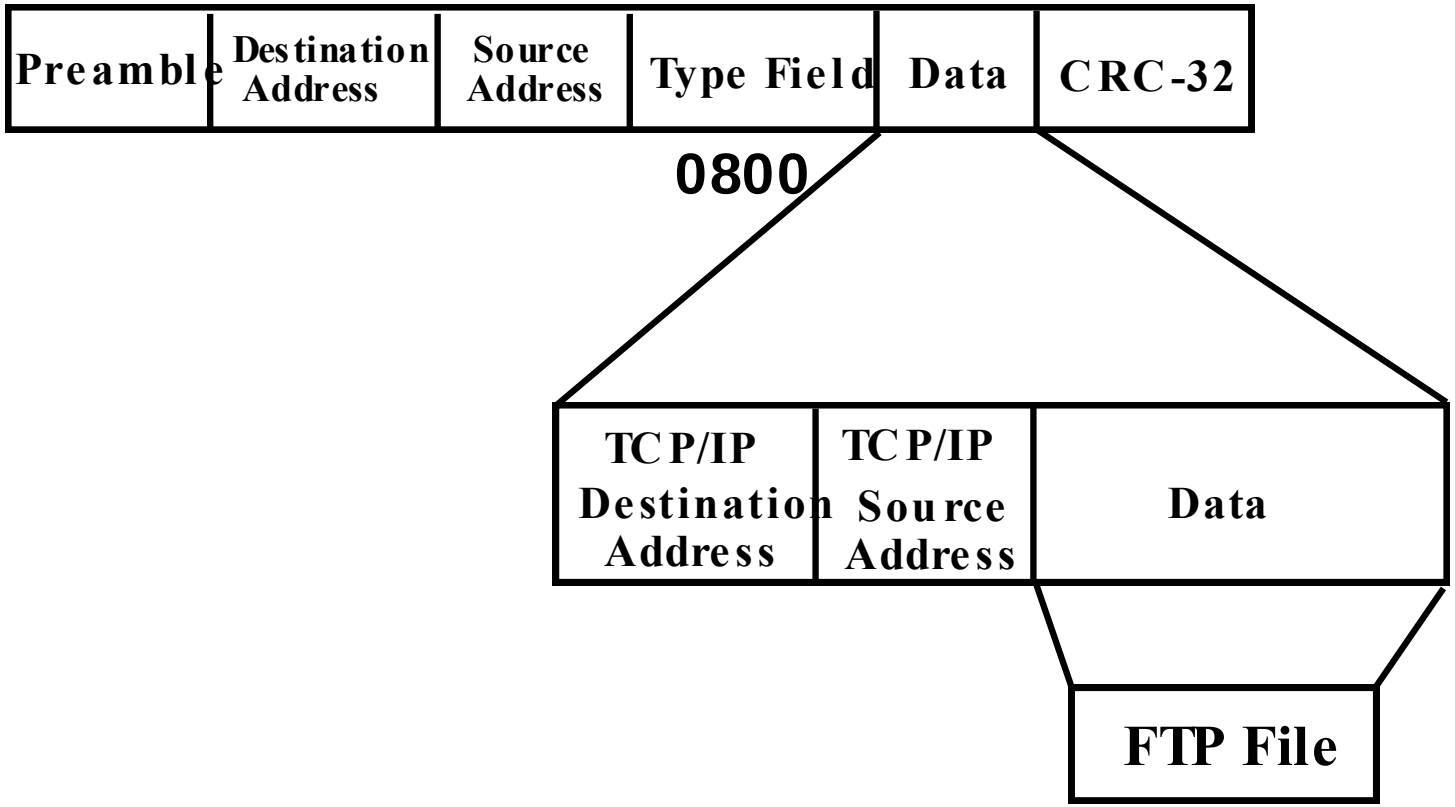
What is job of a router - Interconnect Networks (at TCP/IP Net Layer)

Forward TCP/IP packets between networks

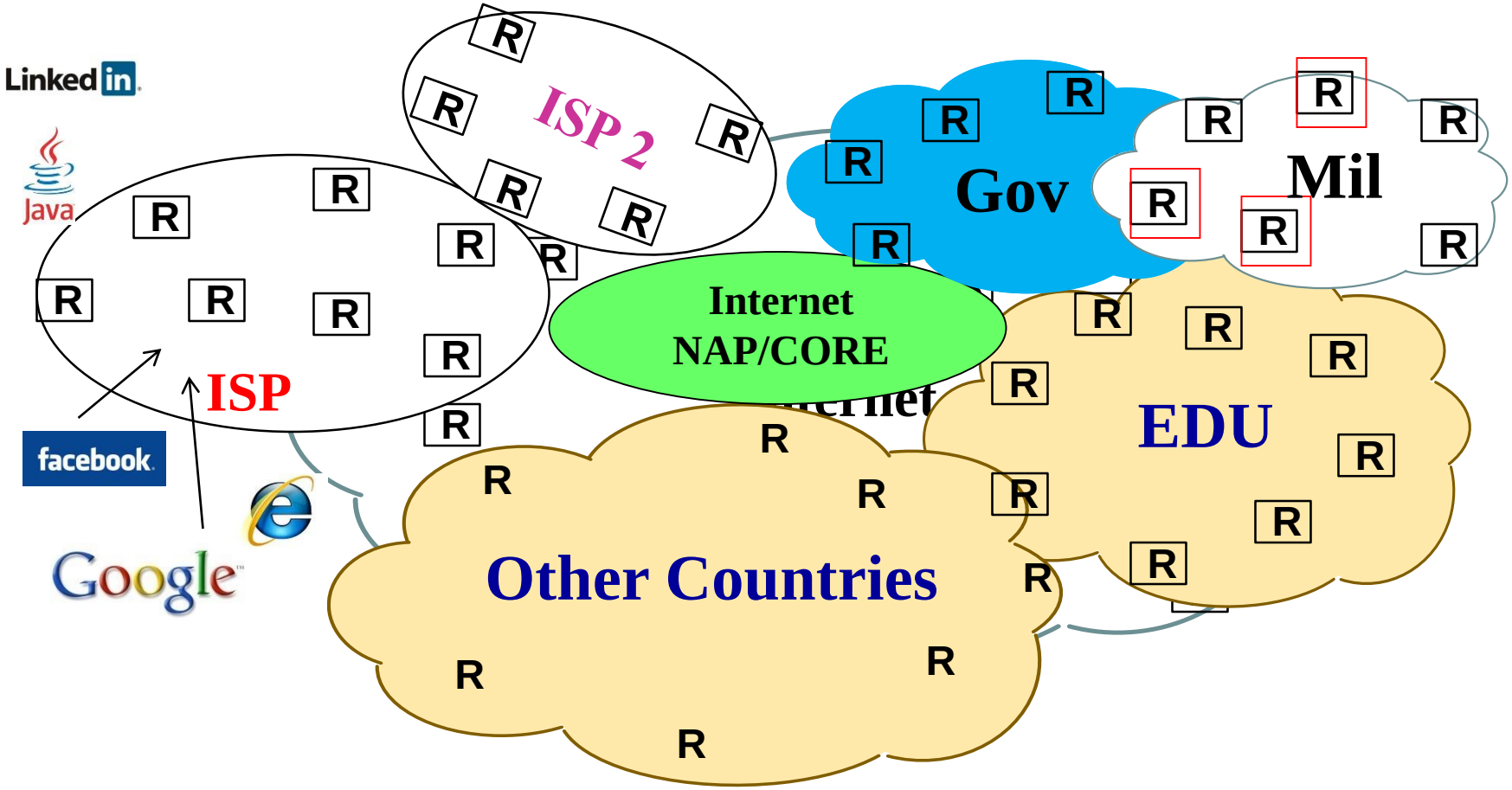
PDU (Protocol Data Unit)

An Ethernet Packet may contain about anything in any format. Ethernet does not interpret the data section, except to look at the protocol type field or length. The data section must be a minimum length of 46 bytes, even if there is only 1 byte to send, and may be as large as 1500 bytes. Typically the data section would contain the protocol packet used by upper layer software such as TCP/IP, XNS, IPX, AppleTalk, SNA,MOP, LAT....)

The following diagram illustrates a FTP (file transfer) request from an end user in a TCP/IP packet inside an Ethernet frame.



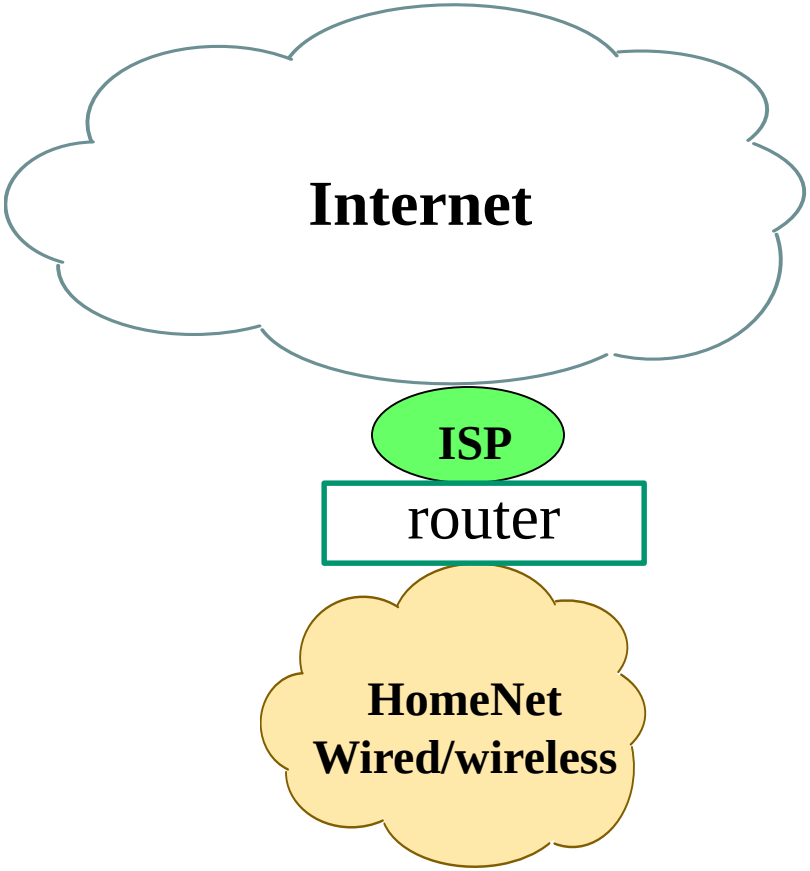
Network Centric



TCP/IP protocols (HTTP, SNMP, SMTP, DNS)

Filter, Inspect, Monitor, Collect

Typical Home – Small Office Scenario

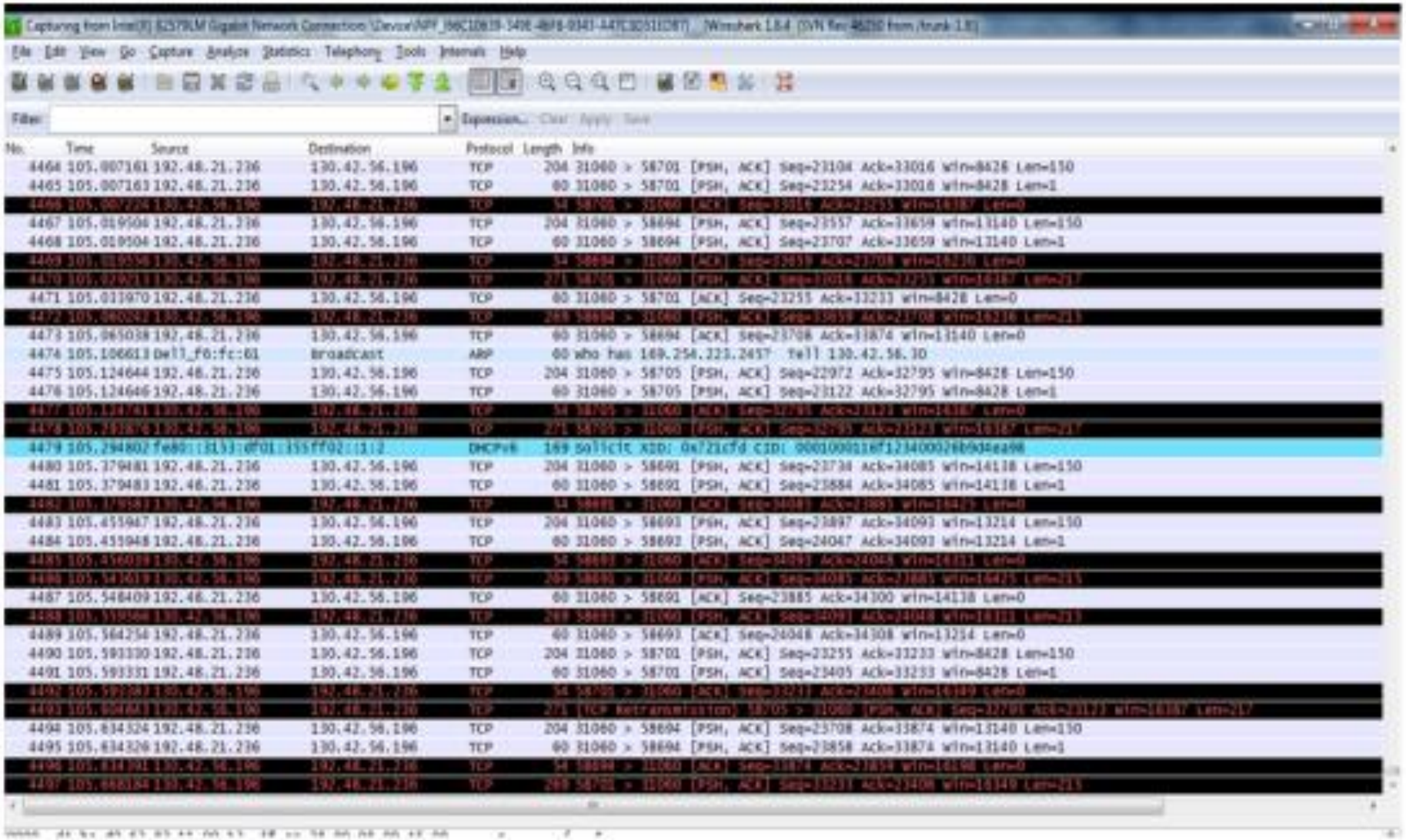


What Security Role Does a Router Provide ? ?

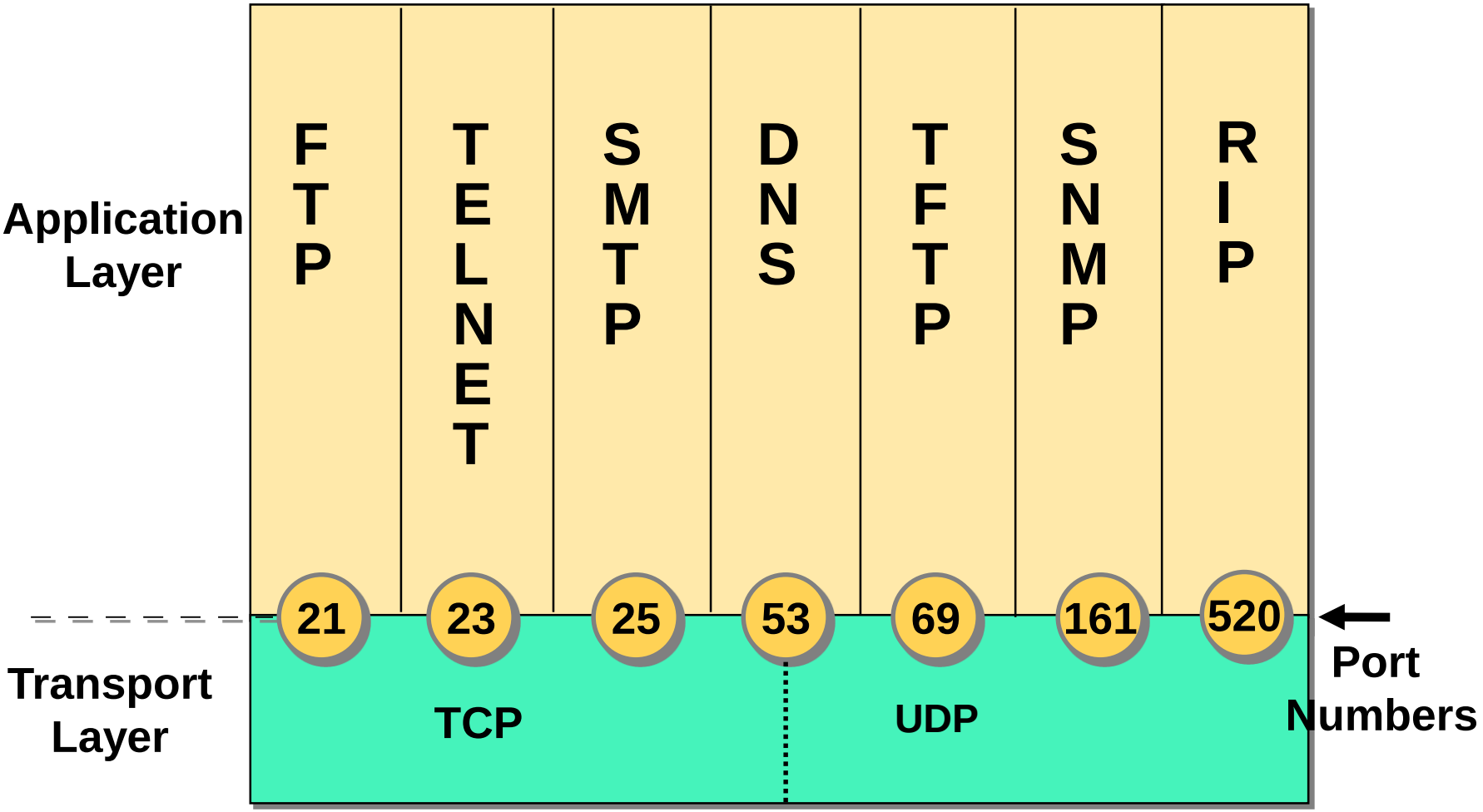
If router isn't doing security function – what is ? ? ?

Network Centric (Net Protocols)

Ethernet Frame Protocol Decodes



Port Numbers



Key Takeaway

The primary components and strategies of cyber security/IA are network centric based.

They attempt to inspect, monitor, filter/block traffic on network based mechanisms;

- **internet protocol (IP) address**
- **IP TCP/UDP port**
- **network access control lists (ACLs)**

Ethernet frames and TCP/IP Packets

Sniffer - Local, SX - [IPARP: Decode, 4/65 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR	60	0:00:48.026	0.000.855	
9		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642	60	0:00:48.033	0.001.230	
11		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	
12		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.001.545	
13		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.000.675	
14		[144.116.200.1]	[144.116.200.10	Telnet: R PORT=1024 IAC Will Echo	60	0:00:48.042	0.001.080	
15		[144.116.200.1]	[144.116.200.10	Telnet: R PORT=1024 <0D0A0D0A0D0A> DAN McIn	246	0:00:48.054	0.011.505	
16		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642787 WIN=28474	60	0:00:48.204	0.150.345	
17		[144.116.200.10	[144.116.200.1]	Telnet: C PORT=1024 IAC Do Suppress go-ahead	60	0:00:48.231	0.027.180	
18		[144.116.200.1]	[144.116.200.10	Telnet: R PORT=1024 IAC Don't Terminal-type	60	0:00:48.233	0.001.905	

```
LOOP: ----- LOOPBACK Version 2.0 Frame -----
  LOOP:
  LOOP: Skip Count      = 0
  LOOP: Message type    = Reply message
  LOOP: Receipt number  = 27726
  LOOP:
```

```
00000000: 00 00 0c 00 b5 22 00 00 0c 00 b5 22 90 00 00 00  ....µ"....µ"▌...
00000010: 01 00 4e 6c 02 b1 c8 40 7d 01 00 a0 00 00 f4 f4  ..Nl.±È@}.. ..ôô
00000020: 03 00 38 84 01 00 0a 40 03 40 00 00 00 01 11 00  ..8▌...@.@......
00000030: 06 c0 01 ff ff 00 06 c0 02 80 00 00 0c c0 0b 53  .À.ÿÿ..À.▌...À.S
00000040: 4e 49 46 46 45 52 00 00 12 40 0c 00 00 00 00 00  NIFFER...@......
00000050: 00 00 00 00 00 00 00 00 00 71 71 a2 3f 00 34 35  .........qq¢?.45
00000060: 36 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00  67..............
00000070: 00 00 00 00 00 00                                ......
```

Expert Decode Matrix Host Table Protocol Dist. Statistics

For Help, press F1

start Sniffer - Local, SX - [I... Wireshark Protocol Tr... 11:12 AM

Sniffer - Local, SX - [IPARP: Decode, 7/65 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR	60	0:00:48.026	0.000.855	
9		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642	60	0:00:48.033	0.001.230	
11		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	
12		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.001.545	
13		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 ACK=4290181122 WIN=2240	60	0:00:48.041	0.000.675	
14		[144.116.200.1]	[144.116.200.10	Telnet: R PORT=1024 IAC Will Echo	60	0:00:48.042	0.001.080	
15		[144.116.200.1]	[144.116.200.10	Telnet: R PORT=1024 <0D0A0D0A0D0A> DAN McIn	246	0:00:48.054	0.011.505	
16		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642787 WIN=28474	60	0:00:48.204	0.150.345	
17		[144.116.200.10	[144.116.200.1]	Telnet: C PORT=1024 IAC Do Suppress go-ahead	60	0:00:48.231	0.027.180	
18		[144.116.200.1]	[144.116.200.10	Telnet: R PORT=1024 IAC Don't Terminal-type	60	0:00:48.233	0.001.905	

```
DLC:  ----- DLC Header -----
  DLC:
  DLC:  Frame 7 arrived at  10:55:45.0257; frame size is 60 (003C hex) bytes.
  DLC:  Destination = BROADCAST FFFFFFFFFFFF, Broadcast
  DLC:  Source      = Station UB    076082
  DLC:  Ethertype   = 0806 (ARP)
  DLC:
ARP: ----- ARP/RARP frame -----
  ARP:
  ARP: Hardware type = 1 (10Mb Ethernet)
  ARP: Protocol type = 0800 (IP)
  ARP: Length of hardware address = 6 bytes
  ARP: Length of protocol address = 4 bytes
  ARP: Opcode 1 (ARP request)
  ARP: Sender's hardware address = 00DD01076082
  ARP: Sender's protocol address = [144.116.200.107]
  ARP: Target hardware address   = 000000000000
  ARP: Target protocol address   = [144.116.200.1]
  ARP:
  ARP: 18 bytes frame padding
```

```
00000000: ff ff ff ff ff ff 00 dd 01 07 60 82 08 06 00 01 ÿÿÿÿÿÿ.Ý..`‚..
```

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

For Help, press F1

start | Sniffer - Local, SX - [I... | Wireshark Protocol Tr... | Sniffer_IP-ARP_ENC | 11:16 AM

Sniffer - Local, SX - [IPARP: Decode, 9/65 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR	60	0:00:48.026	0.000.855	
9		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642	60	0:00:48.033	0.001.230	
11		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	

```
TCP: ----- TCP header -----
TCP:
TCP: Source port              =  1024
TCP: Destination port         =    23 (Telnet)
TCP: Initial sequence number = 4290181121
TCP: Next expected Seq number= 4290181122
TCP: Data offset              = 24 bytes
TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
TCP: Flags                    = 02
TCP:                ..0. .... = (No urgent pointer)
TCP:                ...0 .... = (No acknowledgment)
TCP:                .... 0... = (No push)
TCP:                .... .0.. = (No reset)
TCP:                .... ..1. = SYN
TCP:                .... ...0 = (No FIN)
TCP: Window                   = 28672
TCP: Checksum                 = 7B4F (correct)
TCP: Urgent pointer           = 0
TCP:
TCP: Options follow
TCP: Maximum segment size = 1381
TCP:
DLC:  Frame padding= 2 bytes
```

```
00000000: 00 00 0c 00 b5 22 00 dd 01 07 60 82 08 00 45 00  ....µ".Ý..`‚..E.
00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74  .,Óù.....}‚tÈk‚t
```

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

For Help, press F1

start | Sniffer - Local, SX - [I... | Wireshark Protocol Tr... | Sniffer_IP-ARP_ENC | 11:17 AM

Sniffer - Local, SX - [IPARP: Decode, 9/65 Ethernet Frames]

File Monitor Capture Display Tools Database Window Help

Default

No.	Status	Source Address	Dest Address	Summary	Len (B	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	0:00:30.000	9.979.035	
5		[144.116.200.1]	[144.116.200.25	IGRP: Update AS=9 Subnets=1 AS network=0 AS	60	0:00:33.015	3.015.465	
6		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =117	118	0:00:40.000	6.984.750	
7		UB 076082	Broadcast	ARP: C PA=[144.116.200.1] PRO=IP	60	0:00:48.025	8.025.060	
8		Cisco 00B522	UB 076082	ARP: R PA=[144.116.200.1] HA=Cisco 00B522 PR	60	0:00:48.026	0.000.855	
9		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 SYN SEQ=4290181121 LEN=0 WI	60	0:00:48.032	0.005.760	
10		[144.116.200.1]	[144.116.200.10	TCP: D=1024 S=23 SYN ACK=4290181122 SEQ=3642	60	0:00:48.033	0.001.230	
11		[144.116.200.10	[144.116.200.1]	TCP: D=23 S=1024 ACK=3642589 WIN=28672	60	0:00:48.039	0.006.015	

```
TCP: ----- TCP header -----
TCP:
TCP: Source port              =  1024
TCP: Destination port         =    23 (Telnet)
TCP: Initial sequence number = 4290181121
TCP: Next expected Seq number= 4290181122
TCP: Data offset              = 24 bytes
TCP: Reserved Bits: Reserved for Future Use (Not shown in the Hex Dump)
TCP: Flags                    = 02
TCP:                ..0. .... = (No urgent pointer)
TCP:                ...0 .... = (No acknowledgment)
TCP:                .... 0... = (No push)
TCP:                .... .0.. = (No reset)
TCP:                .... ..1. = SYN
TCP:                .... ...0 = (No FIN)
TCP: Window                   = 28672
TCP: Checksum                 = 7B4F (correct)
TCP: Urgent pointer           = 0
TCP:
TCP: Options follow
TCP: Maximum segment size = 1381
TCP:
DLC:  Frame padding= 2 bytes
```

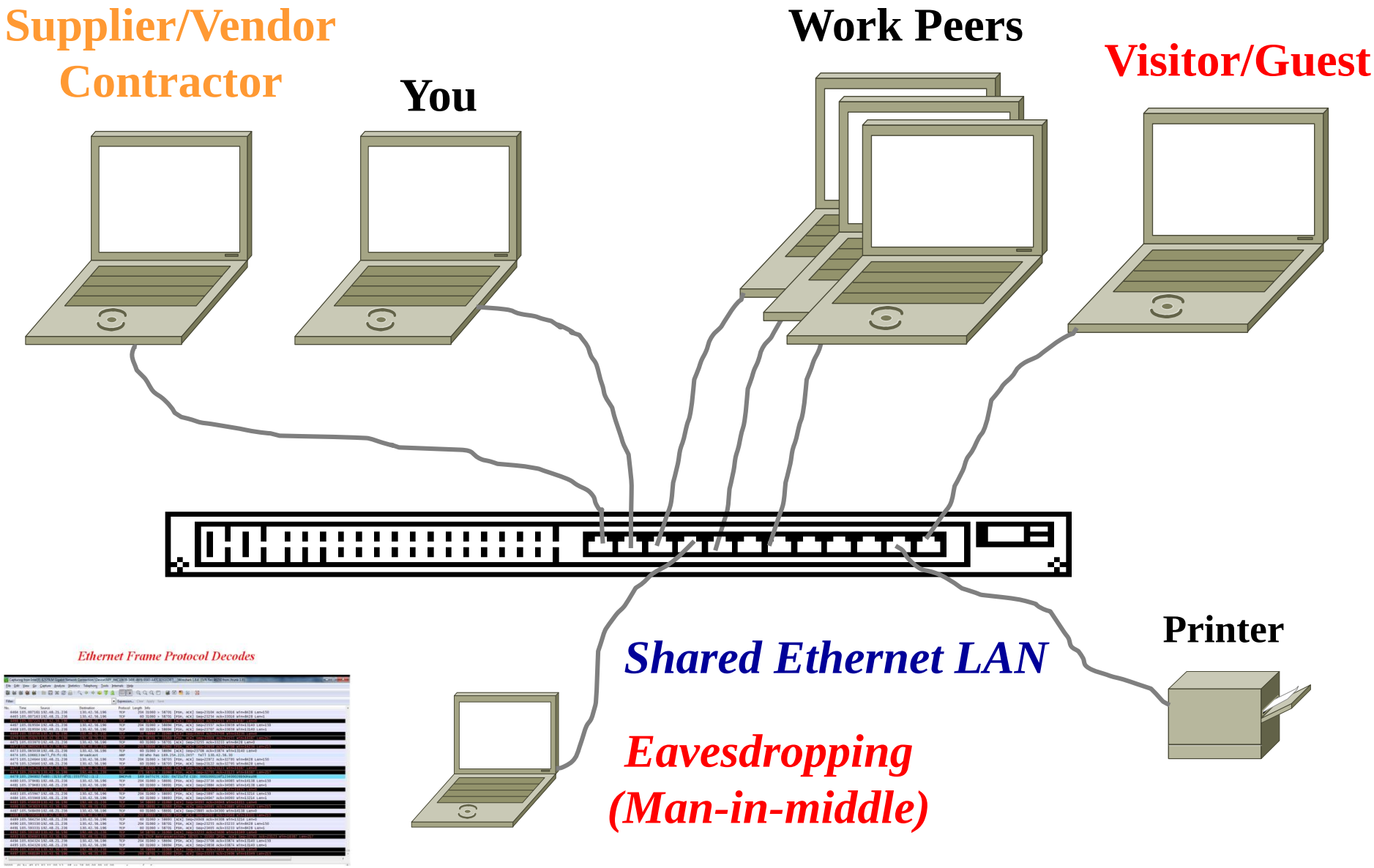
```
00000000: 00 00 0c 00 b5 22 00 dd 01 07 60 82 08 00 45 00  ....µ".Ý..`‚..E.
00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74  .,Óù.....}‚tÈk‚t
```

Expert | Decode | Matrix | Host Table | Protocol Dist. | Statistics

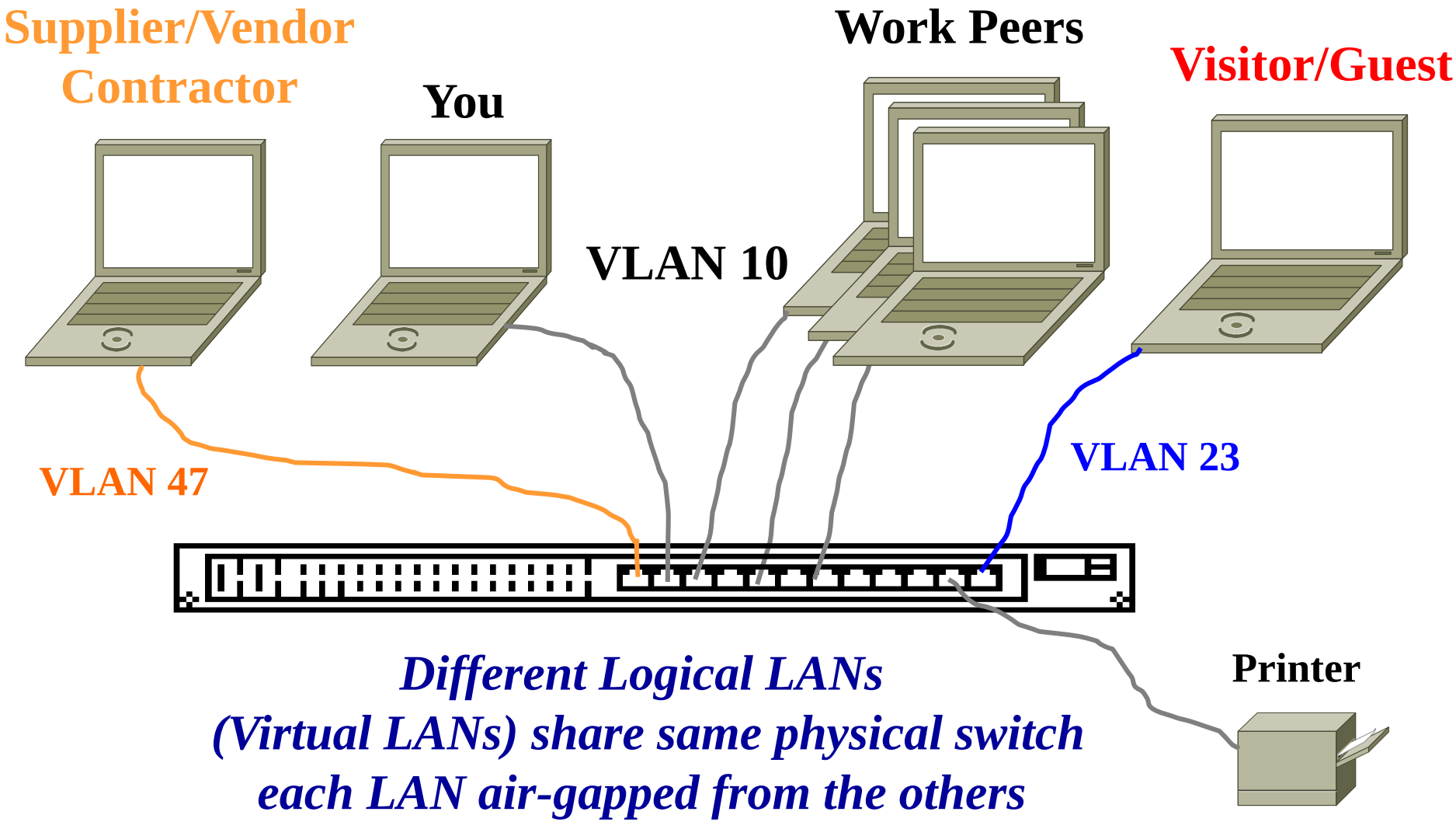
For Help, press F1

start | Sniffer - Local, SX - [I... | Wireshark Protocol Tr... | Sniffer_IP-ARP_ENC | 11:17 AM

VLANs (Virtual LANs)

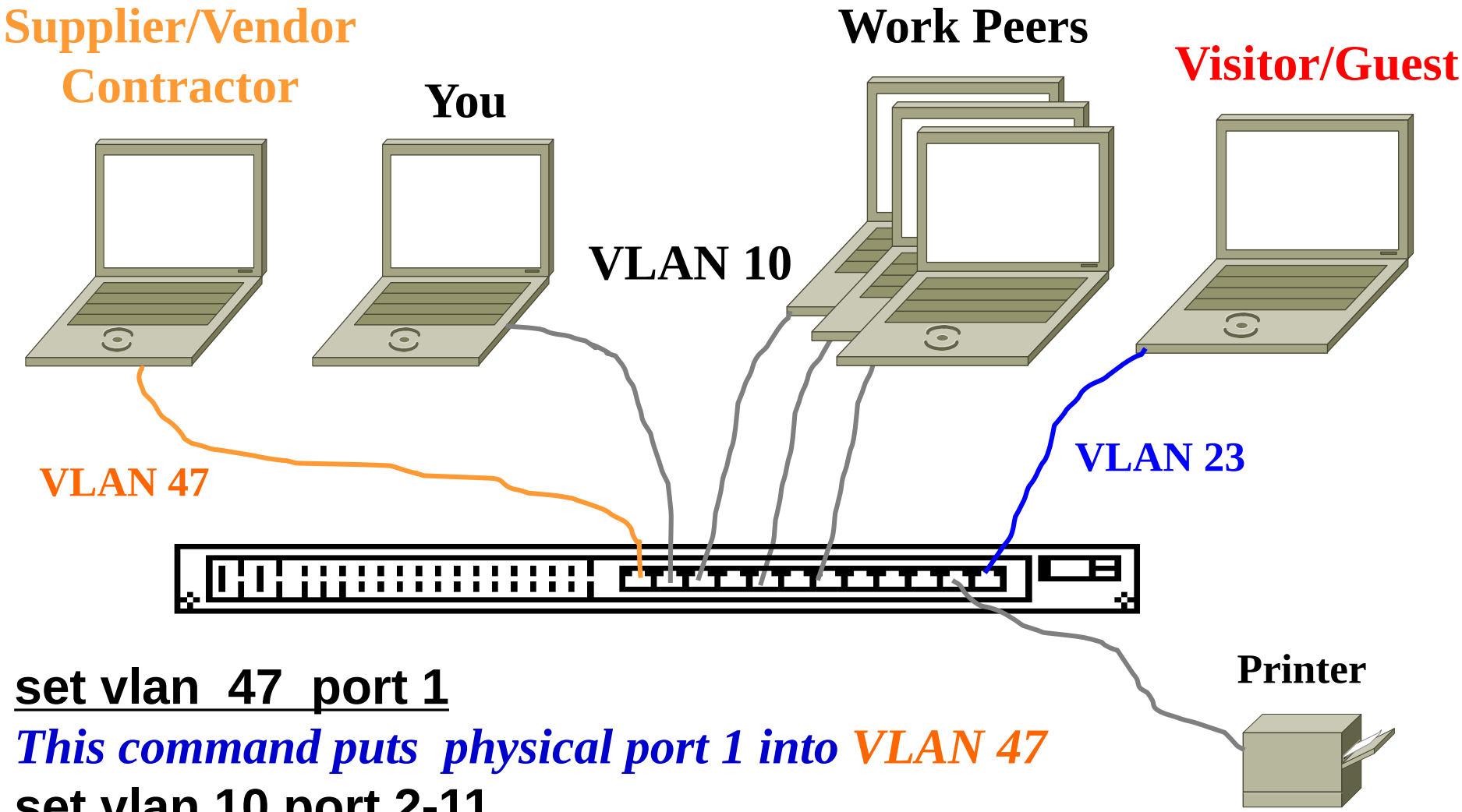


VLANs (Virtual LANs)



Different Logical LANs
(Virtual LANs) share same physical switch
each LAN air-gapped from the others

VLANs (Virtual LANs)



<u>set vlan 47 port 1</u>

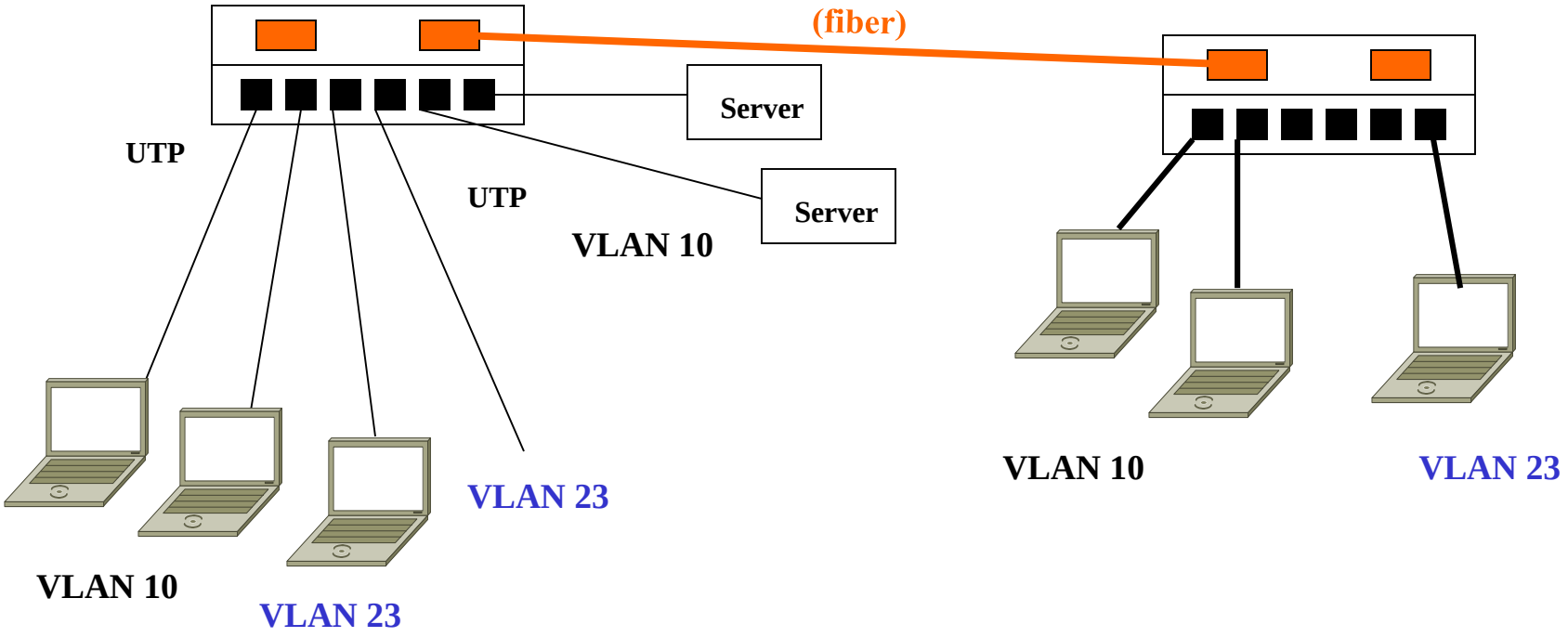
This command puts physical port 1 into VLAN 47

<u>set vlan 10 port 2-11</u>

This would put physical ports 2 thru 11 into VLAN 10

Question: ***What command set for Visitor/Guest port into VLAN 23 ?***

Interconnected LAN Switches



Workplace

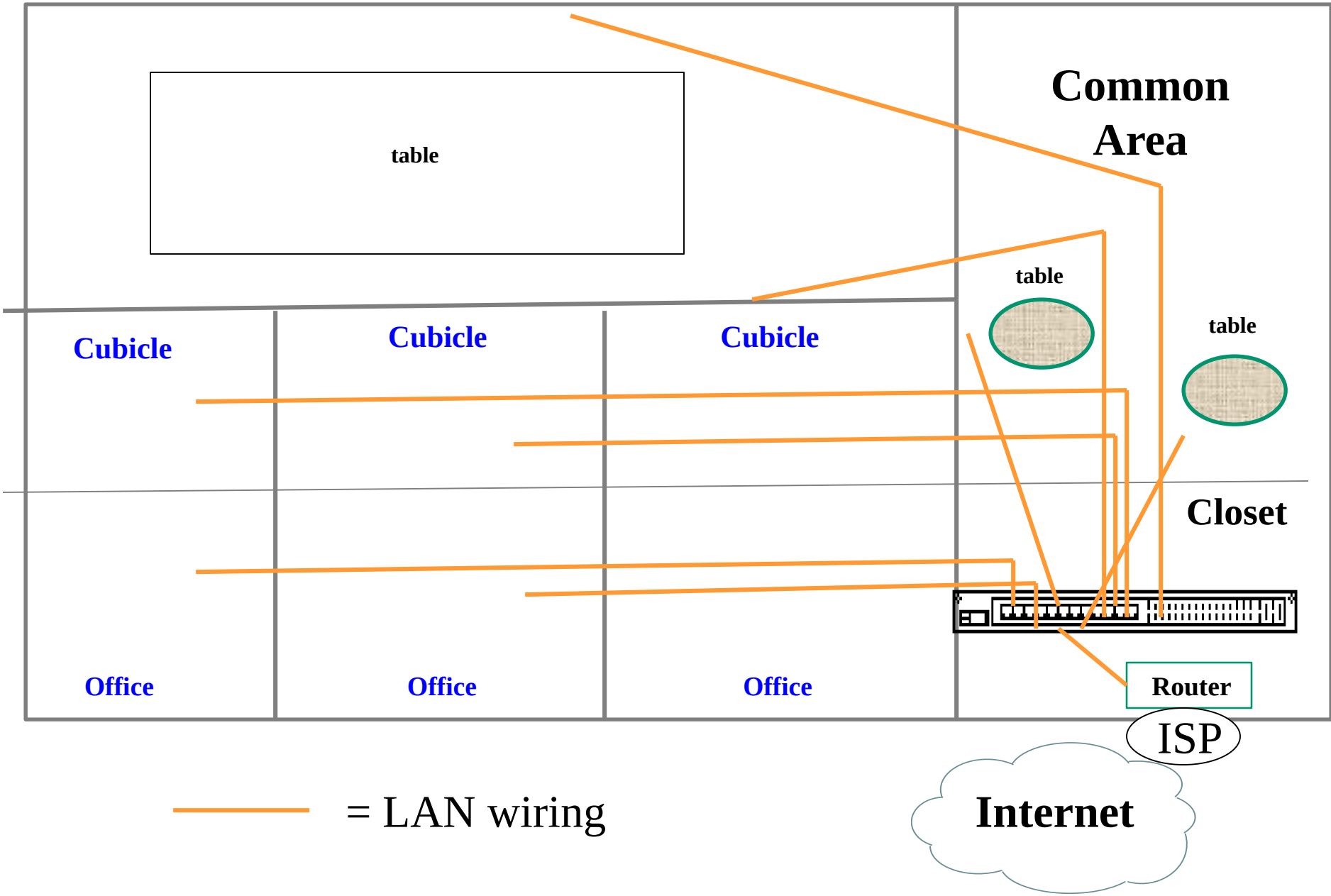
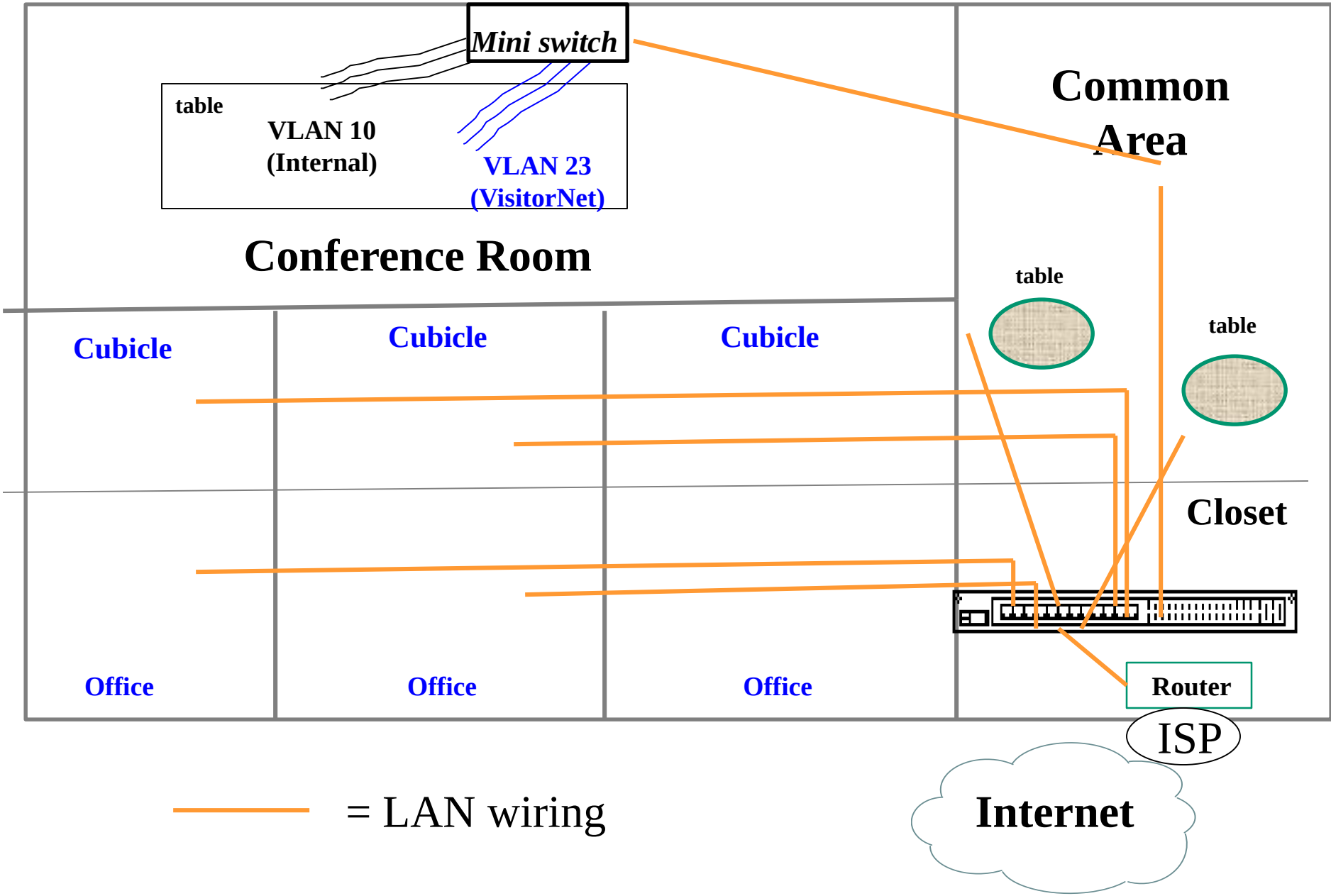
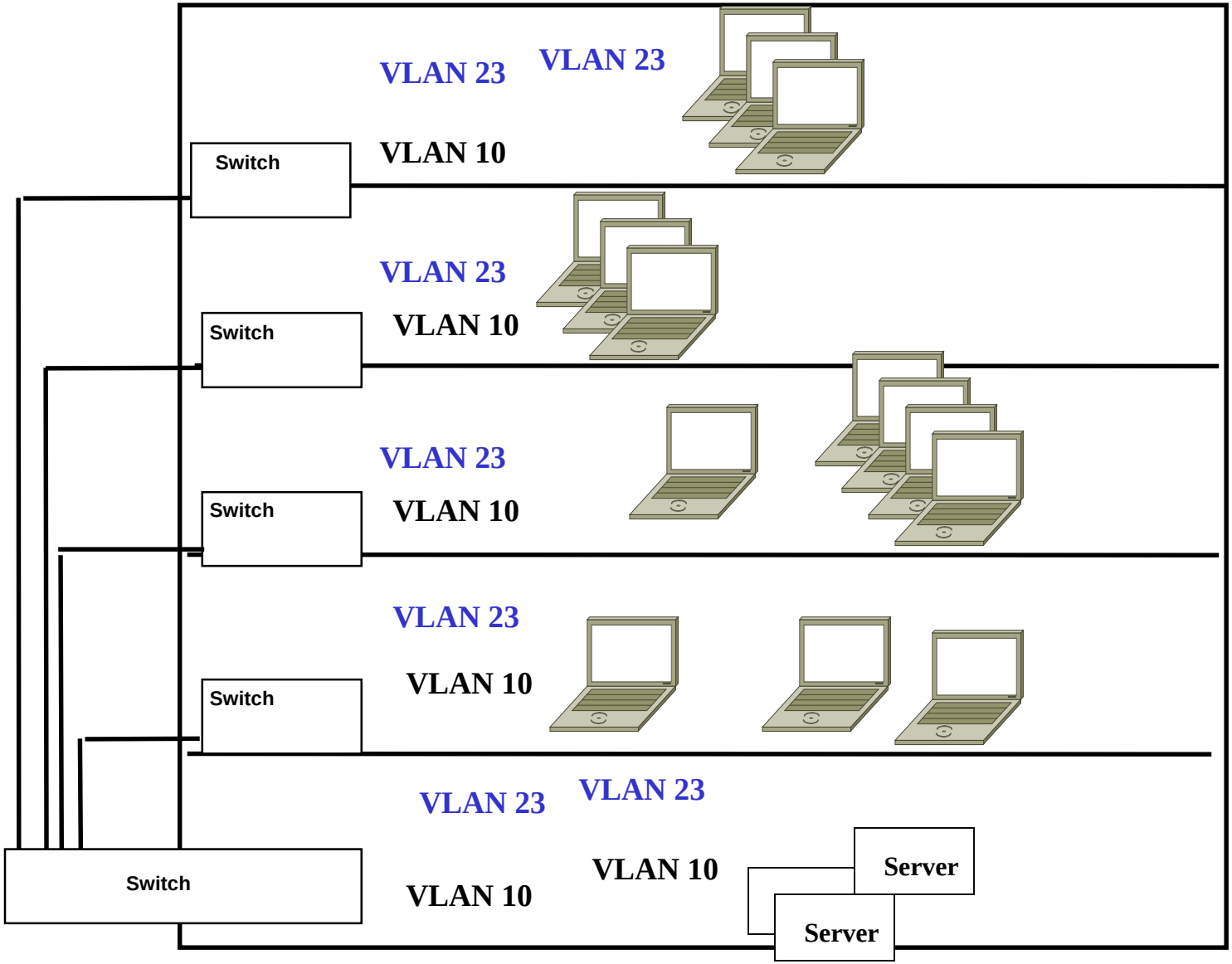


table
Common Area
table
table
Cubicle
Cubicle
Cubicle
Closet
Office
Office
Office
Router
ISP
Internet
= LAN wiring

Workplace


Mini switch
table
VLAN 10
(Internal)
VLAN 23
(VisitorNet)
Conference Room
Common
Area
table
table
Cubicle
Cubicle
Cubicle
Closet
Office
Office
Office
Router
ISP
Internet
= LAN wiring

Office Environment



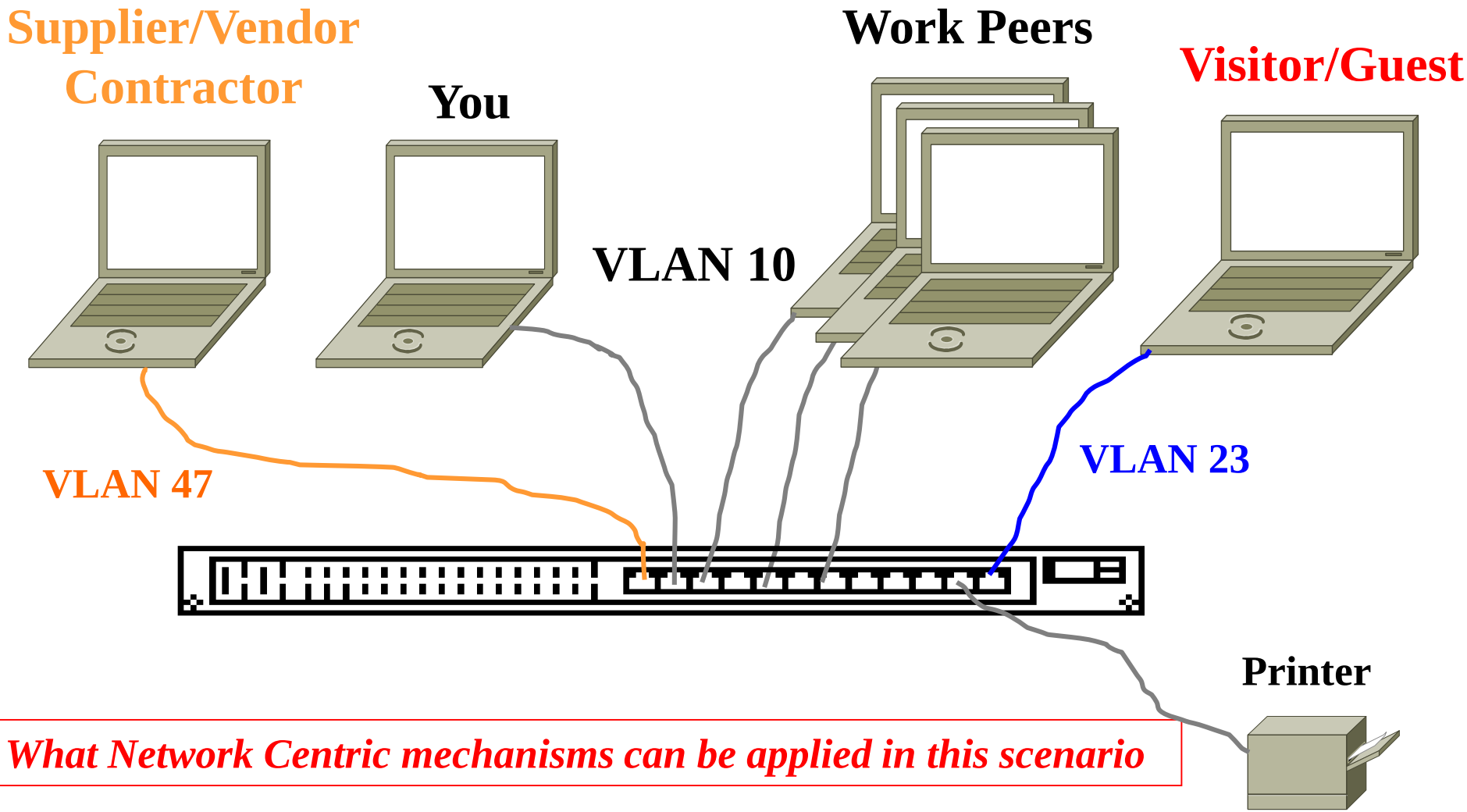
What is the name of the technology that allows multiple VLANs to run over a single cable (between LAN Switches) ?

VLAN <u>Trunking</u>

Are VLANs a Security Mechanism ?

Yes, VLANs allow separation of LAN traffic based on user need (princ of least priv)

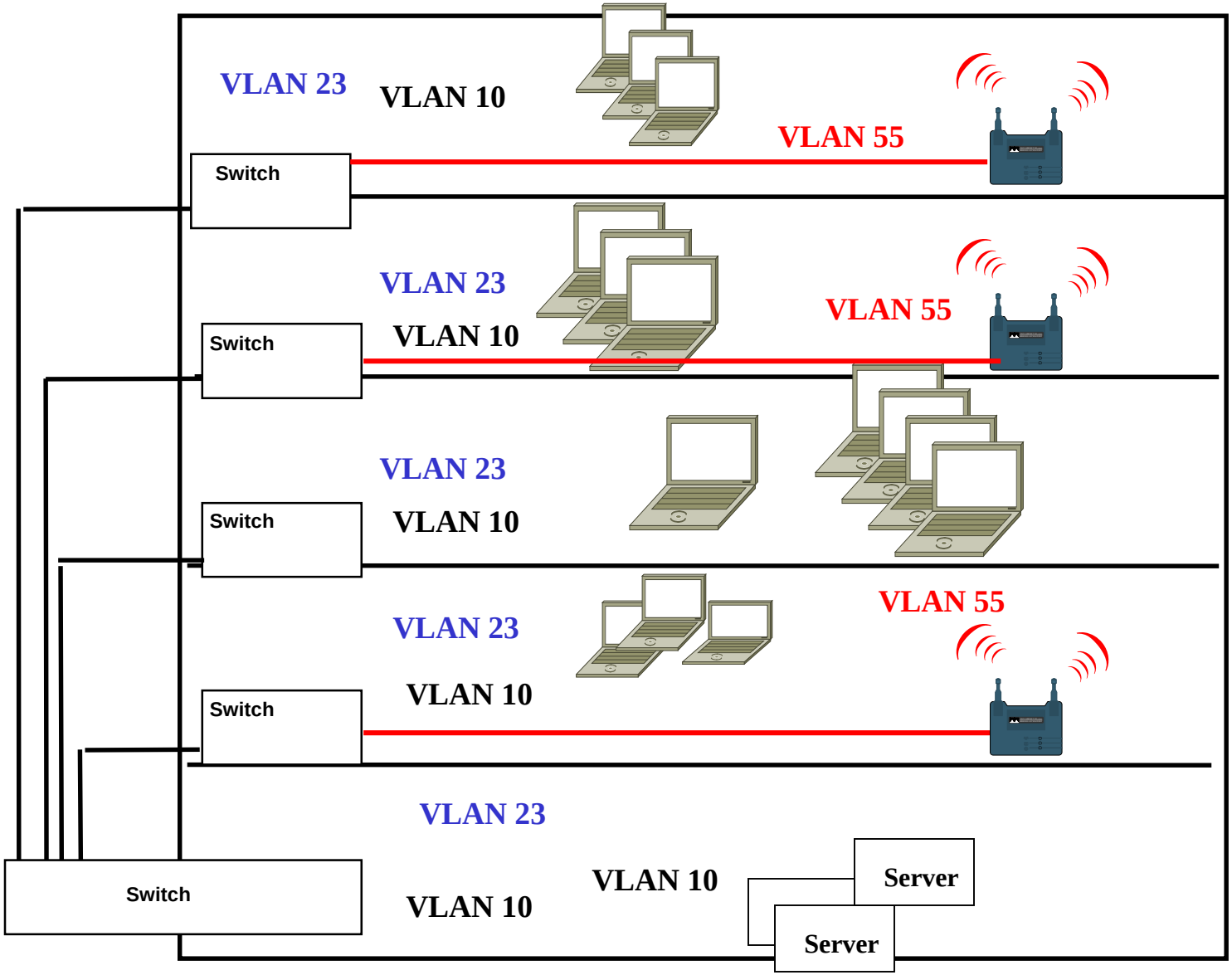
Protection Mechanisms



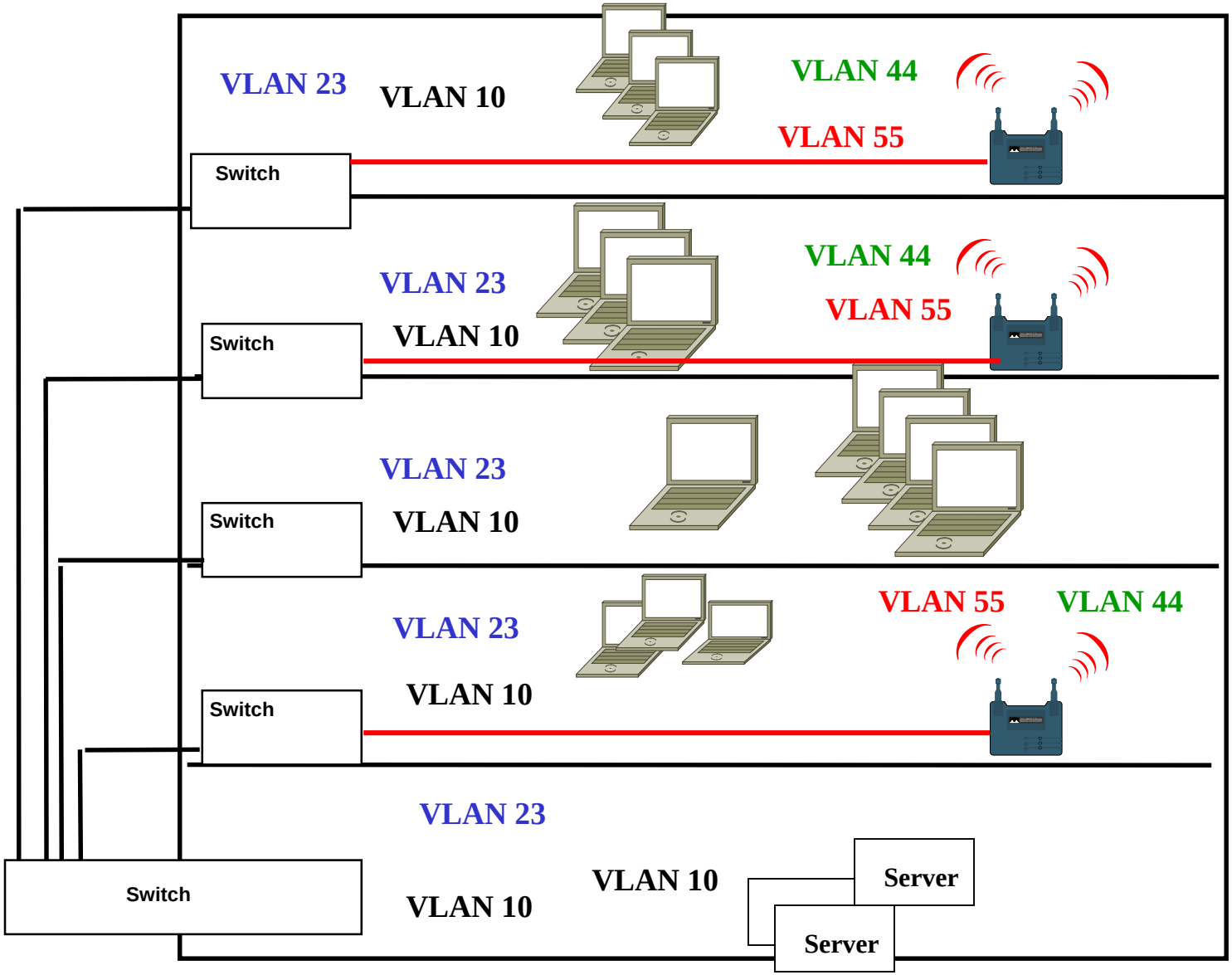
What Network Centric mechanisms can be applied in this scenario

What Data Centric mechanisms can be applied in this scenario

Office Environment



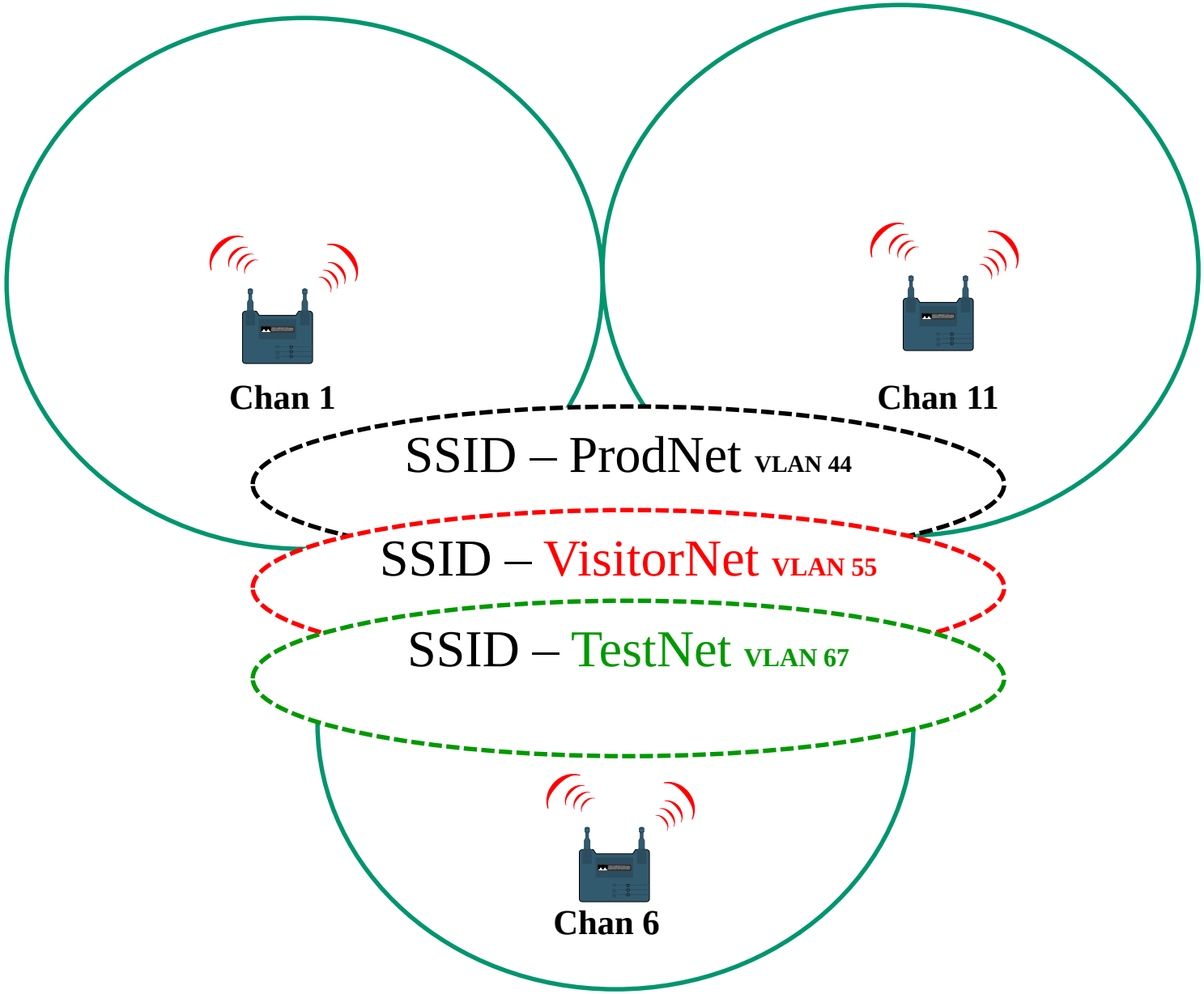
Office Environment



Rev: Feb, 2013

Wireless LAN Channel Reuse Patterns

IEEE 802.11b/g 3 Channel Reuse Pattern



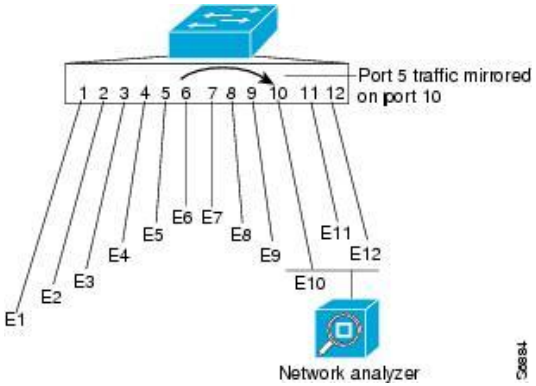
What separates access to the different WLAN SSID's ??

Lab 3. Port Mirroring - Configuring SPAN capability

Understanding How SPAN Works

SPAN mirrors traffic from one or more source ports (Ethernet, Fast Ethernet, Token Ring, or FDDI) on any VLAN to a destination port for analysis (see Figure 27-1).

Figure 27-1 Example SPAN Configuration



In Figure 27-1, all traffic on Ethernet port 5 (the source port) is mirrored to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to it.

SPAN Configuration Guidelines - Configuring SPAN

To configure SPAN, perform this task in privileged mode:

	Task	Command
Step 1	Configure a SPAN source and a SPAN destination port.	**set span** {*src_mod*/*src_ports* | *src_vlan* | *sc0*} *dest_mod*/*dest_port* [**rx** | **tx** | **both**] [**inpkts** {**enable** | **disable**}] [**learning** {**enable** | **disable**}] [**multicast** {**enable** | **disable**}] [**create**]
Step 2	Verify the SPAN configuration.	**show span**

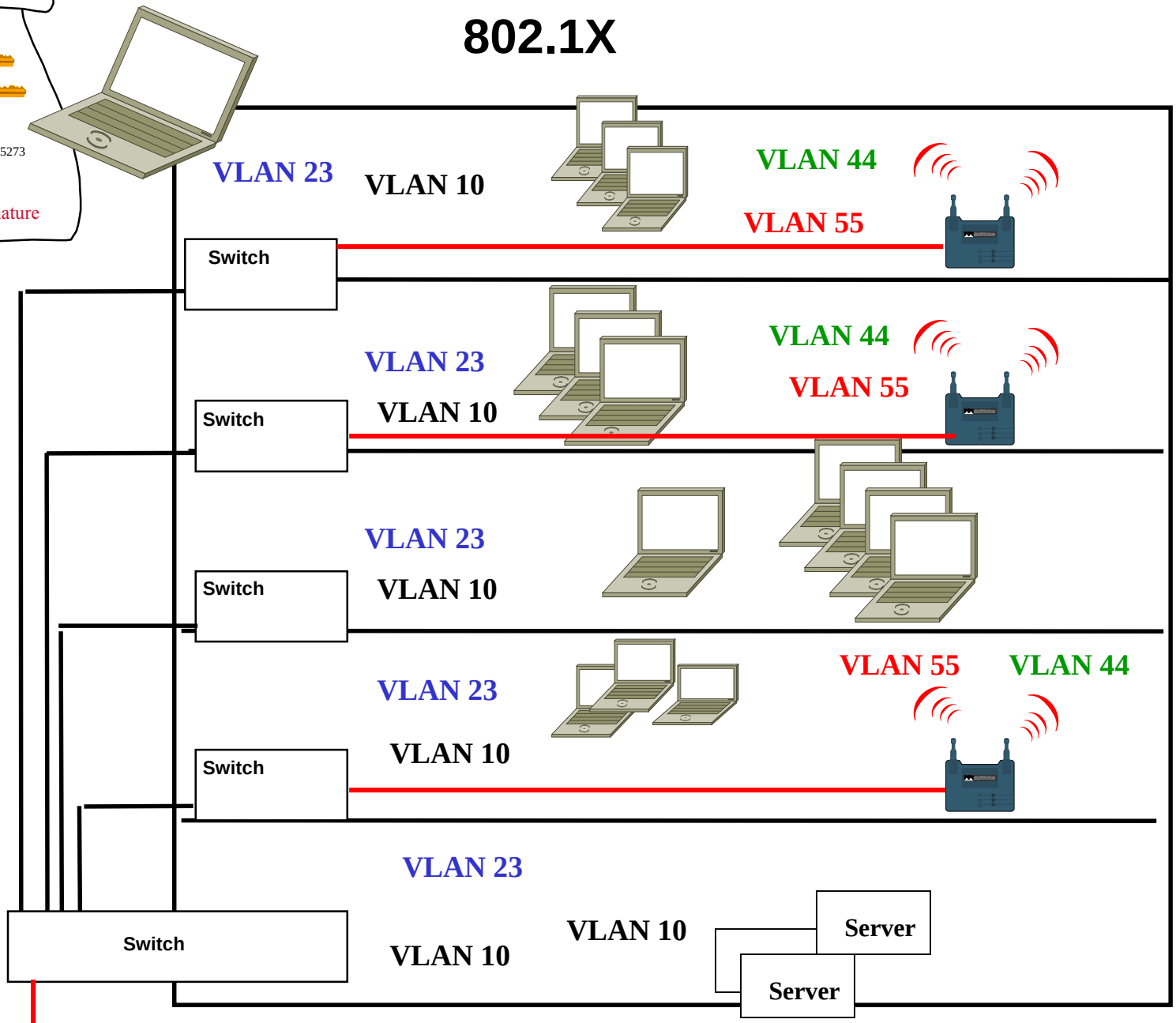
802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

Technically, IEEE 802.1X defines the encapsulation of the Extensible Autentication Protocol (EAP).

What Does it *REALLY* do ?

802.1X



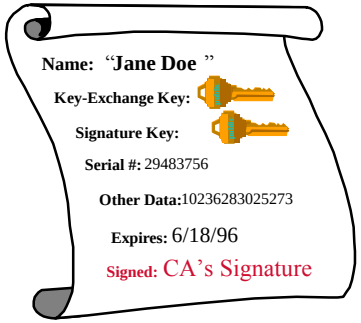
Wired Ports

Control what apps they access

Wireless VLANs w/X509 – WPA2 w/out guest net access

Authentication Server/Mgr validates key, device gets IP add

What is a Certificate?



- Security certificates are data files
- Netscape and Microsoft web browsers store certificates in a password protected area on the user's desktop
- More trusted than passwords (strong authentication)
- They can be carried on floppies
- They can be carried in Smart Cards
- They are used to authenticate identity and establish encrypted communications

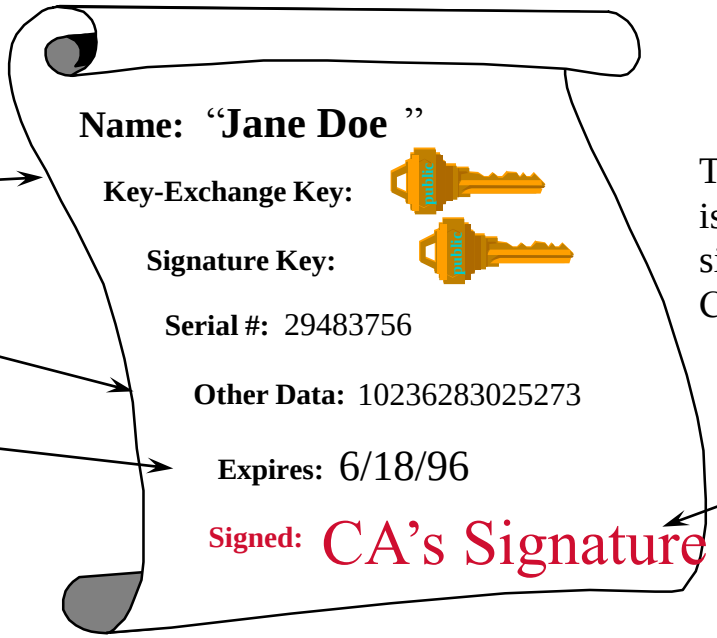
What is a Certificate?

Binds a public key to an identity

Certificate ties a name or identity to public keys

Other data

Certificate Validation



The authenticity of the certificate is guaranteed by the digital signature generated using the Certificate Authority's private key.

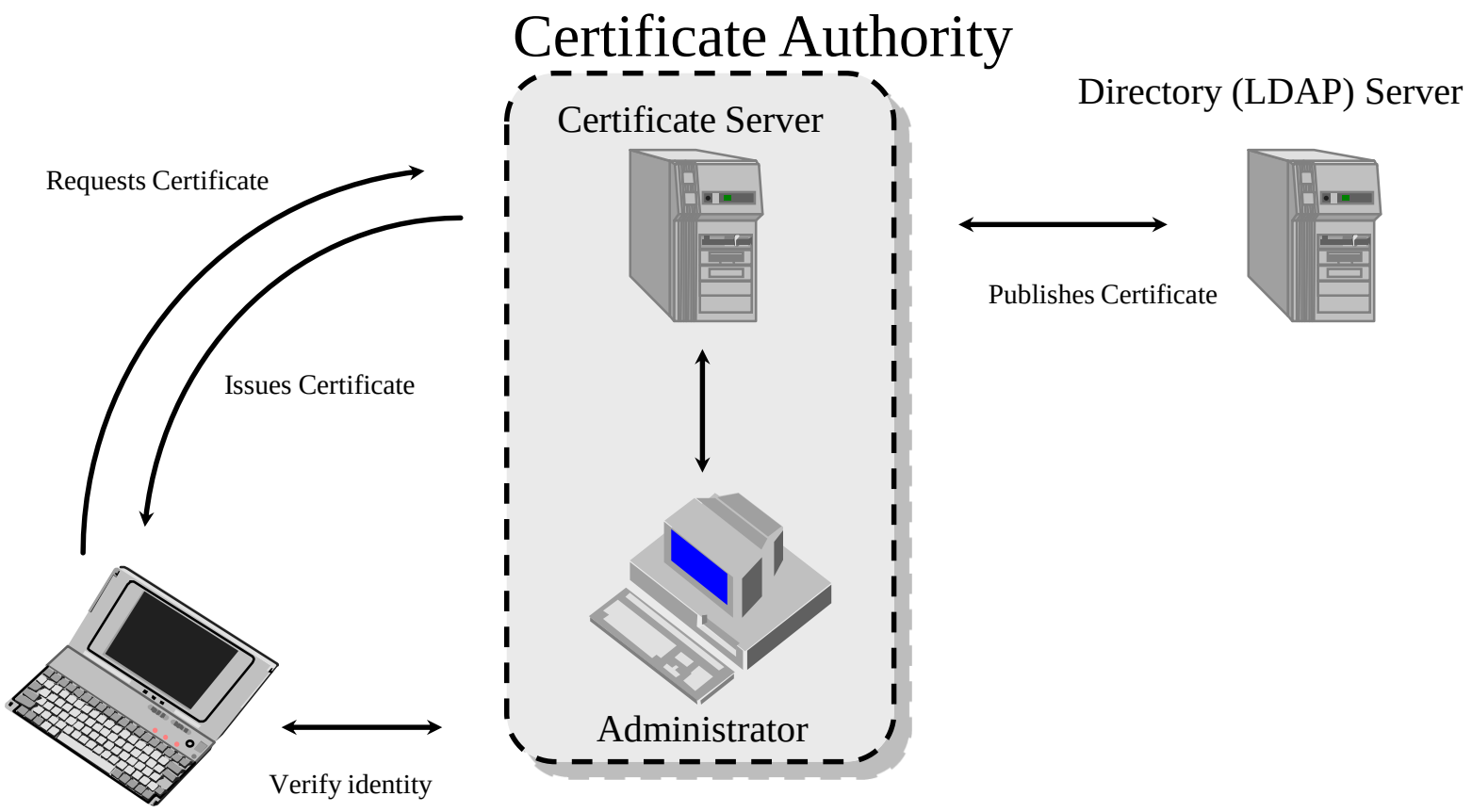
What Is a Certification Authority?

It is the service (software, servers, policies, procedures and support staff) which issues X.509 security certificates.

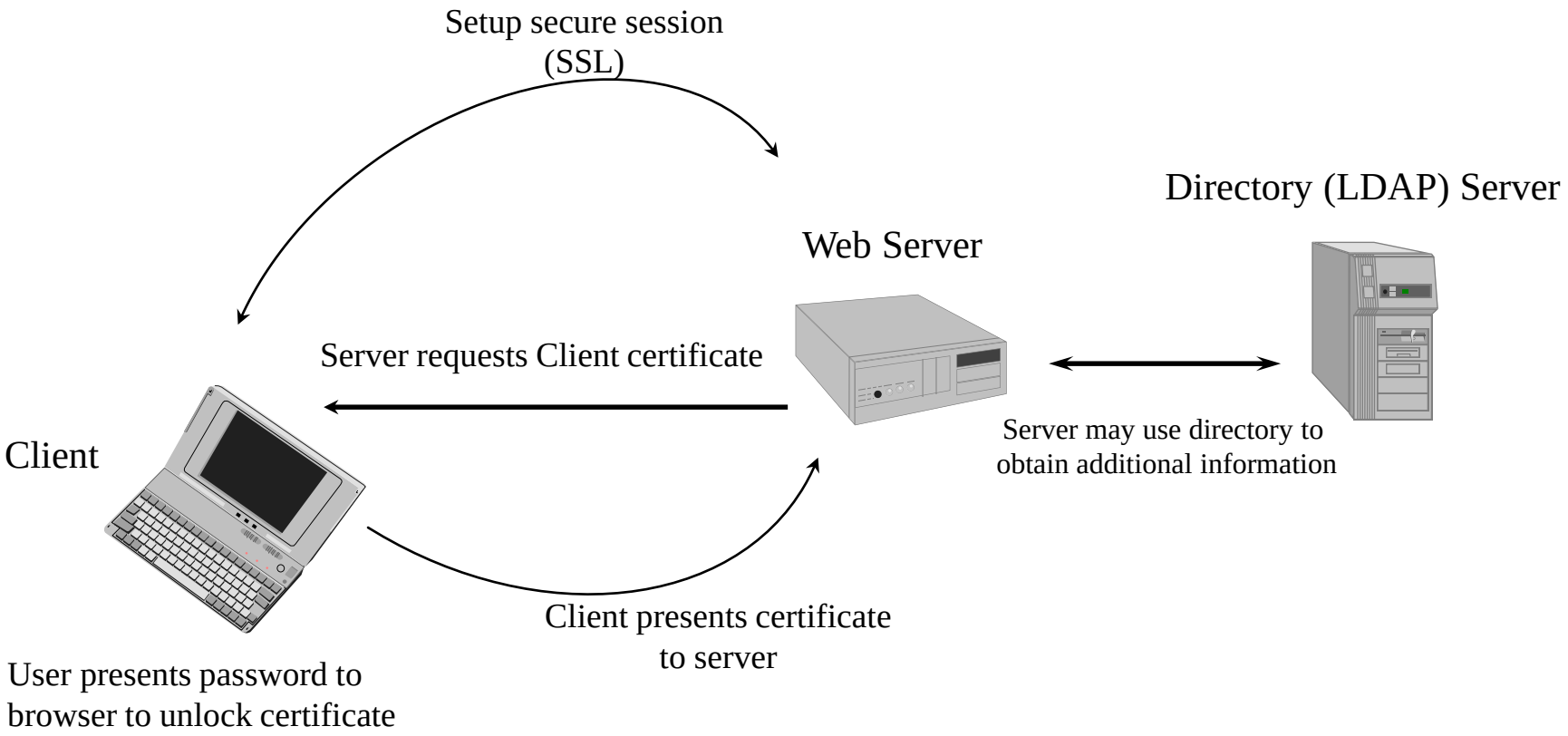
Primary responsibility of the Certificate Authority is to assure the identity of the person receiving the certificate.

The Authority is also responsible for revoking certificates.

Obtaining a Client Certificate



How to Use a Certificate



EAP Transaction