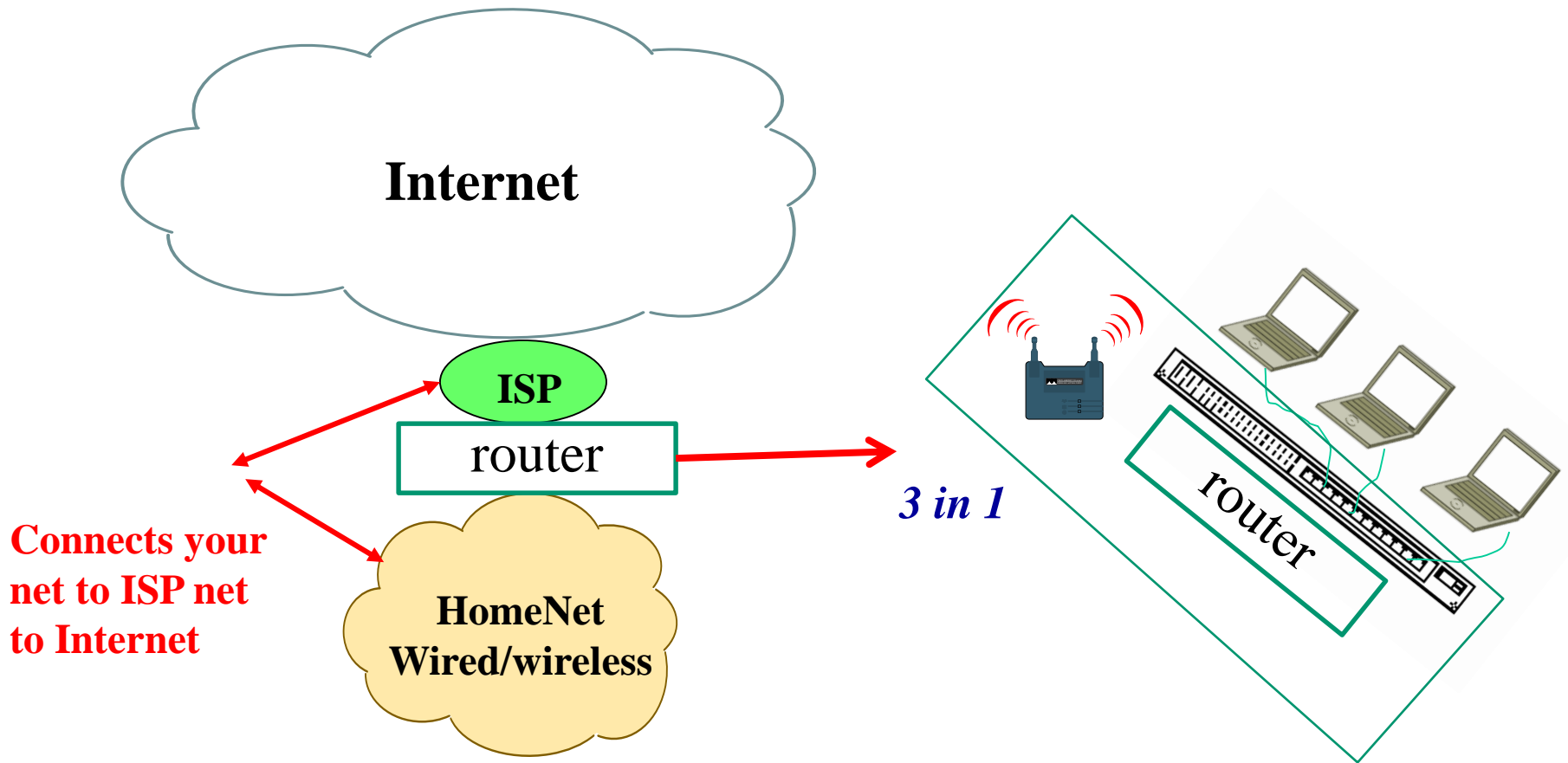


Network Security Summary

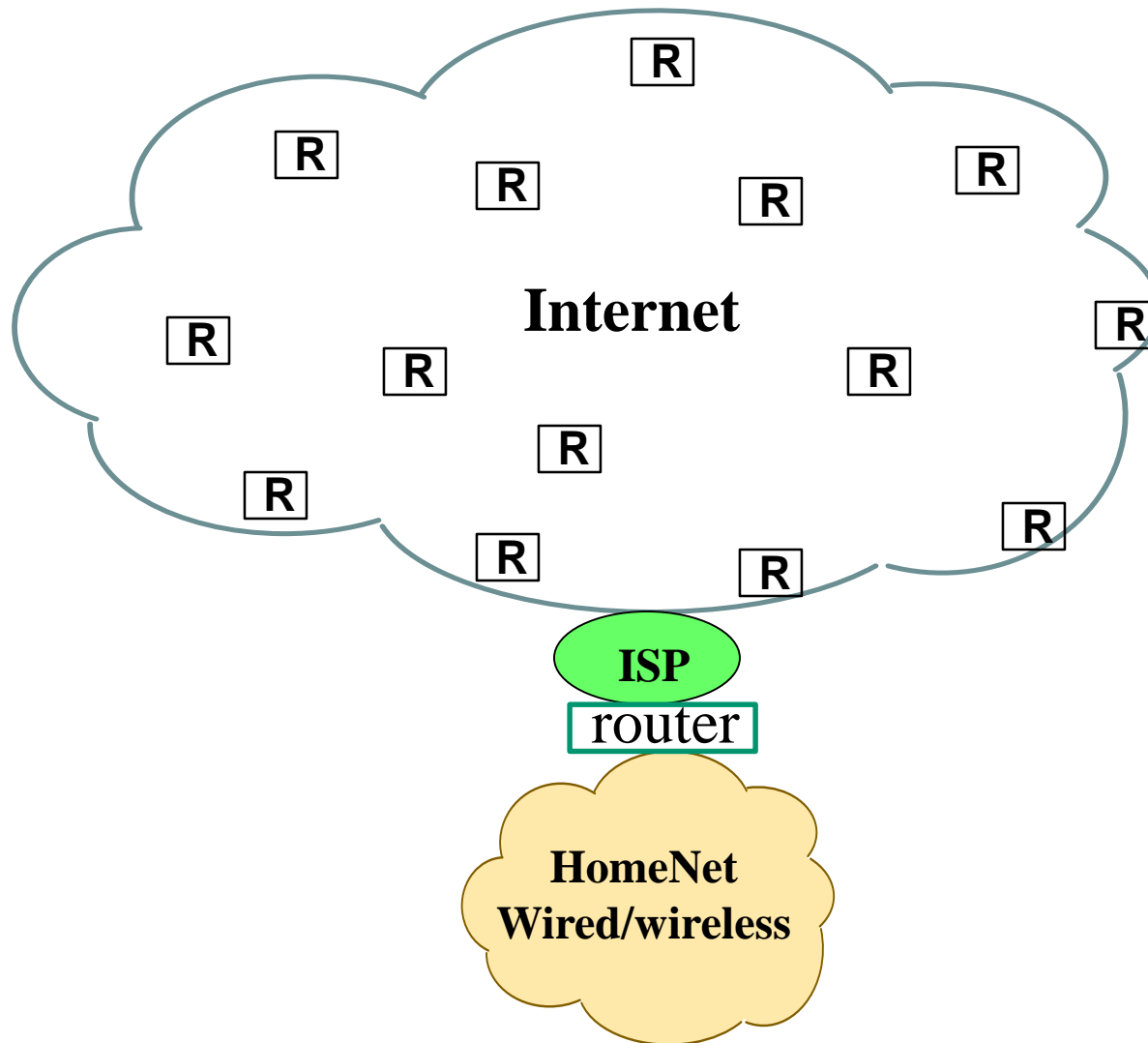
UW i310– 2016

Typical Home – Small Office Scenario



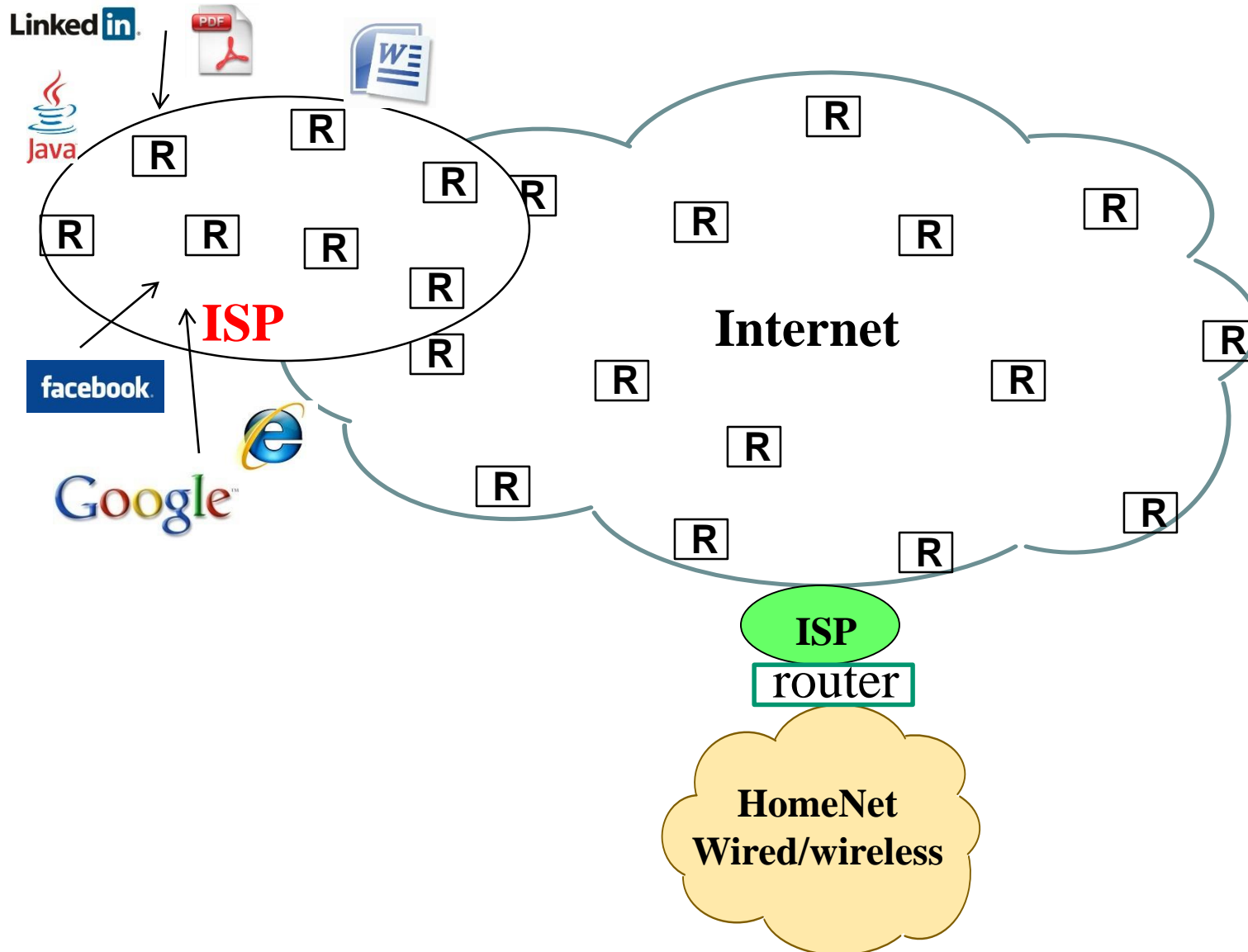
What is job of router - Interconnect Networks (at TCP/IP Net Layer)

Routers – Masters of Internet Domain

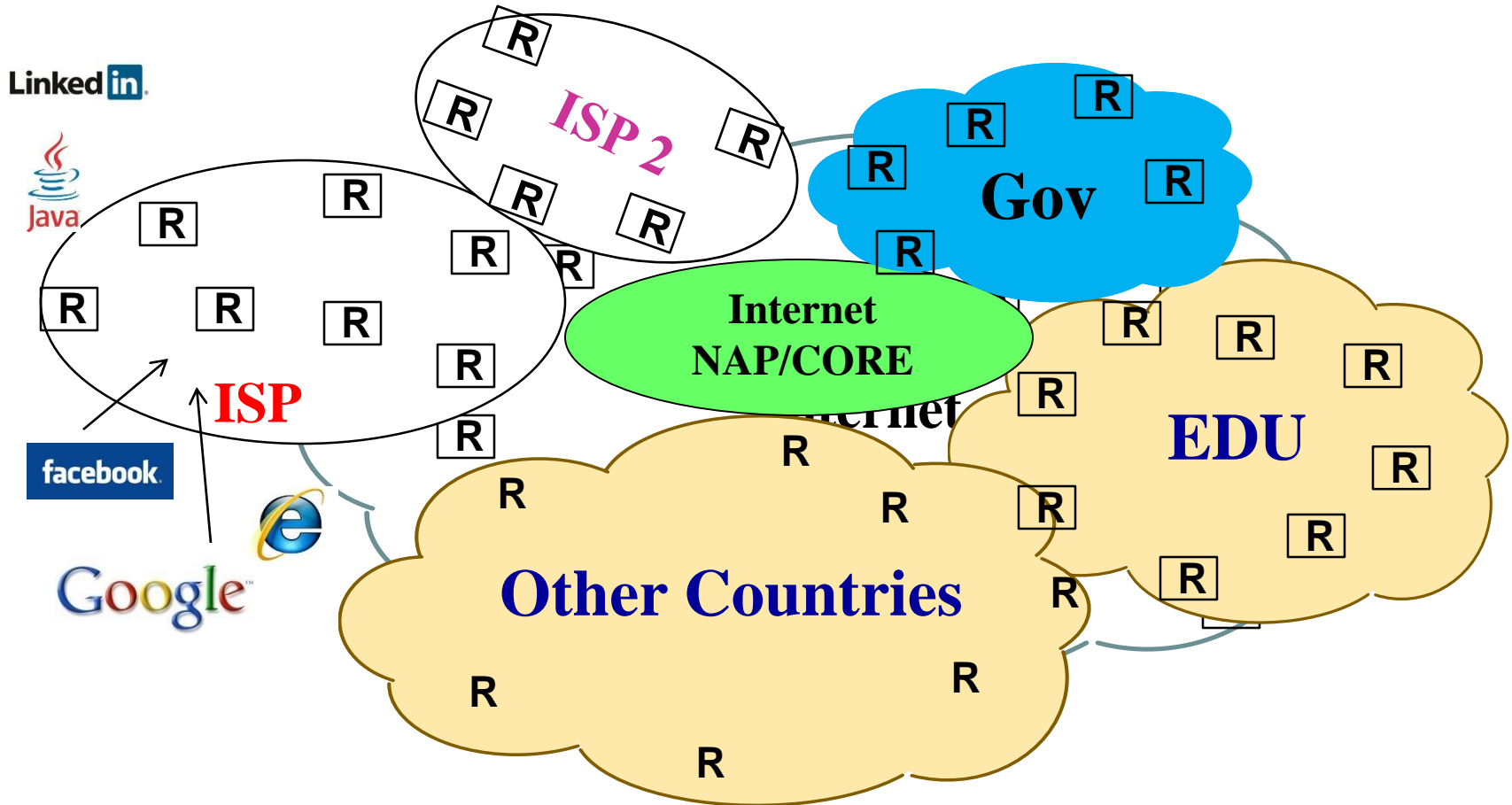


Routers – Masters of Internet Domain

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

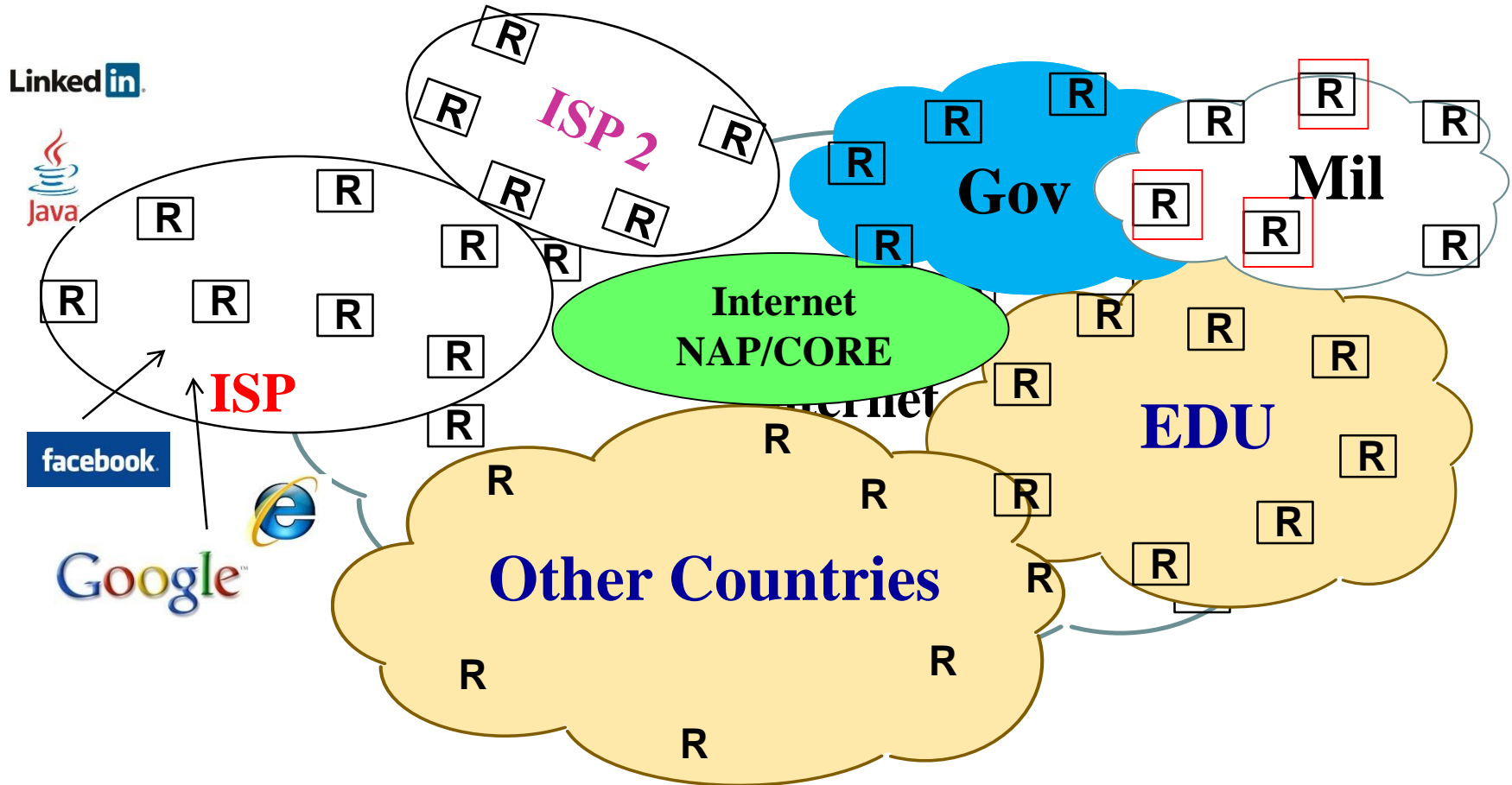


Routers – Greater Internet Domain



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)

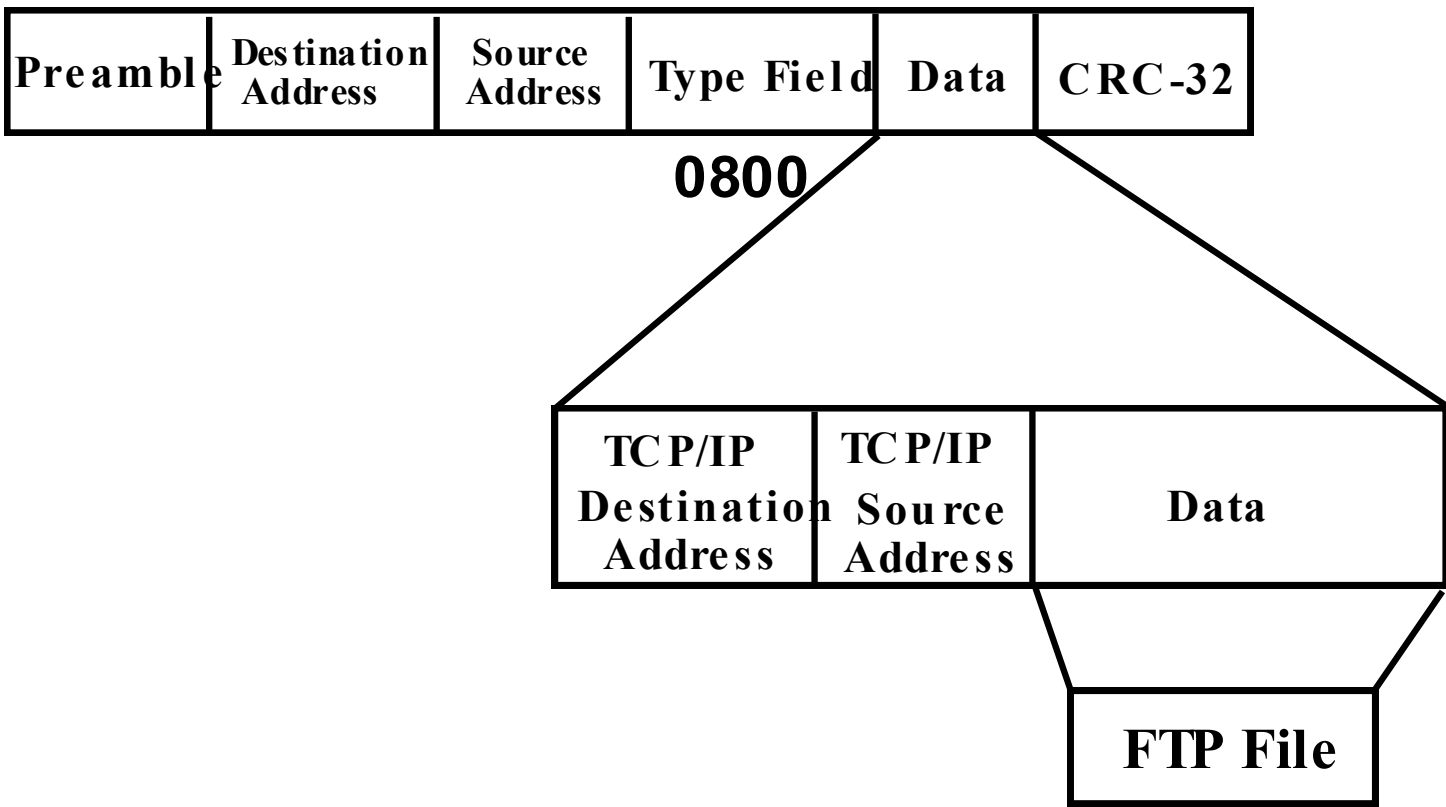
What is job of a router - Interconnect Networks (at TCP/IP Net Layer)

Forward TCP/IP packets between networks

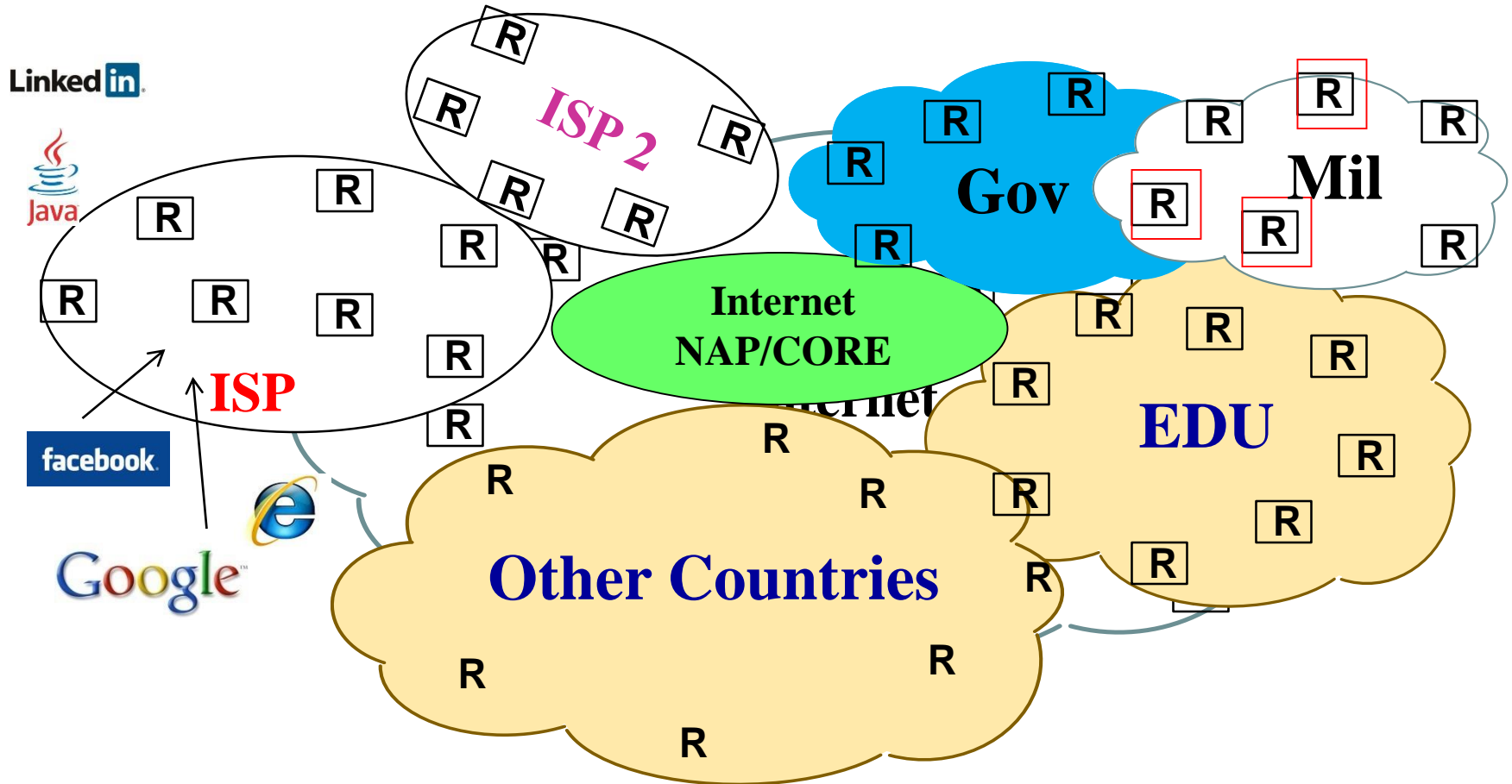
PDU (Protocol Data Unit)

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.



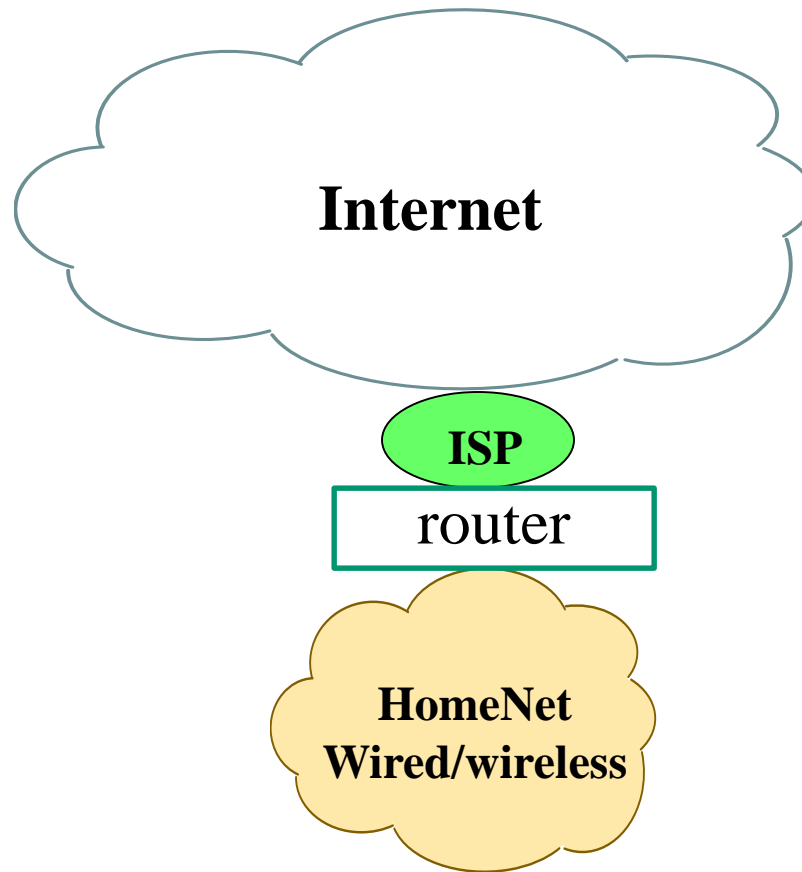
Network Centric



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

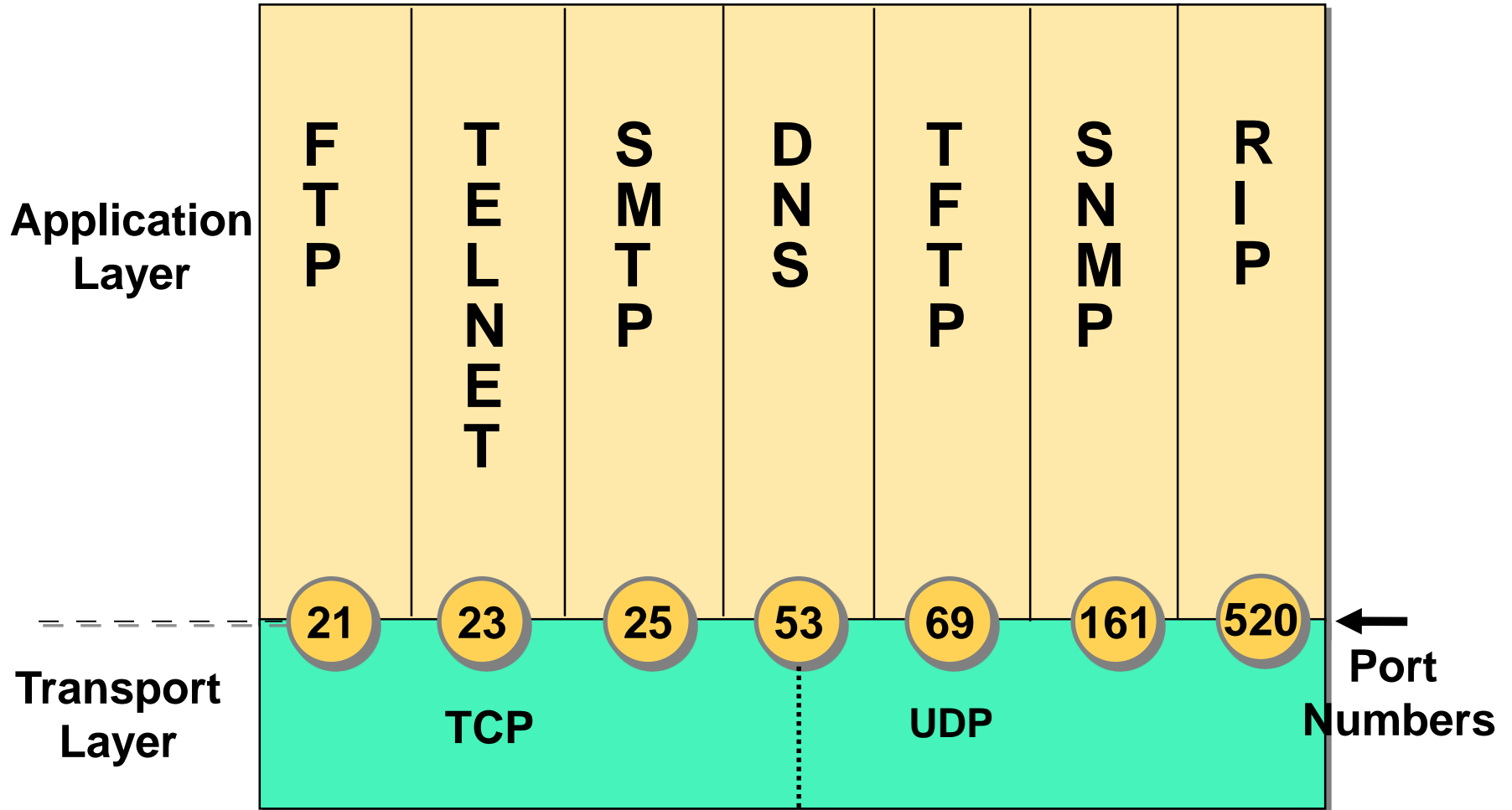
Capturing from Intel(R) 82576LM Gigabit Network Connection (Device\NPF_{56C1D819-3426-46F8-9141-447C3D511287}) [Wireshark 1.8.4 (SVN Rev 46210 from Anish L.S.)]

File Edit View Go Capture Analysis Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4464	105.007163	192.48.21.236	130.42.56.196	TCP	204	31060 > 58701 [PSH, ACK] Seq=23104 Ack=33016 win=8428 Len=150
4465	105.007163	192.48.21.236	130.42.56.196	TCP	60	31060 > 58701 [PSH, ACK] Seq=23254 Ack=33016 win=8428 Len=1
4466	105.007224	130.42.56.196	192.48.21.236	TCP	54	58705 > 31060 [ACK] Seq=33016 Ack=23255 win=16387 Len=0
4467	105.019504	192.48.21.236	130.42.56.196	TCP	204	31060 > 58694 [PSH, ACK] Seq=23557 Ack=33659 win=13140 Len=150
4468	105.019504	192.48.21.236	130.42.56.196	TCP	60	31060 > 58694 [PSH, ACK] Seq=23707 Ack=33659 win=13140 Len=1
4469	105.029536	130.42.56.196	192.48.21.236	TCP	54	58694 > 31060 [ACK] Seq=33659 Ack=23708 win=16236 Len=0
4470	105.029537	130.42.56.196	192.48.21.236	TCP	271	58705 > 31060 [PSH, ACK] Seq=33016 Ack=23255 win=16387 Len=217
4471	105.031970	192.48.21.236	130.42.56.196	TCP	60	31060 > 58701 [ACK] Seq=23255 Ack=33233 win=8428 Len=0
4472	105.040292	130.42.56.196	192.48.21.236	TCP	268	58694 > 31060 [PSH, ACK] Seq=33659 Ack=23708 win=16236 Len=215
4473	105.045038	192.48.21.236	130.42.56.196	TCP	60	31060 > 58694 [ACK] Seq=23708 Ack=33874 win=13140 Len=0
4474	105.106613	Dn13_f0:fc:61	Broadcast	ARP	60	who has 169.254.223.245? Tell 130.42.56.30
4475	105.124644	192.48.21.236	130.42.56.196	TCP	204	31060 > 58705 [PSH, ACK] Seq=21972 Ack=32795 win=8428 Len=150
4476	105.124646	192.48.21.236	130.42.56.196	TCP	60	31060 > 58705 [PSH, ACK] Seq=23122 Ack=32795 win=8428 Len=1
4477	105.124741	130.42.56.196	192.48.21.236	TCP	54	58705 > 31060 [ACK] Seq=32795 Ack=23123 win=16387 Len=0
4478	105.243876	130.42.56.196	192.48.21.236	TCP	271	58795 > 31060 [PSH, ACK] Seq=32795 Ack=23123 win=16387 Len=217
4479	105.294802	fe80::1133:0f01:355f:f02::12		DHCPv6	169	solicit xid: 0x721cfd cid: 000100021a7123400028b9d4e498
4480	105.379481	192.48.21.236	130.42.56.196	TCP	204	31060 > 58691 [PSH, ACK] Seq=23734 Ack=34085 win=14118 Len=150
4481	105.379483	192.48.21.236	130.42.56.196	TCP	60	31060 > 58691 [PSH, ACK] Seq=23884 Ack=34085 win=14118 Len=1
4482	105.379583	130.42.56.196	192.48.21.236	TCP	54	58691 > 31060 [ACK] Seq=34085 Ack=23885 win=16425 Len=0
4483	105.455947	192.48.21.236	130.42.56.196	TCP	204	31060 > 58693 [PSH, ACK] Seq=23497 Ack=34093 win=13214 Len=150
4484	105.455948	192.48.21.236	130.42.56.196	TCP	60	31060 > 58693 [PSH, ACK] Seq=24067 Ack=34093 win=13214 Len=1
4485	105.456039	130.42.56.196	192.48.21.236	TCP	54	58693 > 31060 [ACK] Seq=34093 Ack=24068 win=16331 Len=0
4486	105.543619	130.42.56.196	192.48.21.236	TCP	269	58693 > 31060 [PSH, ACK] Seq=34085 Ack=23885 win=16425 Len=215
4487	105.548409	192.48.21.236	130.42.56.196	TCP	60	31060 > 58691 [ACK] Seq=23885 Ack=34300 win=14118 Len=0
4488	105.559568	130.42.56.196	192.48.21.236	TCP	268	58693 > 31060 [PSH, ACK] Seq=34093 Ack=34068 win=16331 Len=213
4489	105.564254	192.48.21.236	130.42.56.196	TCP	60	31060 > 58693 [ACK] Seq=24068 Ack=34308 win=13214 Len=0
4490	105.593330	192.48.21.236	130.42.56.196	TCP	204	31060 > 58701 [PSH, ACK] Seq=23255 Ack=33233 win=8428 Len=150
4491	105.593331	192.48.21.236	130.42.56.196	TCP	60	31060 > 58701 [PSH, ACK] Seq=23405 Ack=33233 win=8428 Len=1
4492	105.593383	130.42.56.196	192.48.21.236	TCP	54	58705 > 31060 [ACK] Seq=33211 Ack=23408 win=16389 Len=0
4493	105.604663	130.42.56.196	192.48.21.236	TCP	271	[TCP Reset/Transmission] 58705 > 31060 [PSH, ACK] Seq=32795 Ack=23123 win=16387 Len=217
4494	105.834324	192.48.21.236	130.42.56.196	TCP	204	31060 > 58694 [PSH, ACK] Seq=23708 Ack=33874 win=13140 Len=150
4495	105.834326	192.48.21.236	130.42.56.196	TCP	60	31060 > 58694 [PSH, ACK] Seq=23858 Ack=33874 win=13140 Len=1
4496	105.834391	130.42.56.196	192.48.21.236	TCP	54	58694 > 31060 [ACK] Seq=33874 Ack=23859 win=16198 Len=0
4497	105.848184	130.42.56.196	192.48.21.236	TCP	268	58705 > 31060 [PSH, ACK] Seq=33233 Ack=23408 win=16349 Len=215

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

Default

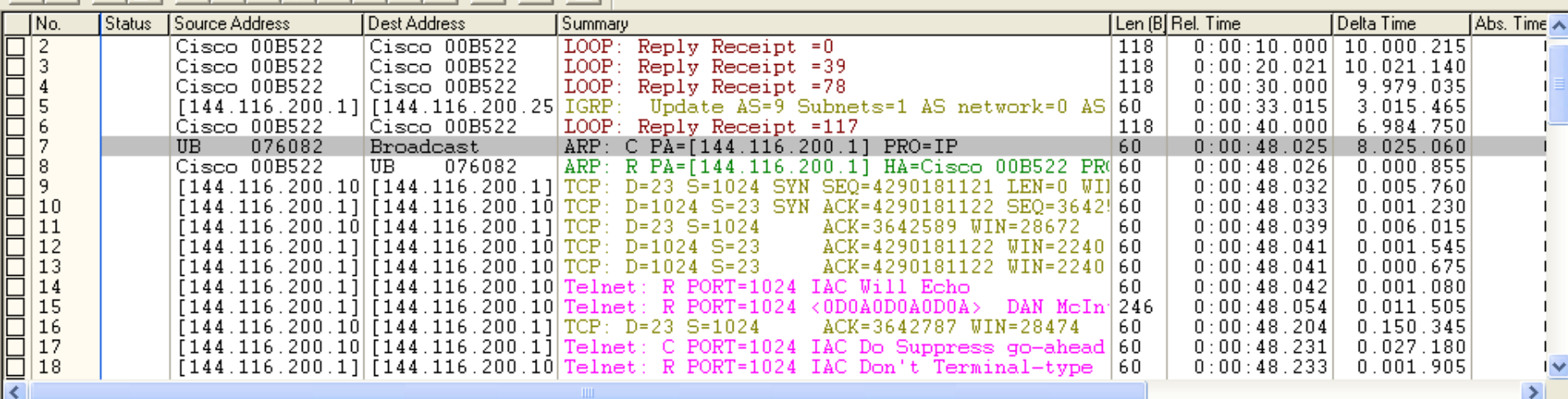
No.	Status	Source Address	Dest Address	Summary	Len [B]	Rel. Time	Delta Time	Abs. Time
2		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =0	118	0:00:10.000	10.000.215	
3		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =39	118	0:00:20.021	10.021.140	
4		Cisco 00B522	Cisco 00B522	LOOP: Reply Receipt =78	118	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 PRO	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 WIN	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  ..N1.±E@}.....ô
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  ....qqc?.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
  
```



```

DLC:
DLC: Frame 7 arrived at 10:55:45.0257; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFF, 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

```

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

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 PRO	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=28672	60	0:00:48.041	0.001.545	

TCP: ----- TCP header -----

- 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: 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  ....p".Y...E.
00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74  ..Où...}tEkIt
00000020: 08 01 04 00 00 17 ff b6 f8 01 00 00 00 00 60 02  ..

```


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 PRO	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=28672	60	0:00:48.041	0.001.545	

TCP: ----- TCP header -----

- 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: 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 00p".Y...E.
 00000010: 00 2c d3 f9 00 00 1e 06 17 7d 90 74 c8 6b 90 74 ...Où...}tEkIt
 00000020: 08 01 04 00 00 17 ff b6 f8 01 00 00 00 00 60 02 ...

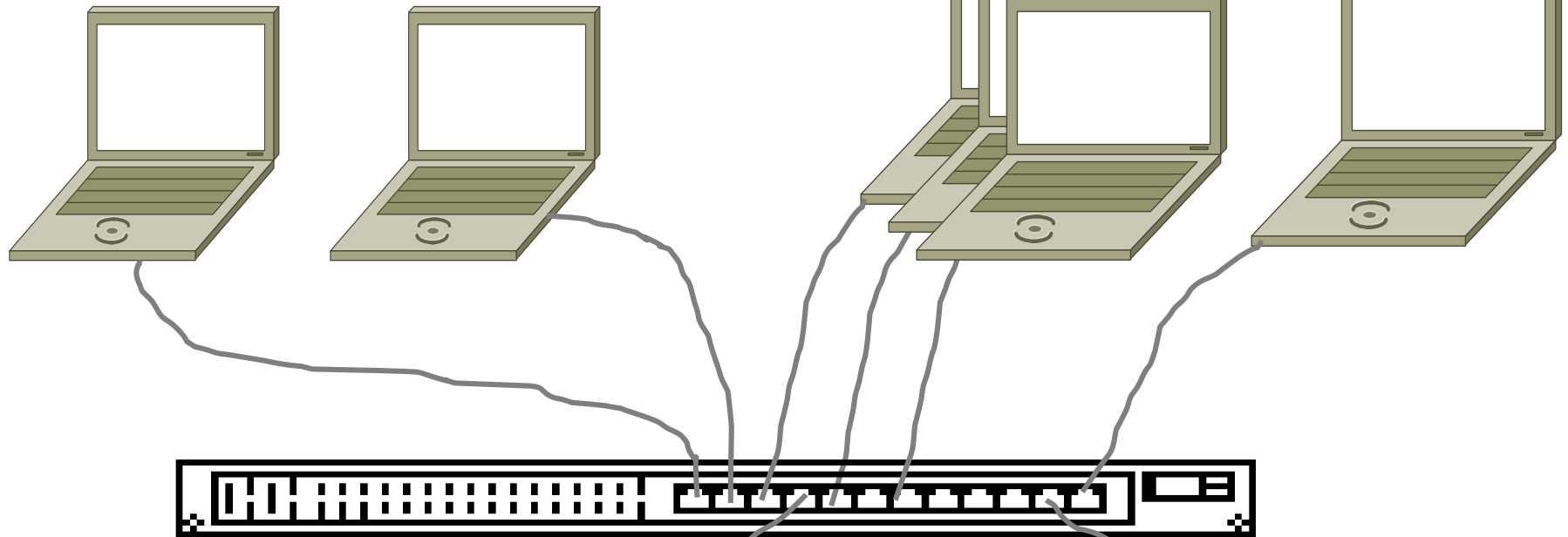
VLANs (Virtual LANs)

**Supplier/Vendor
Contractor**

You

Work Peers

Visitor/Guest



Ethernet Frame Protocol Decodes

A screenshot of a Wireshark packet capture showing the details of an Ethernet frame. The packet list on the left shows several frames, with the selected frame being a standard Ethernet II frame. The packet details pane on the right shows the frame structure: Ethernet II (Type II), Internet Protocol Version 4, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the frame.

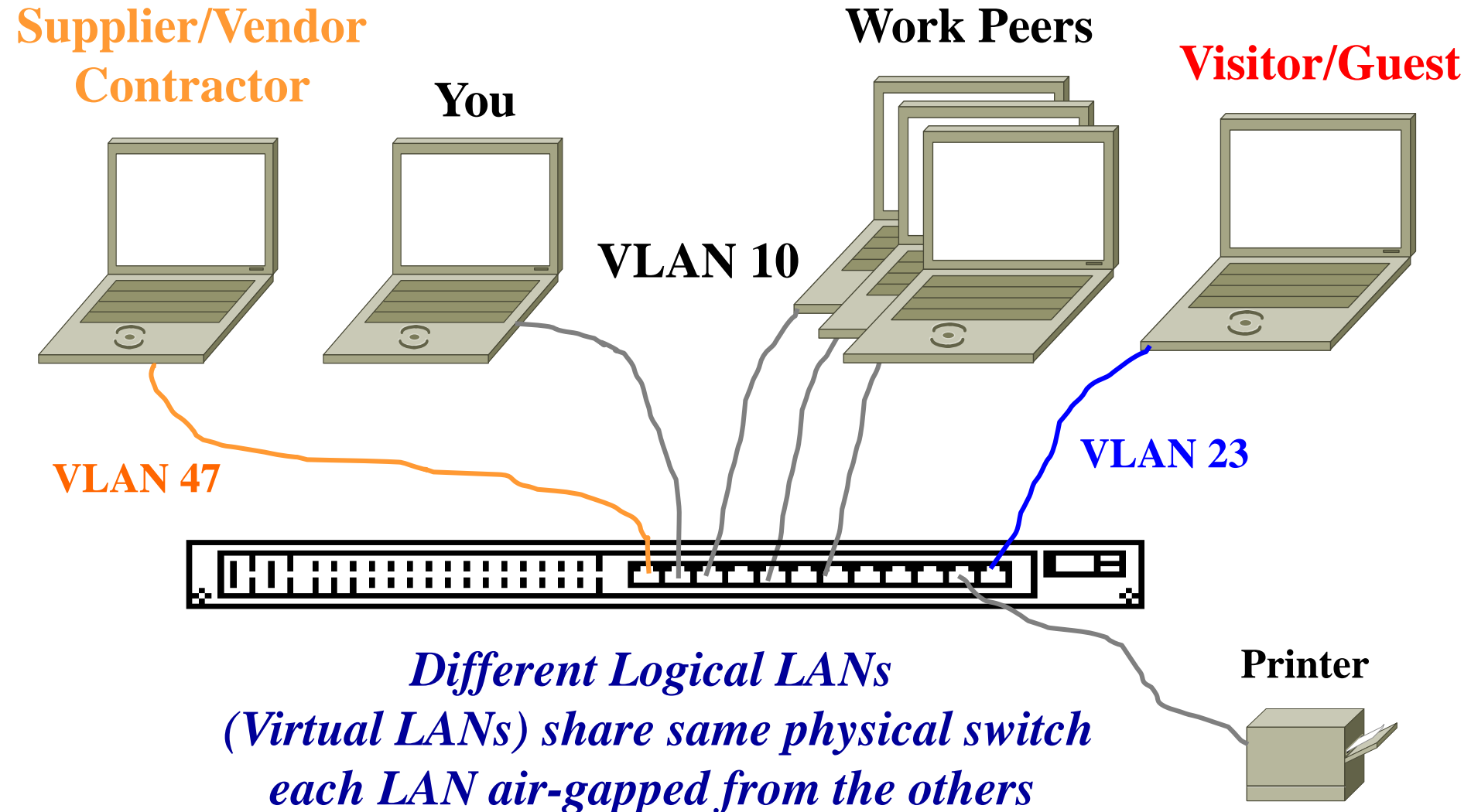
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	Ethernet II (Type II)	1440	Standard Ethernet frame
2	0.000000	192.168.1.1	192.168.1.100	Internet Protocol Version 4	60	Standard IP packet
3	0.000000	192.168.1.1	192.168.1.100	Hypertext Transfer Protocol	1380	Standard HTTP request

Shared Ethernet LAN

**Eavesdropping
(Man-in-middle)**

Printer

VLANs (Virtual LANs)



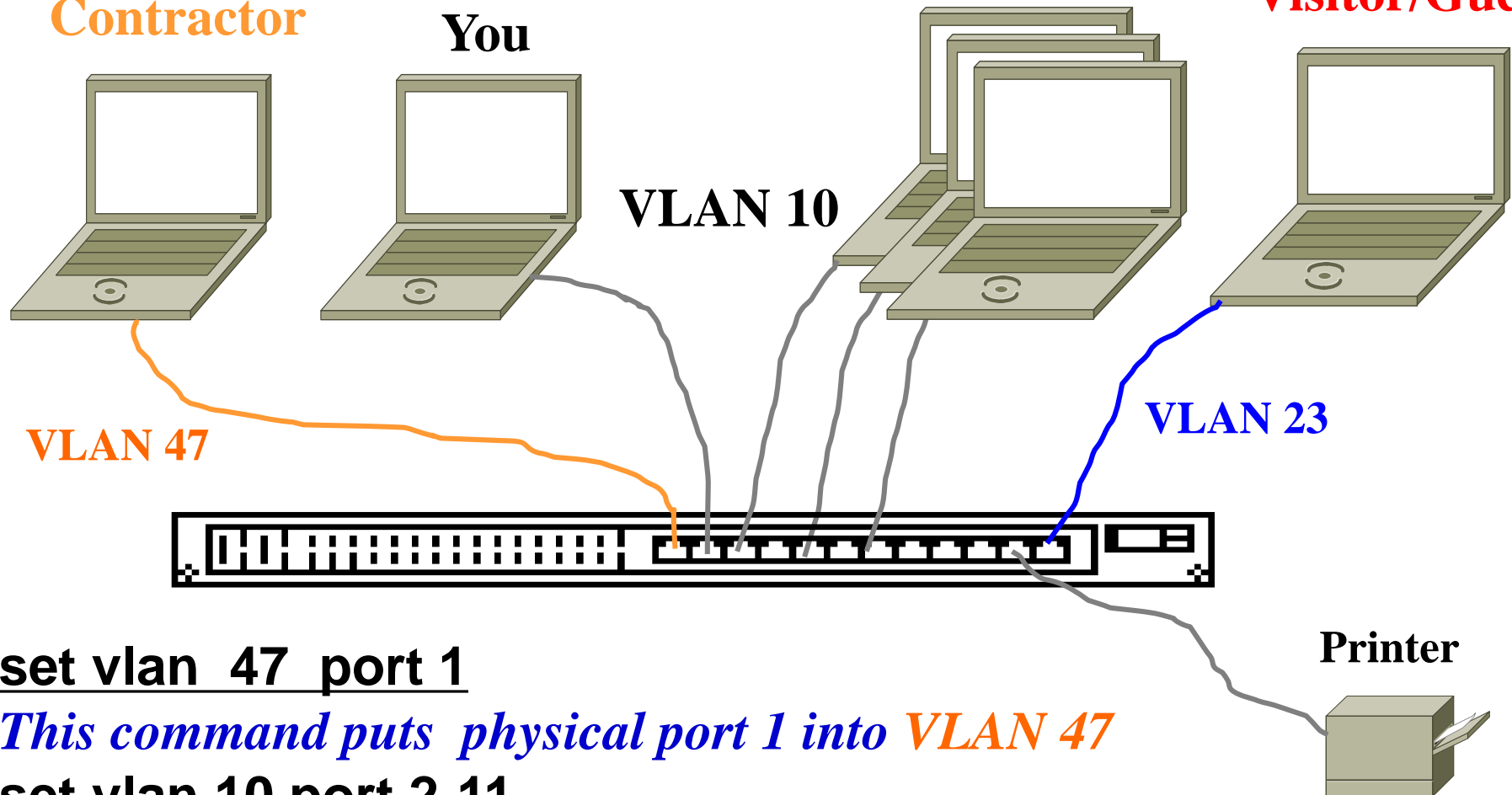
VLANs (Virtual LANs)

Supplier/Vendor
Contractor

You

Work Peers

Visitor/Guest



set vlan 47 port 1

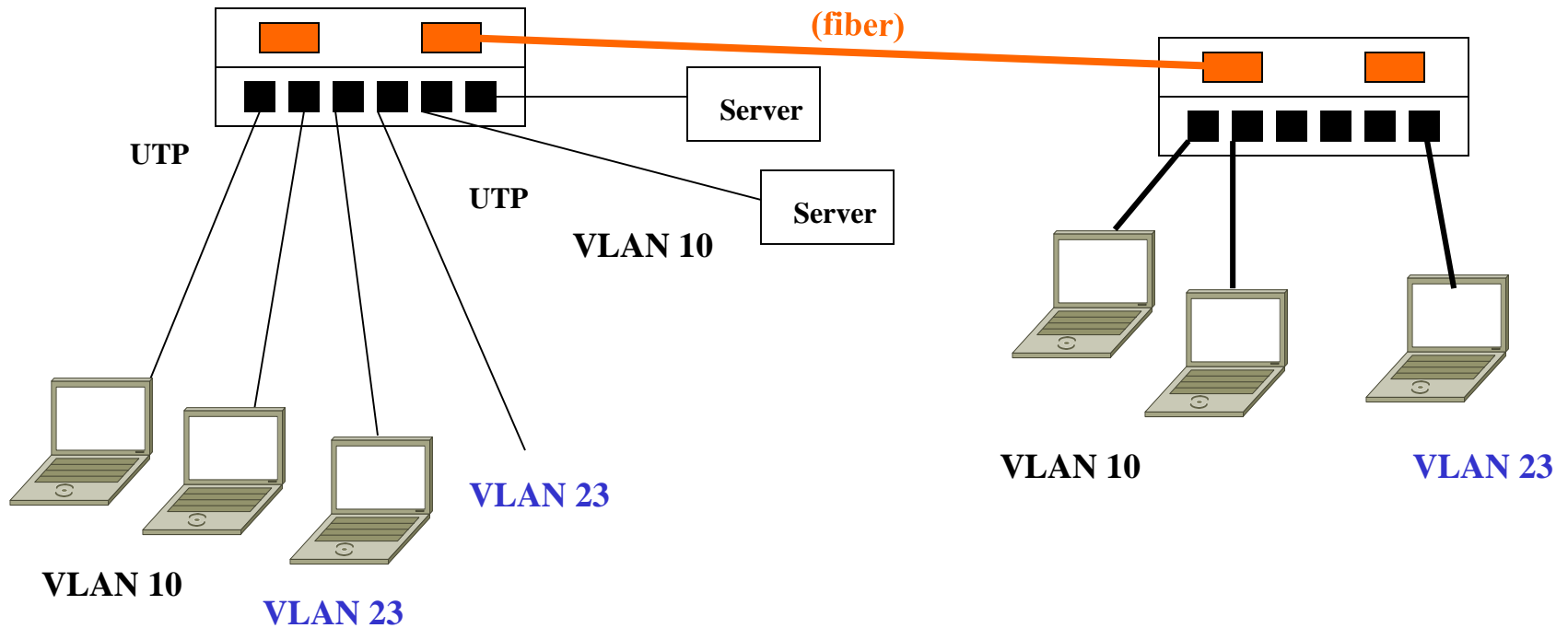
This command puts physical port 1 into VLAN 47

set vlan 10 port 2-11

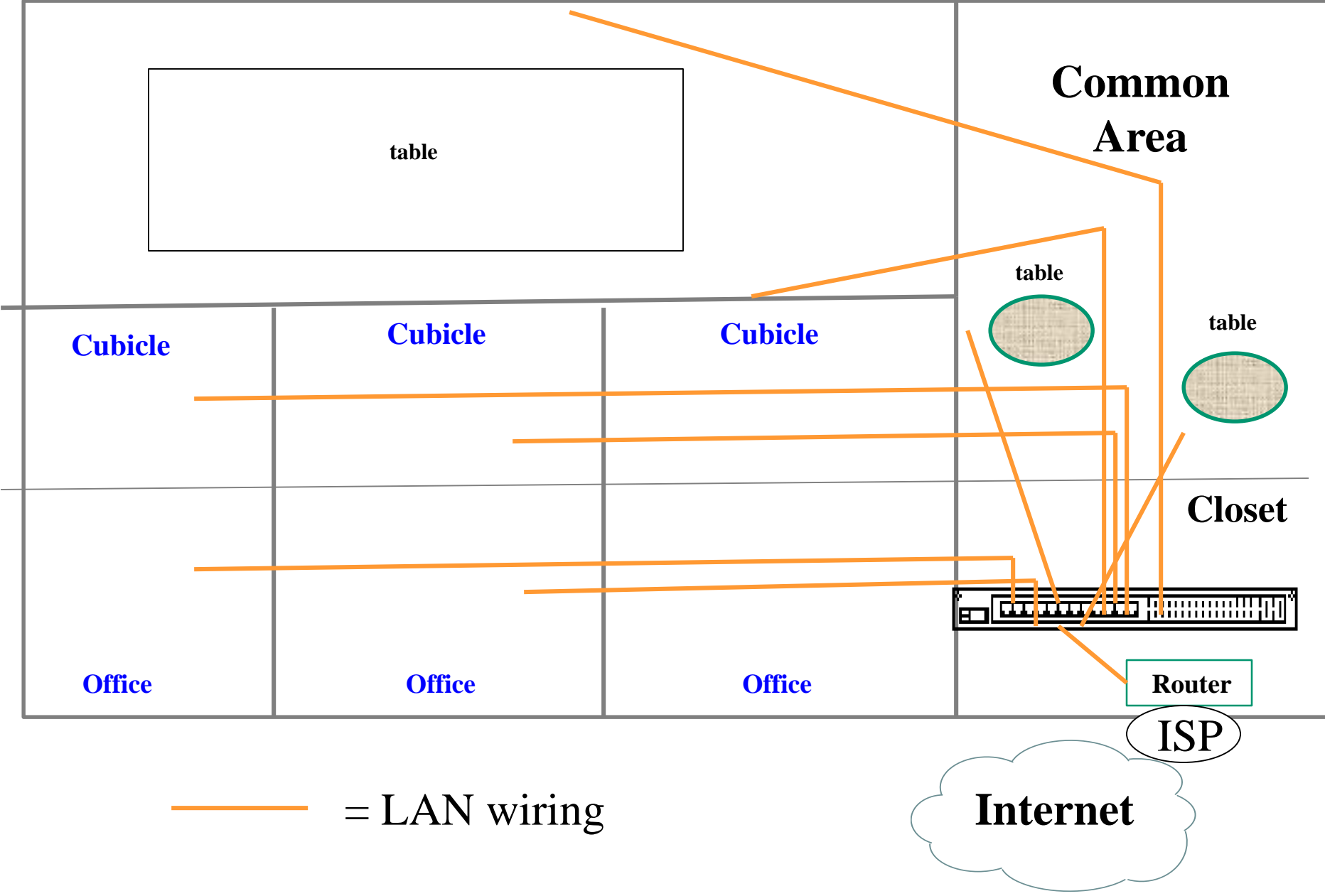
This would put physical ports 2 thru 11 into VLAN 10

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

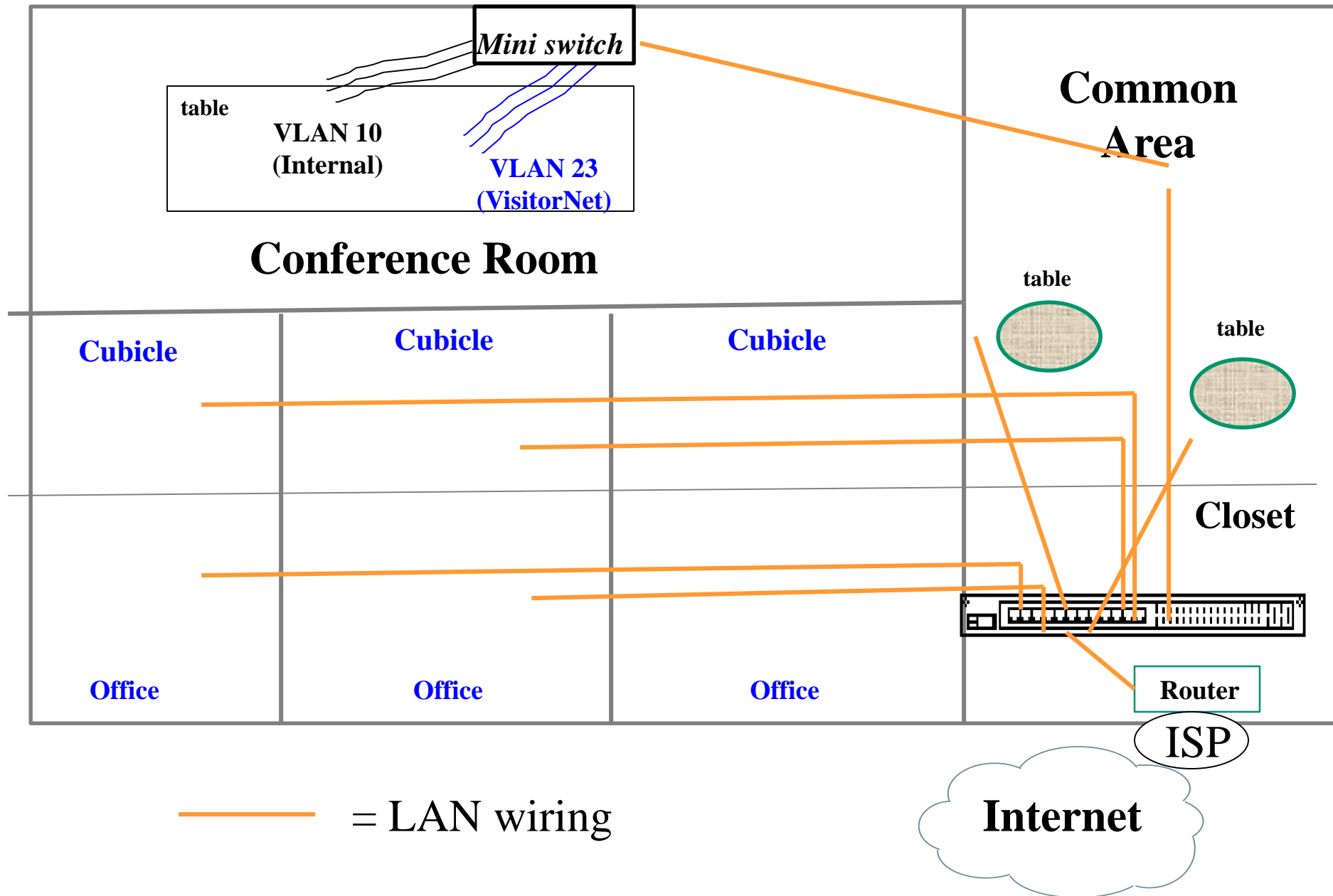
Interconnected LAN Switches



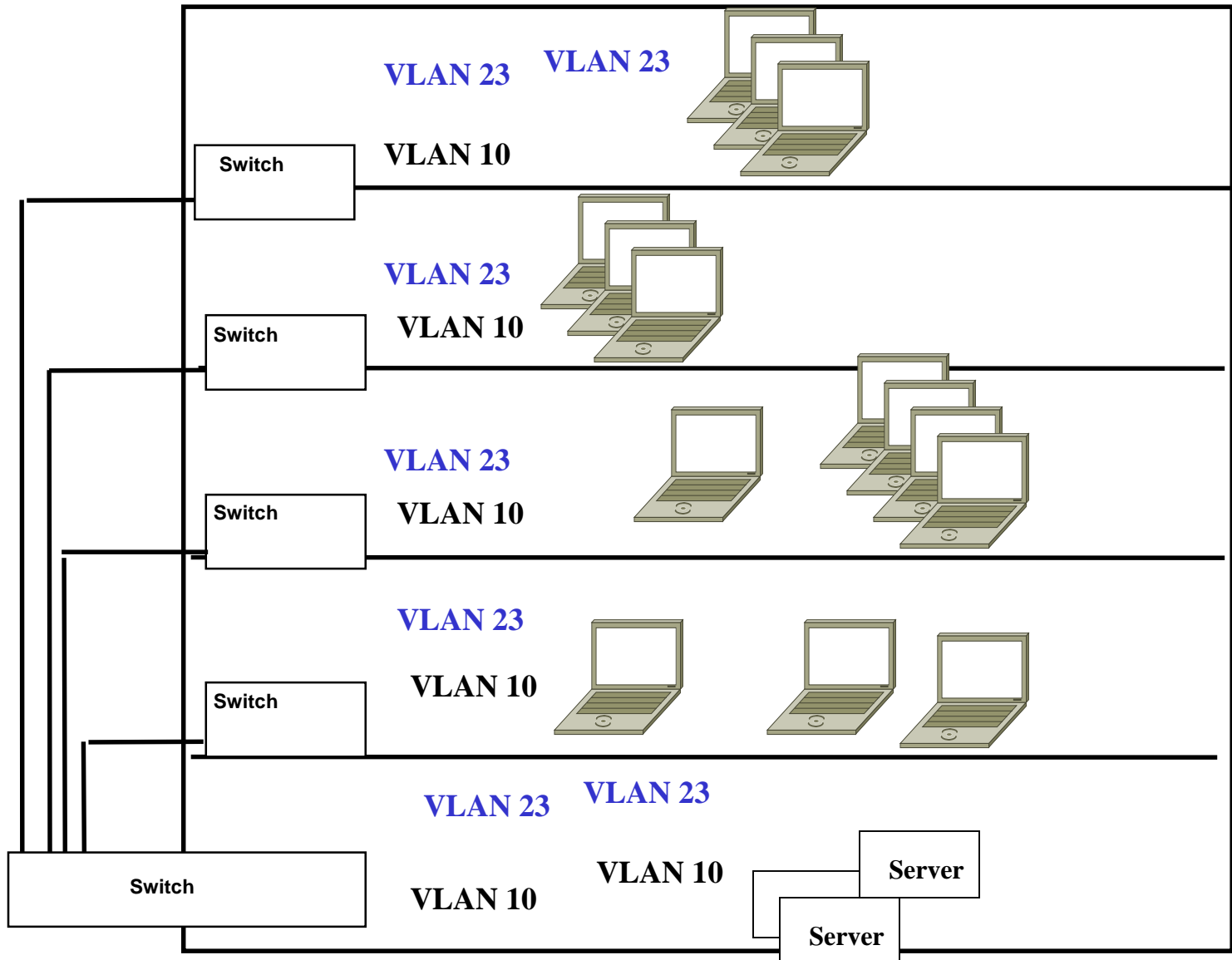
Workplace



Workplace



Office Environment



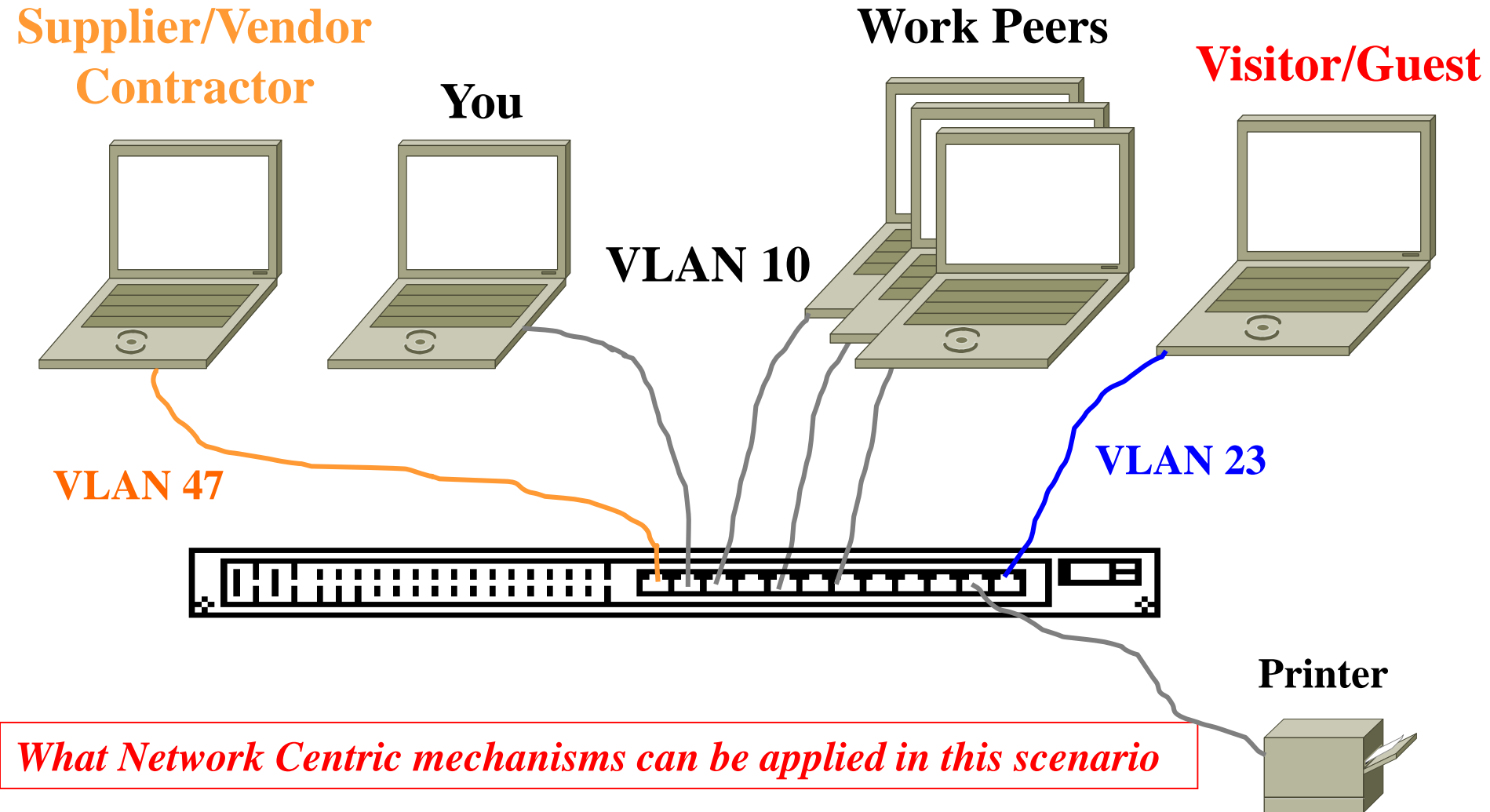
What is the name of the technology that allows multiple VLANs to run over a single cable (between LAN Switches) ?

VLAN Trunking

Are VLANs a Security Mechanism ?

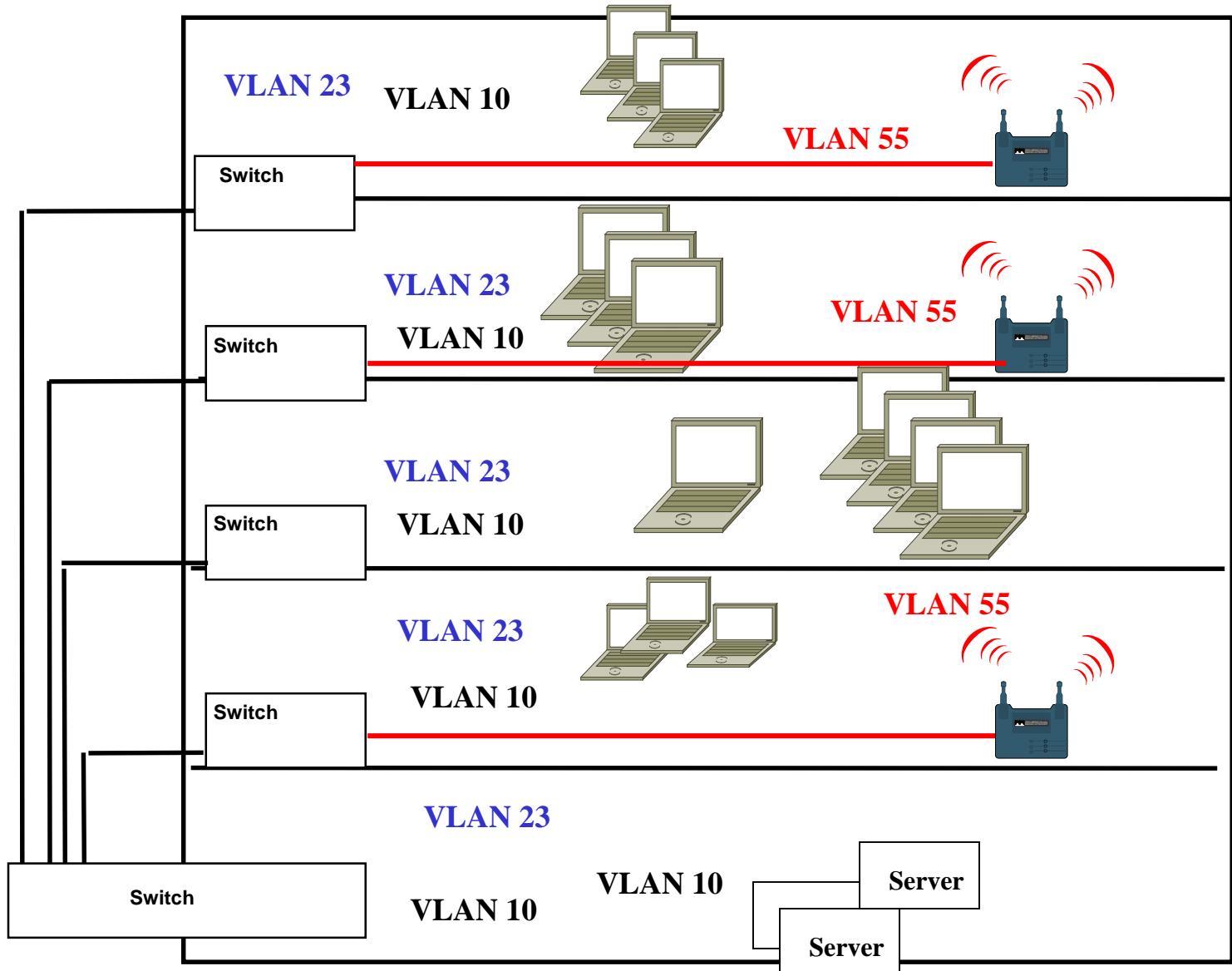
Yes, VLANs allow separation of LAN traffic based on user need (princ of least priv)

Protection Mechanisms

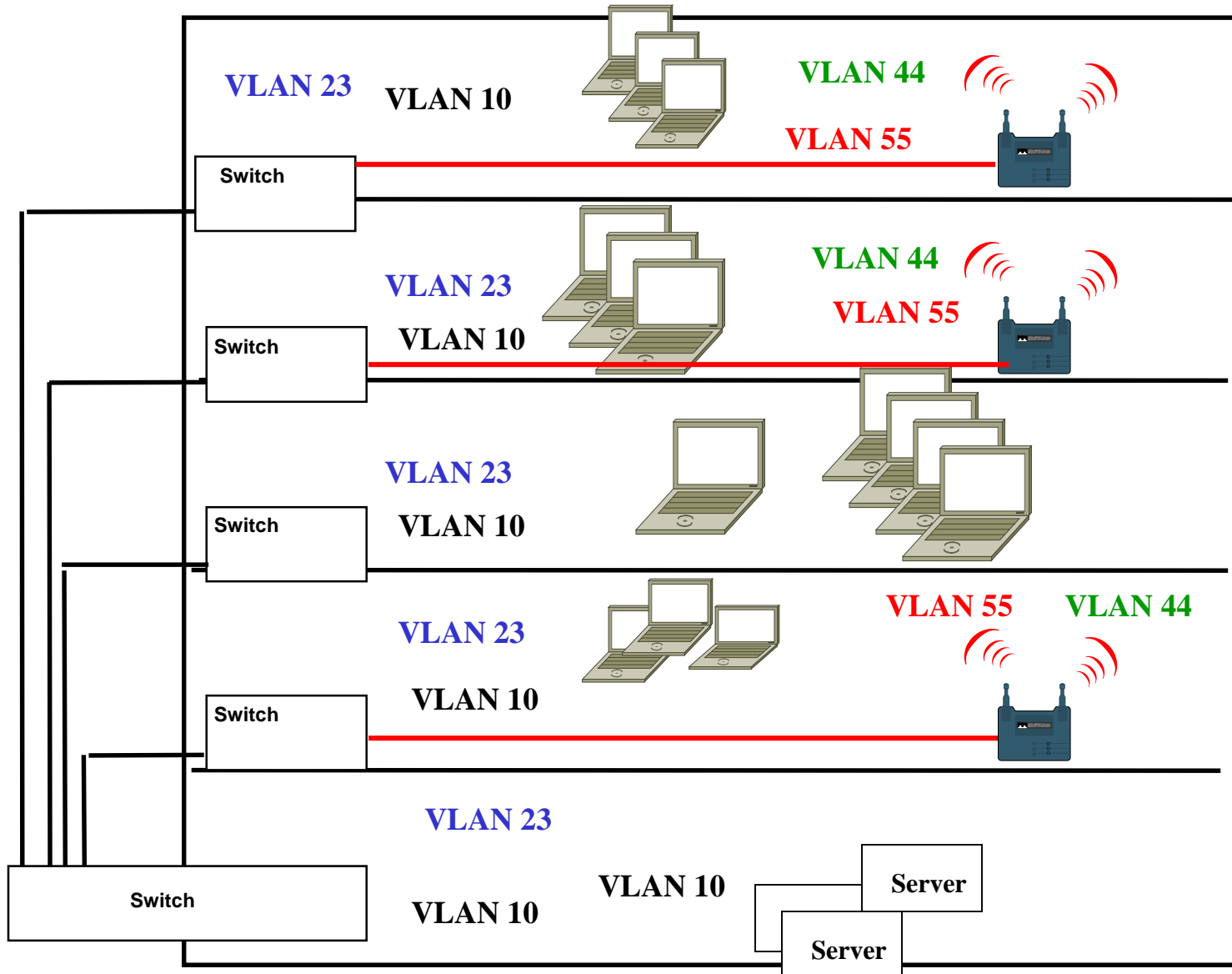


What Data Centric mechanisms can be applied in this scenario

Office Environment



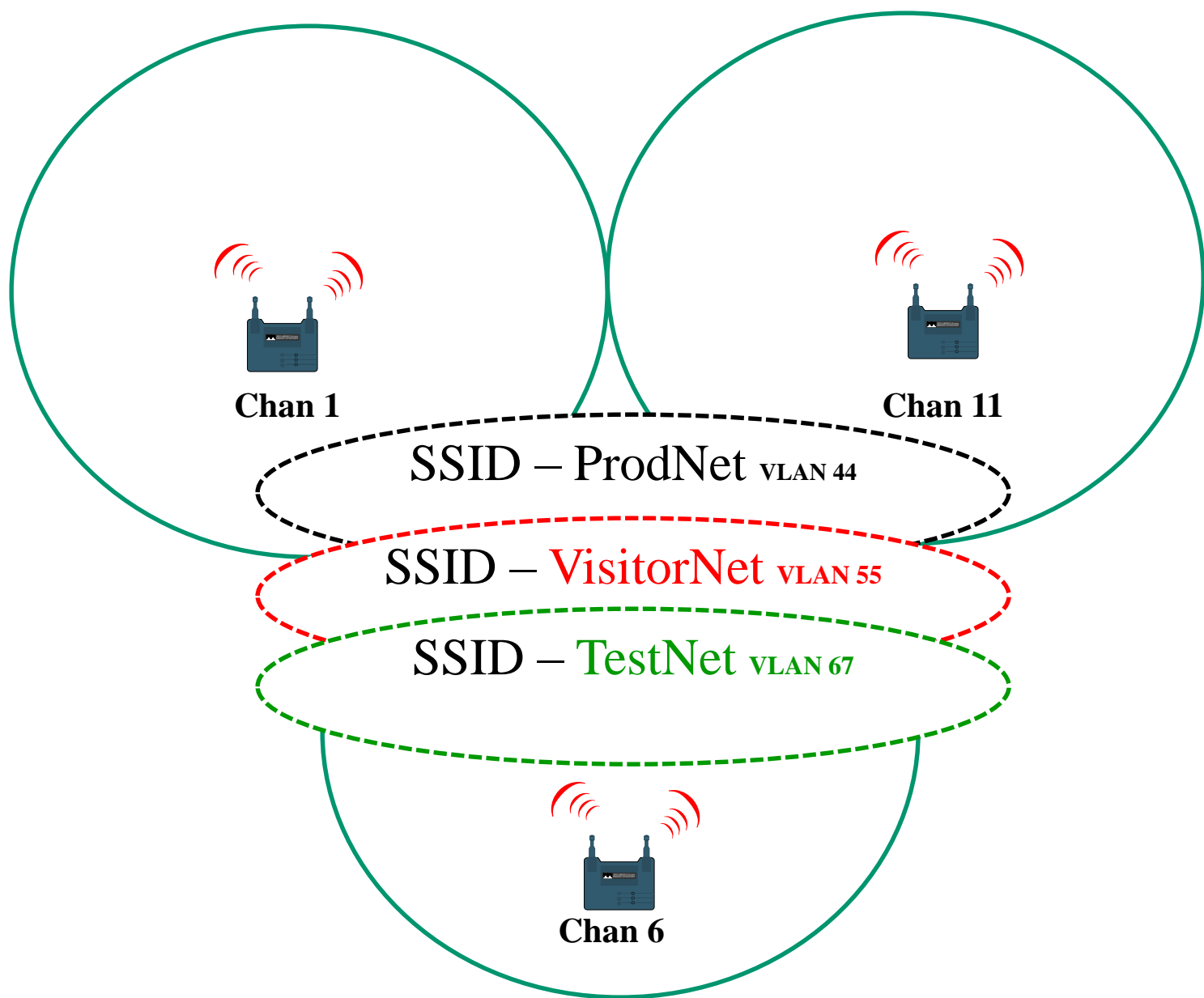
Office Environment



Wireless LAN Channel Reuse Patterns



IEEE 802.11b/g 3 Channel Reuse Pattern



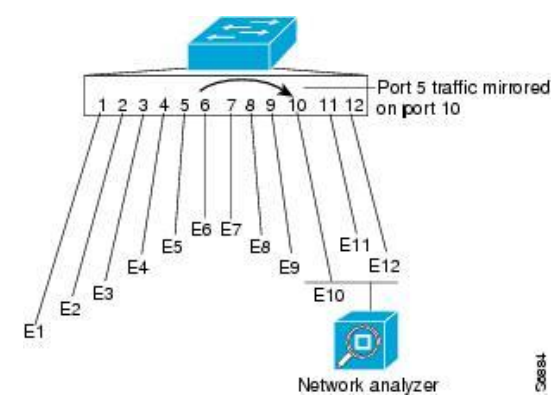
What separates access to the different WLAN SSID's ??

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

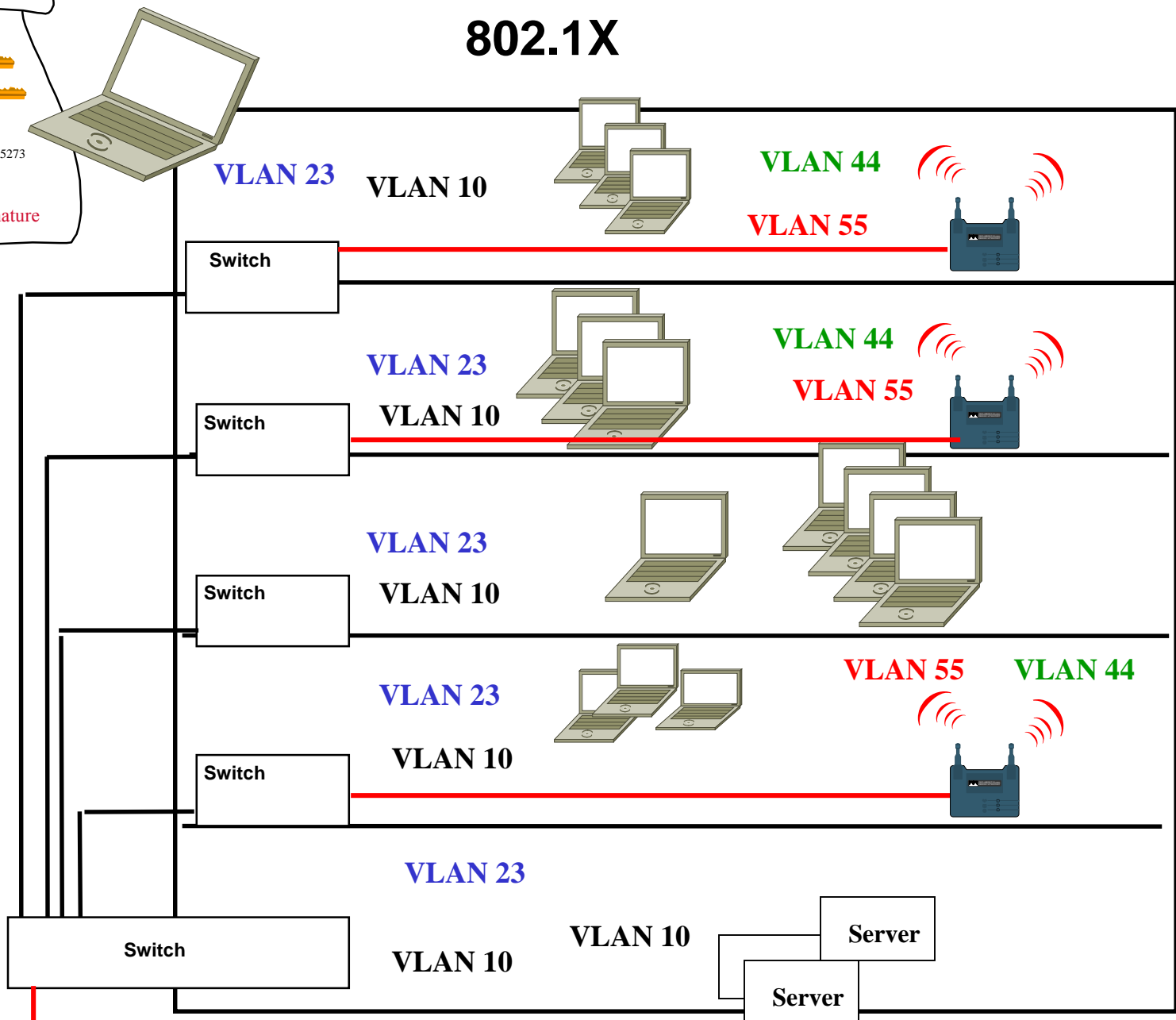
IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

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

What Does it *REALLY* do ?

Name: " "
Key-Exchange Key: 
Signature Key: 
Serial #: 29483756
Other Data: 10236283025273
Expires: 6/18/96
Signed: CA's Signature

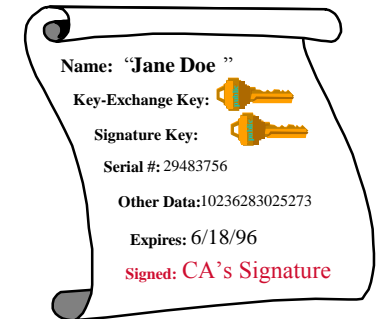
802.1X



Authentication Server/Mgr validates key, device gets IP add

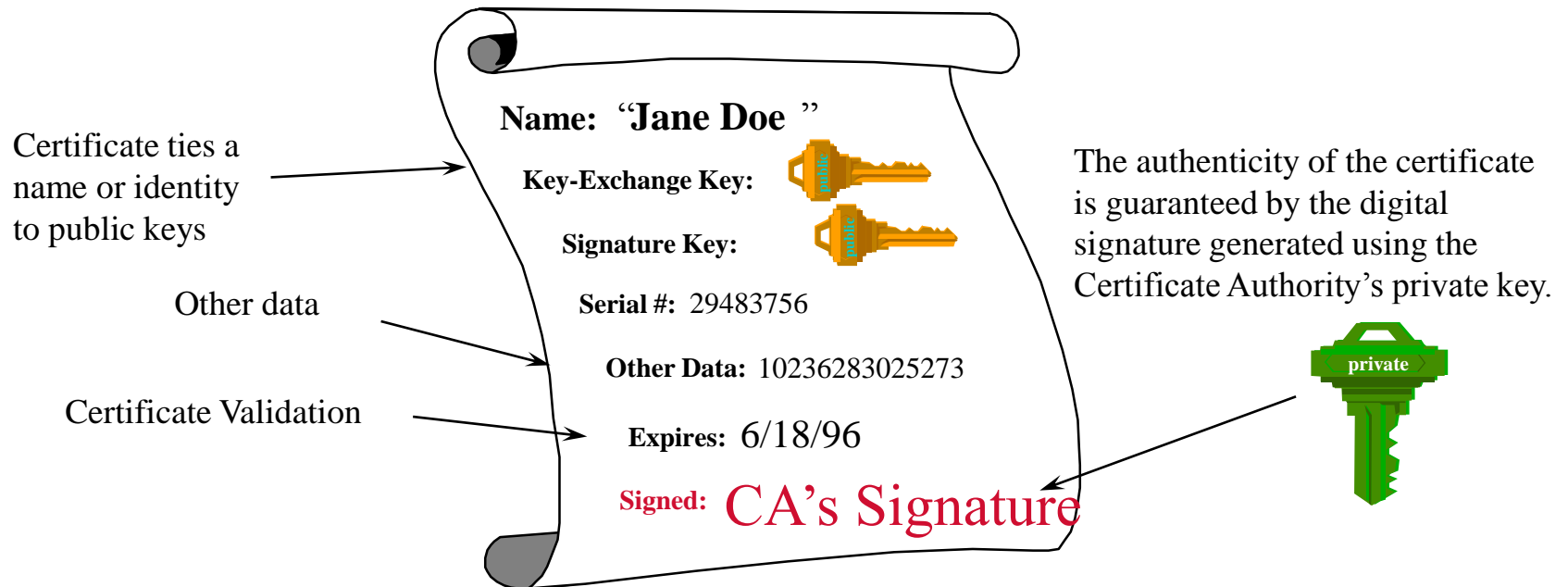
What is a Certificate?

- 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



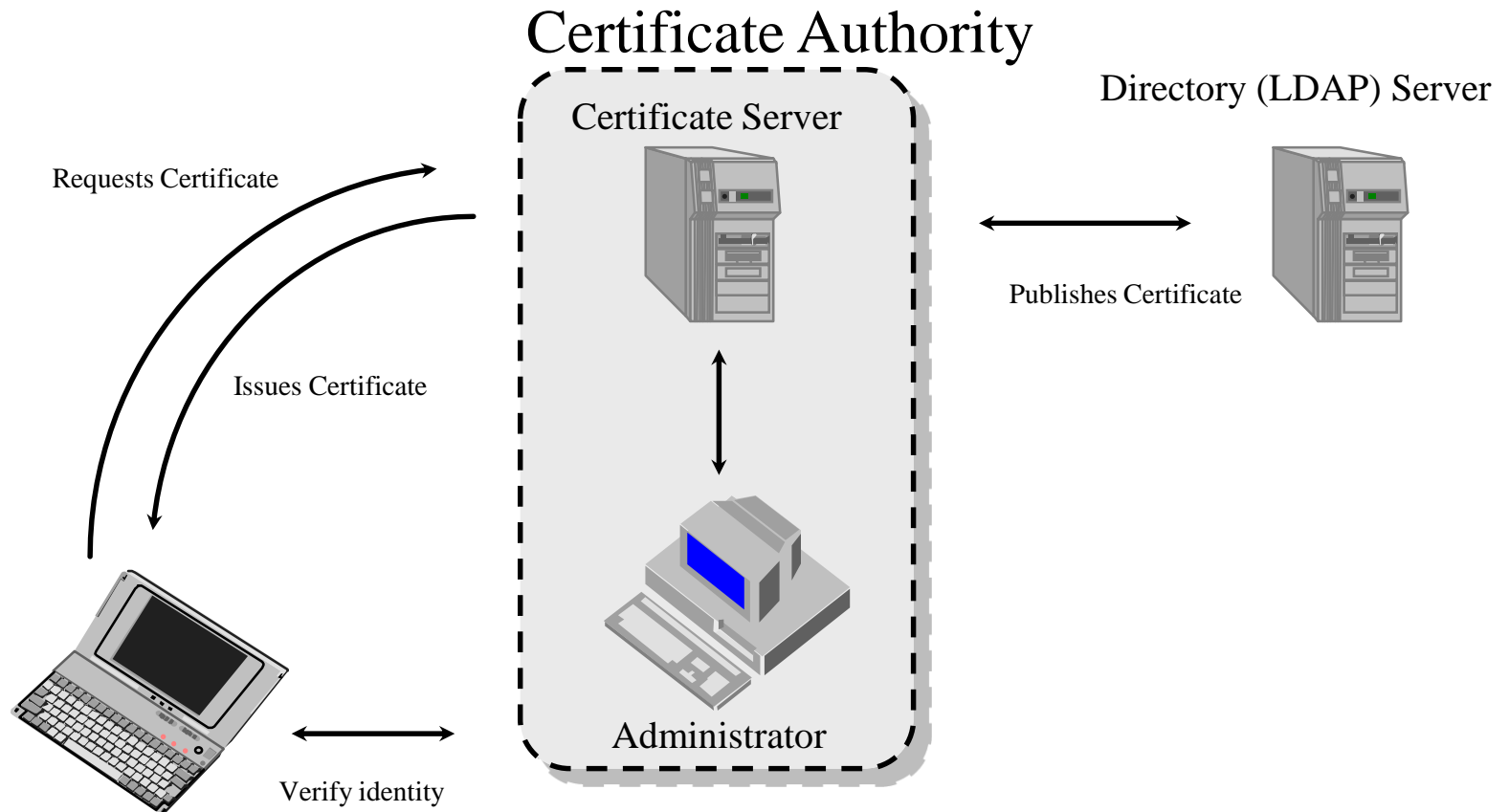
What Is a Certification Authority?

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

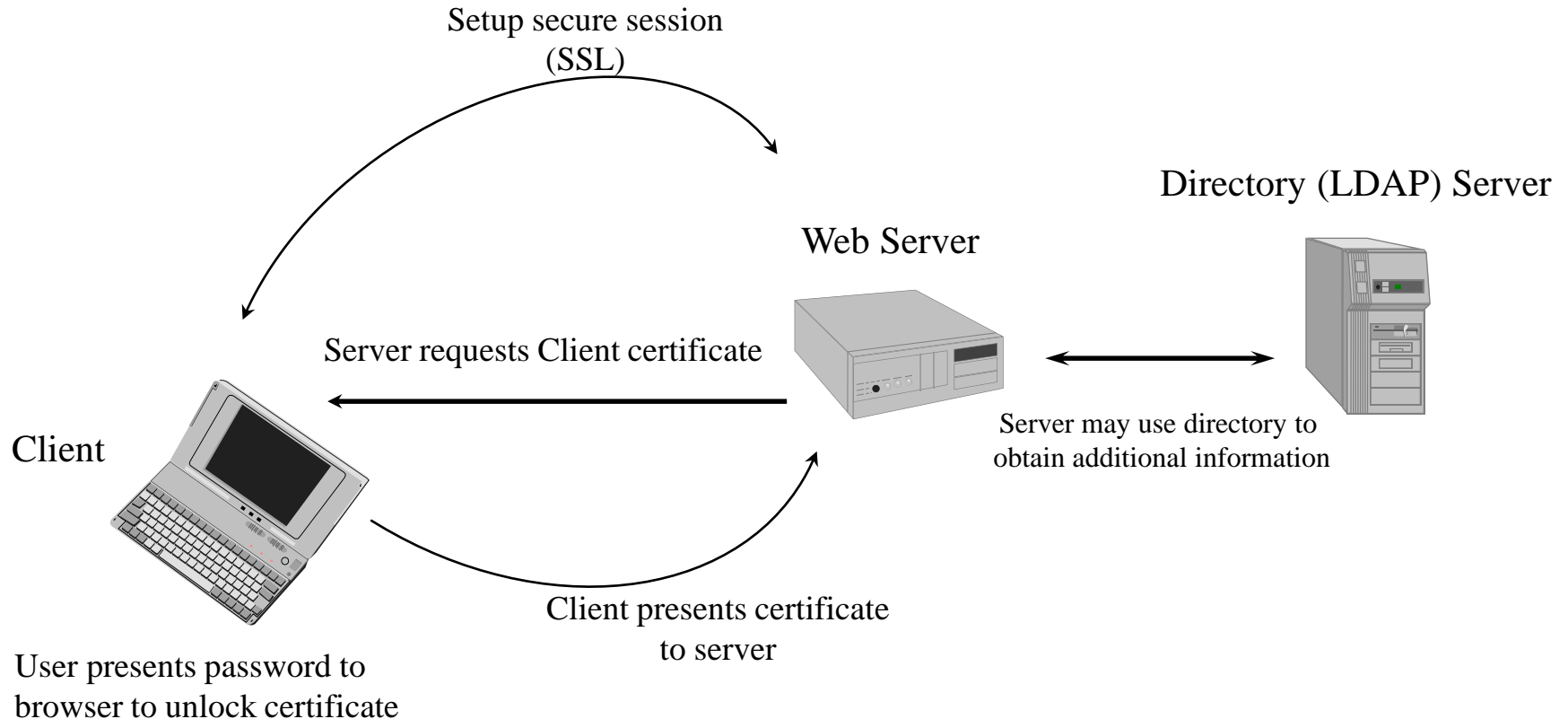
Primary responsibility of the Certificate Authority is to assure the identity of the person receiving the certificate.

The Authority is also responsible for revoking certificates.

Obtaining a Client Certificate



How to Use a Certificate



EAP Transaction

