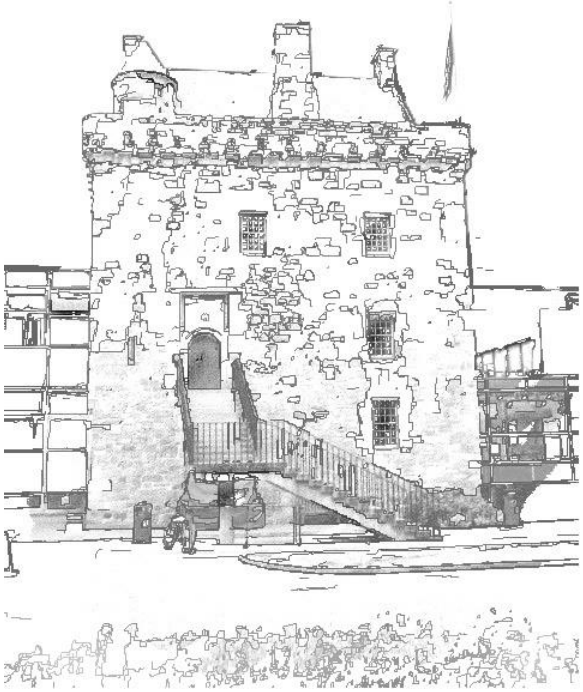
Wireless LAN

Unit 3: Wireless Infrastructure



Edinburgh Napier UNIVERSITY

Author: Bill Buchanan

Areas covered:

Wireless Infrastructures.

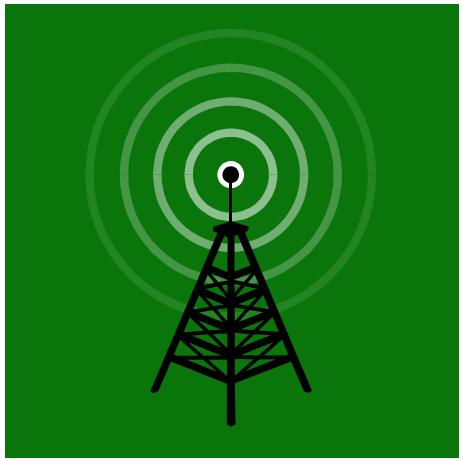
Basic details on bridging and topologies.

Wireless Data Logging and Device Discovery.

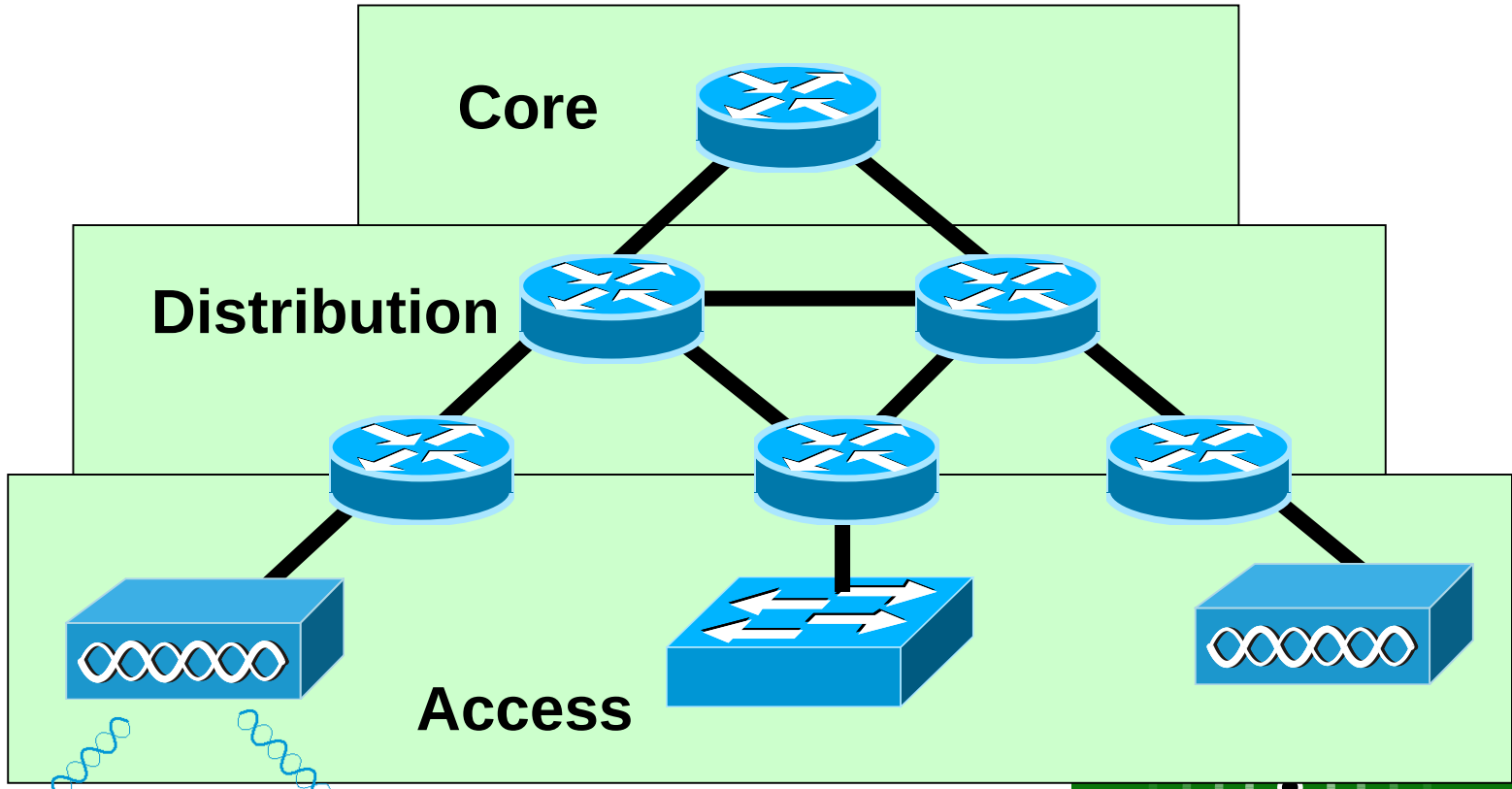
Details on protocols such as SNMP

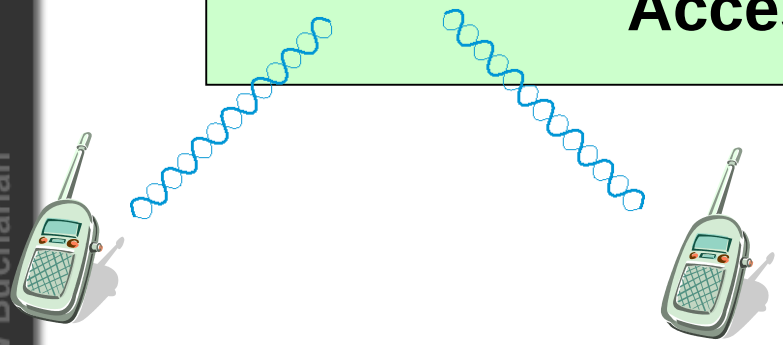
Wireless LAN

Wireless Infrastructures

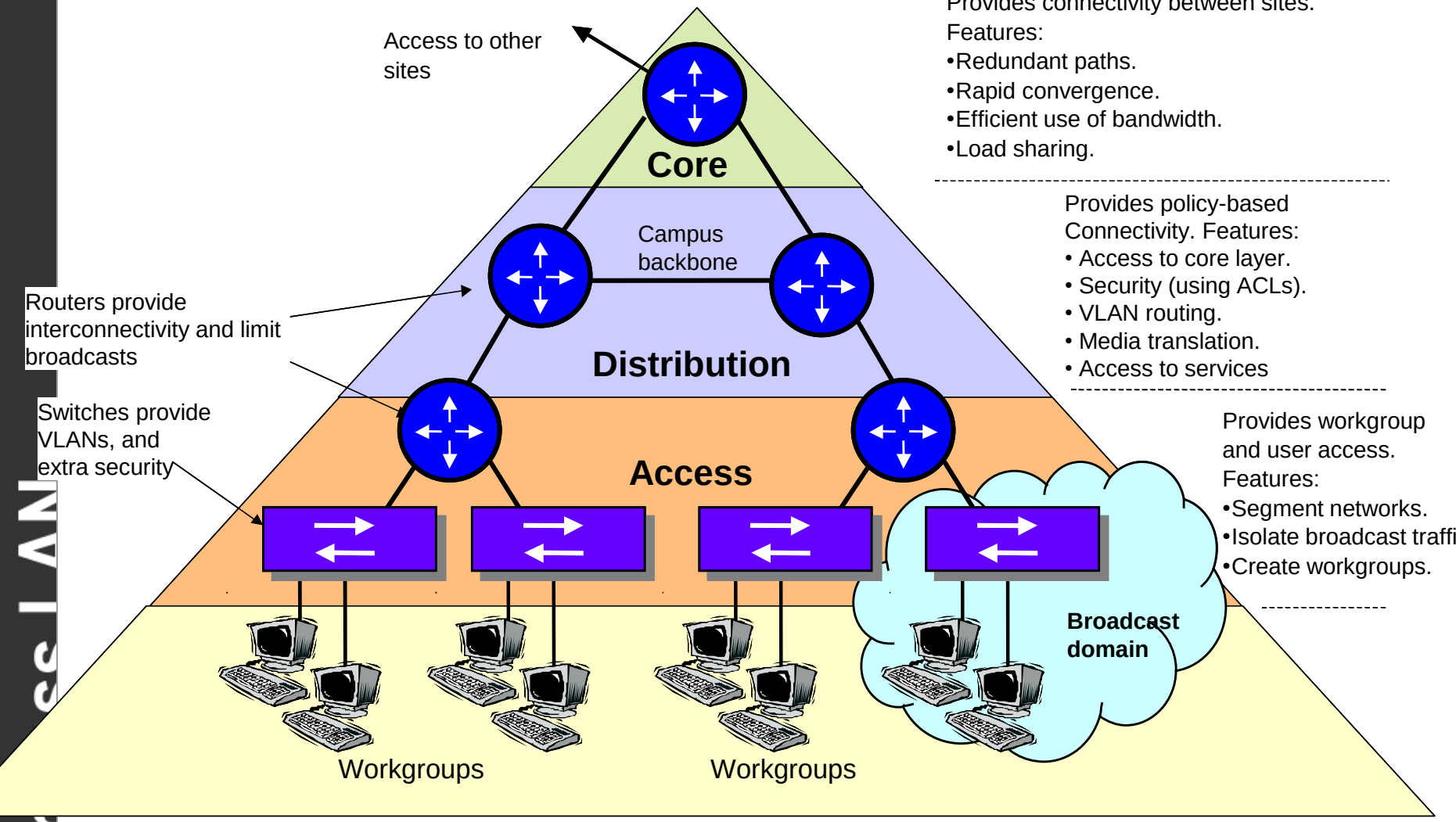


Edinburgh Napier UNIVERSITY
Author: Bill Buchanan


Core
Distribution
Access



Three-layered model



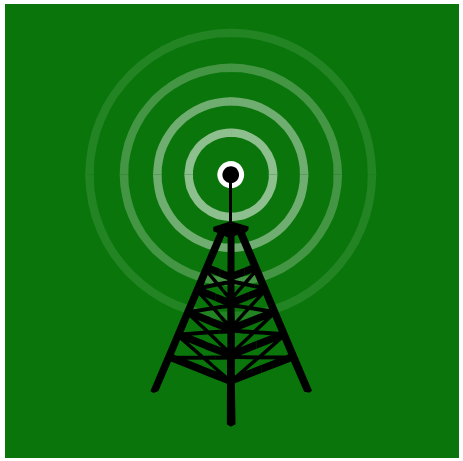
Provides connectivity between sites.
Features:
- Redundant paths.
- Rapid convergence.
- Efficient use of bandwidth.
- Load sharing.

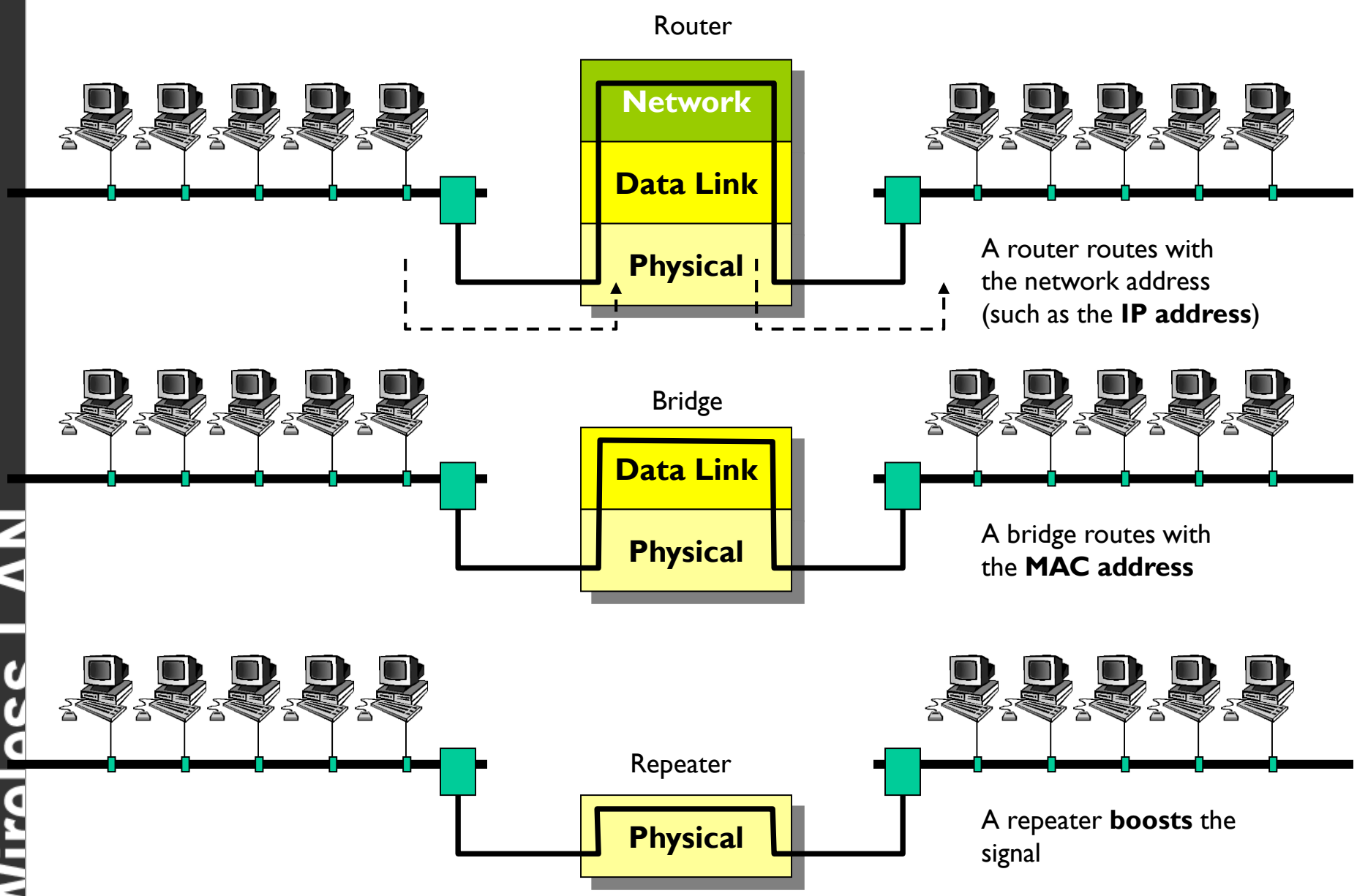
Provides policy-based Connectivity. Features:
- Access to core layer.
- Security (using ACLs).
- VLAN routing.
- Media translation.
- Access to services

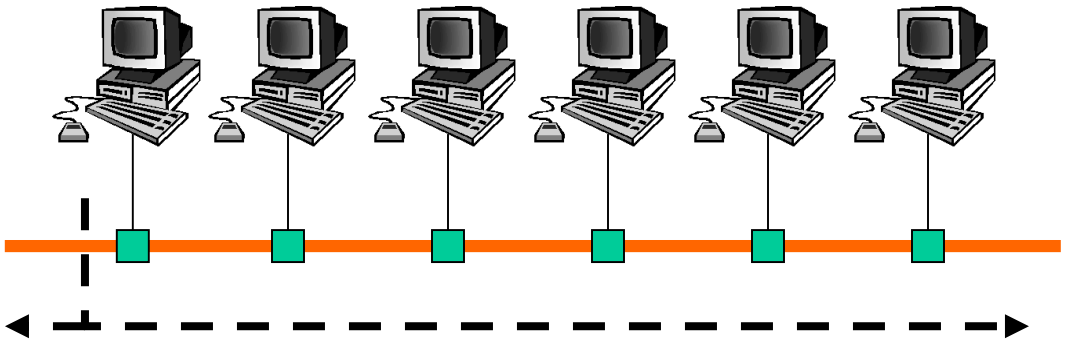
Provides workgroup and user access.
Features:
- Segment networks.
- Isolate broadcast traffic.
- Create workgroups.

Wireless LAN

Root or repeater

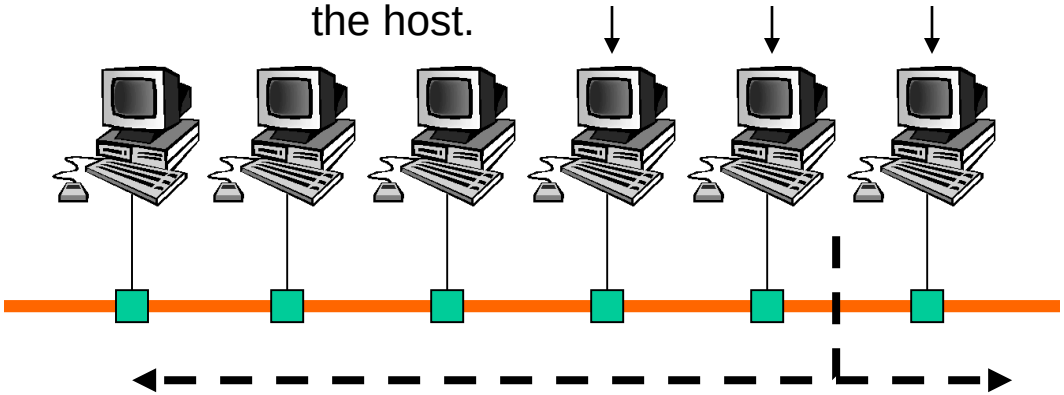



Router
Network
Data Link
Physical
A router routes with the network address (such as the **IP address**)
Bridge
Data Link
Physical
A bridge routes with the **MAC address**
Repeater
Physical
A repeater **boosts** the signal

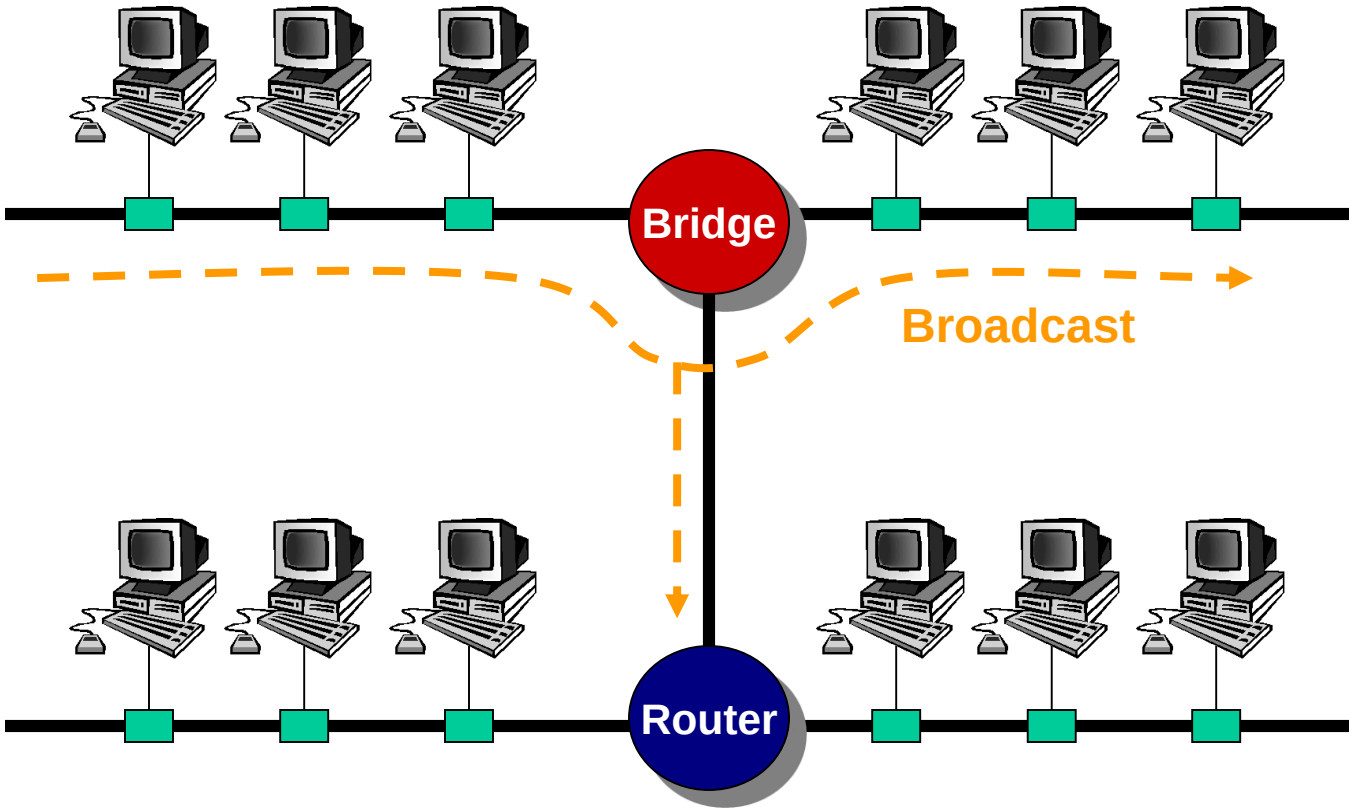


1. Broadcast: What is the MAC address of this network address?

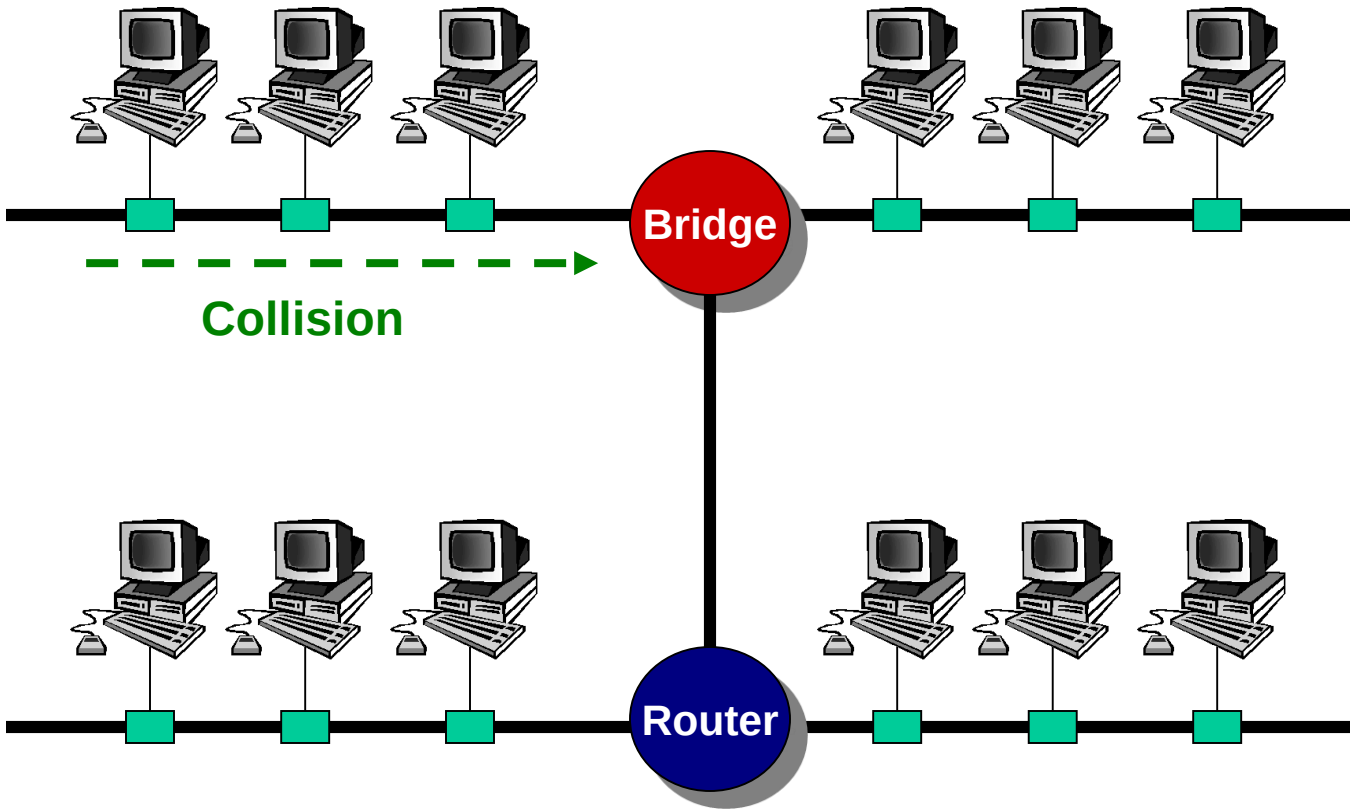
3. Updated ARP table: All the hosts update their ARP table with the correct IP and MAC address for the host.



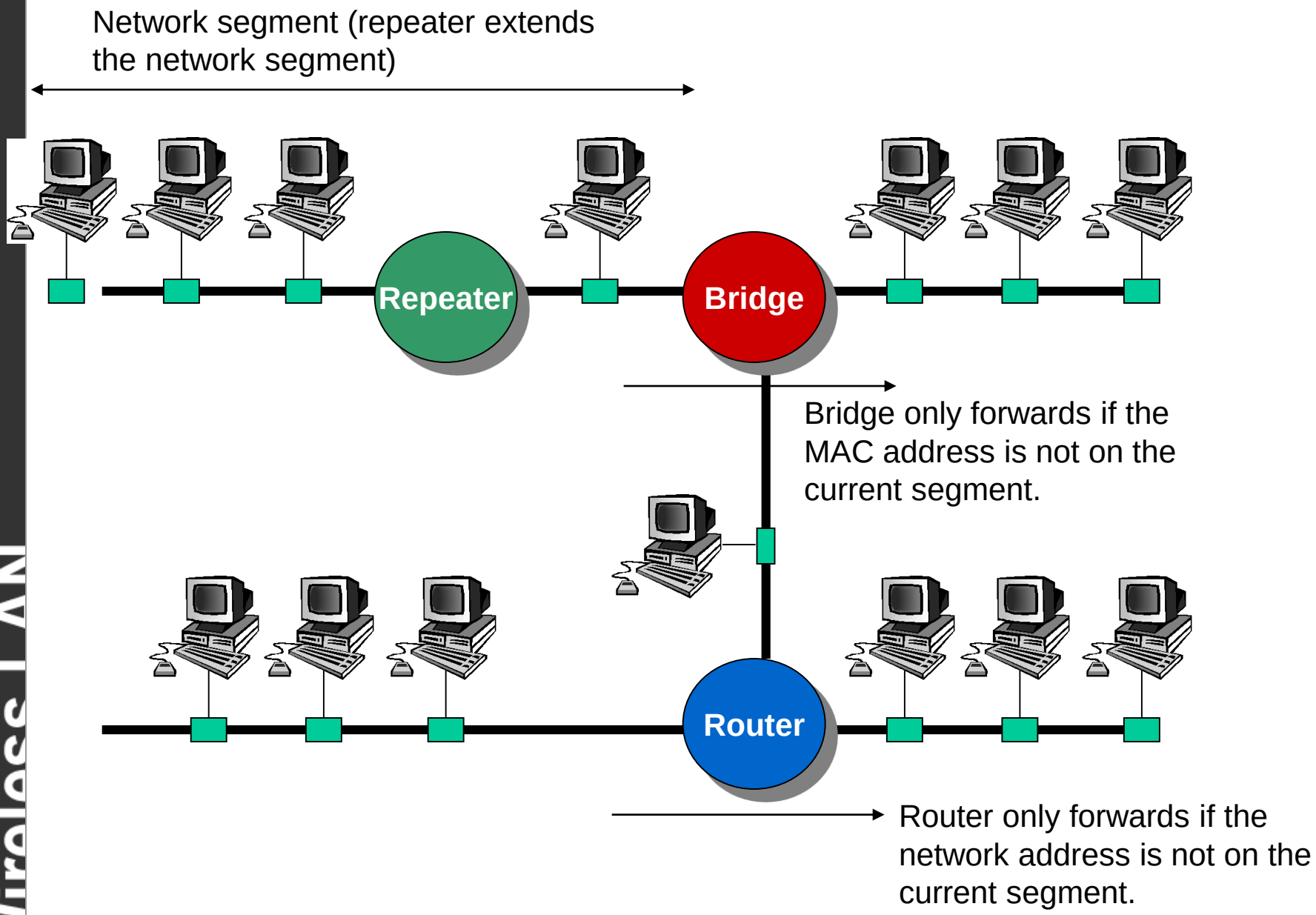
2. Requested host: All the hosts read the broadcast and checks if it relates to them. If it does then they respond back with their MAC address.

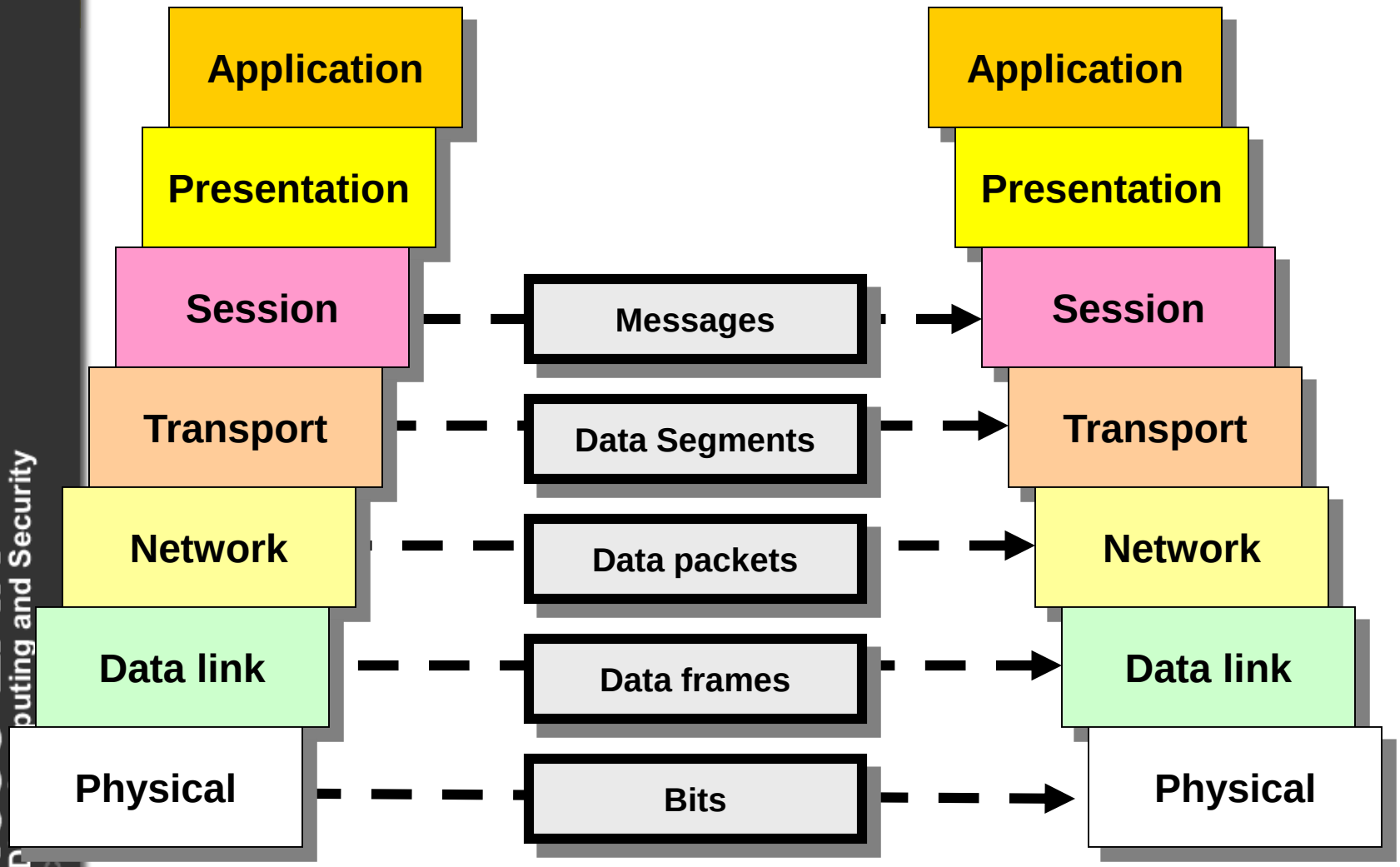


Repeaters:	Forward broadcasts
Bridges:	Forward broadcasts
Routers:	Block broadcasts

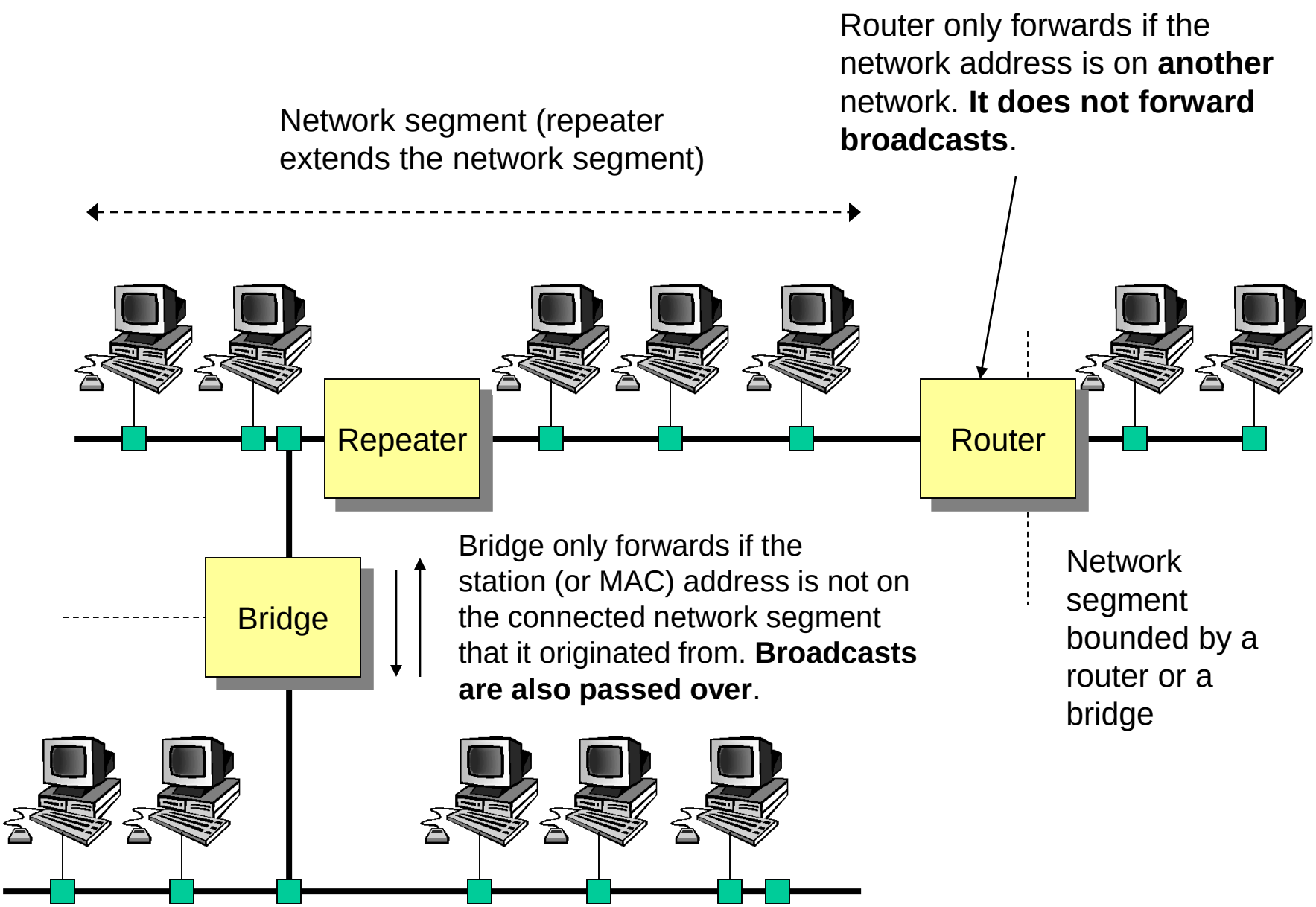


Repeaters:	Forward collisions
Bridges:	Block collisions
Routers:	Block collisions


Network segment (repeater extends the network segment)
Repeater
Bridge
Bridge only forwards if the MAC address is not on the current segment.
Router
Router only forwards if the network address is not on the current segment.


Application
Presentation
Session
Transport
Network
Data link
Physical
Messages
Data Segments
Data packets
Data frames
Bits
Application
Presentation
Session
Transport
Network
Data link
Physical

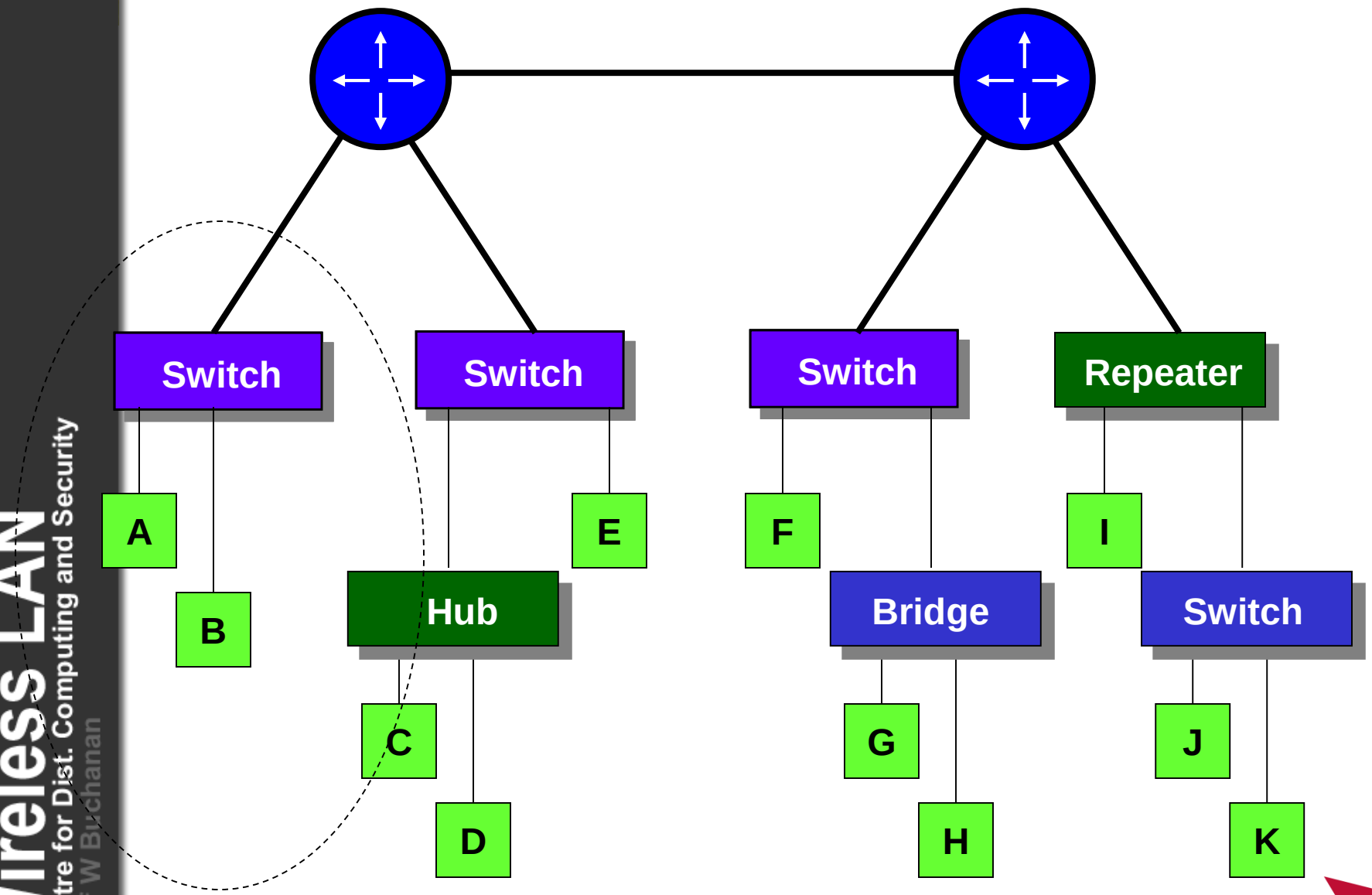
Repeaters, bridges and routers



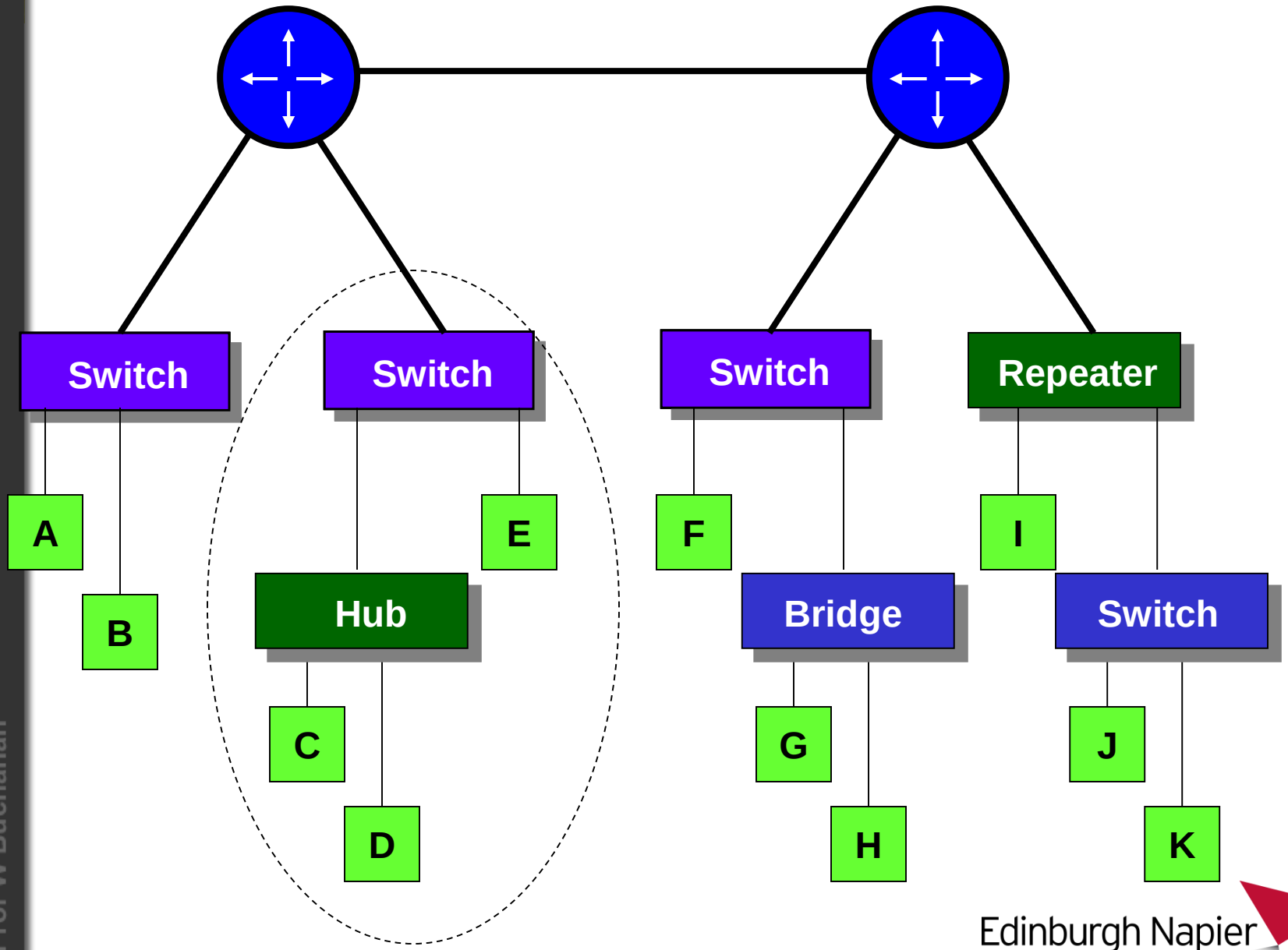
Network
Data Link
Physical

Routers:	Block broadcasts Block collisions
Bridges/switches:	Forward broadcasts Block collisions
Hub/repeaters:	Forward broadcasts Forward collisions

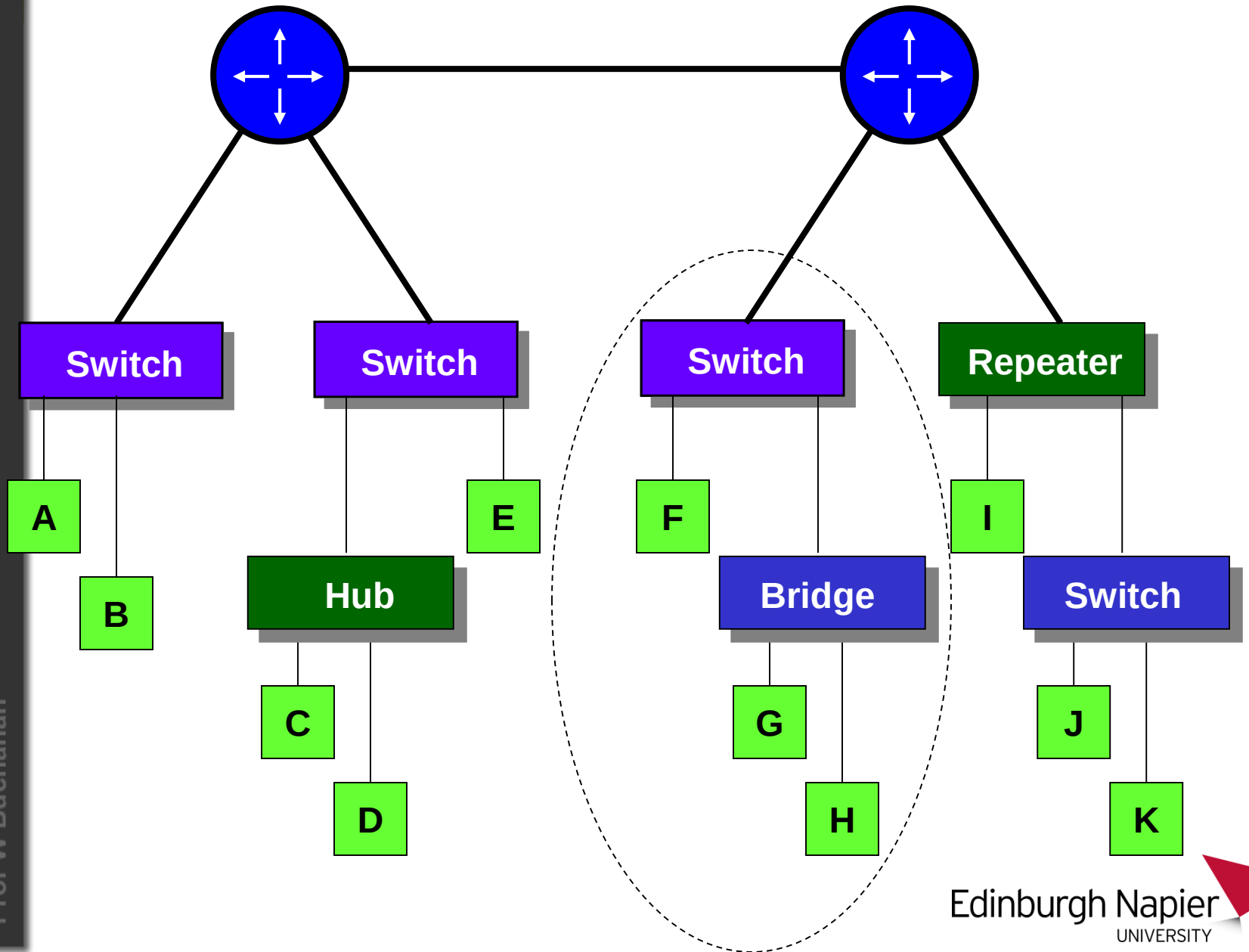
Broadcast domains



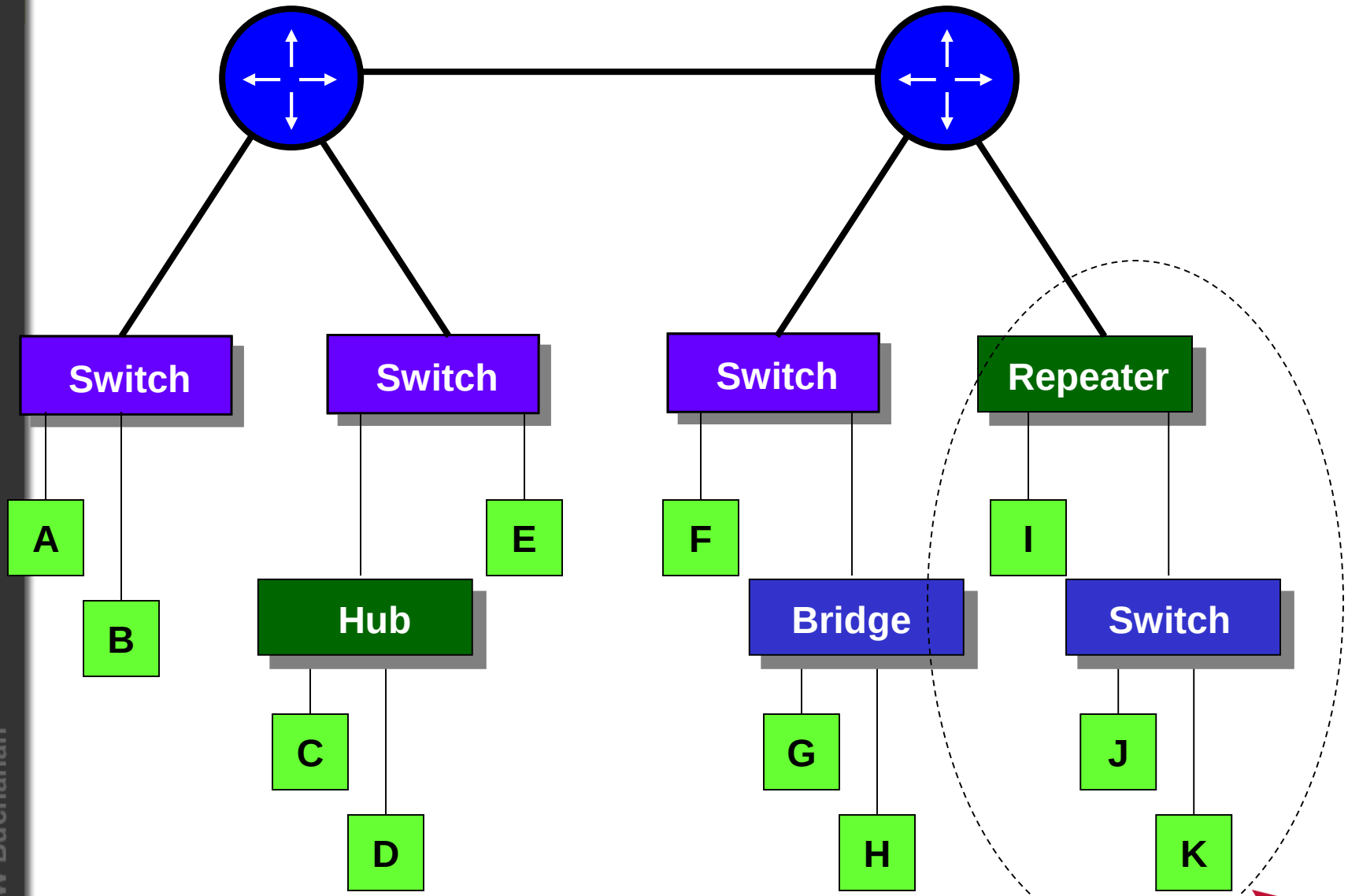
Broadcast domains



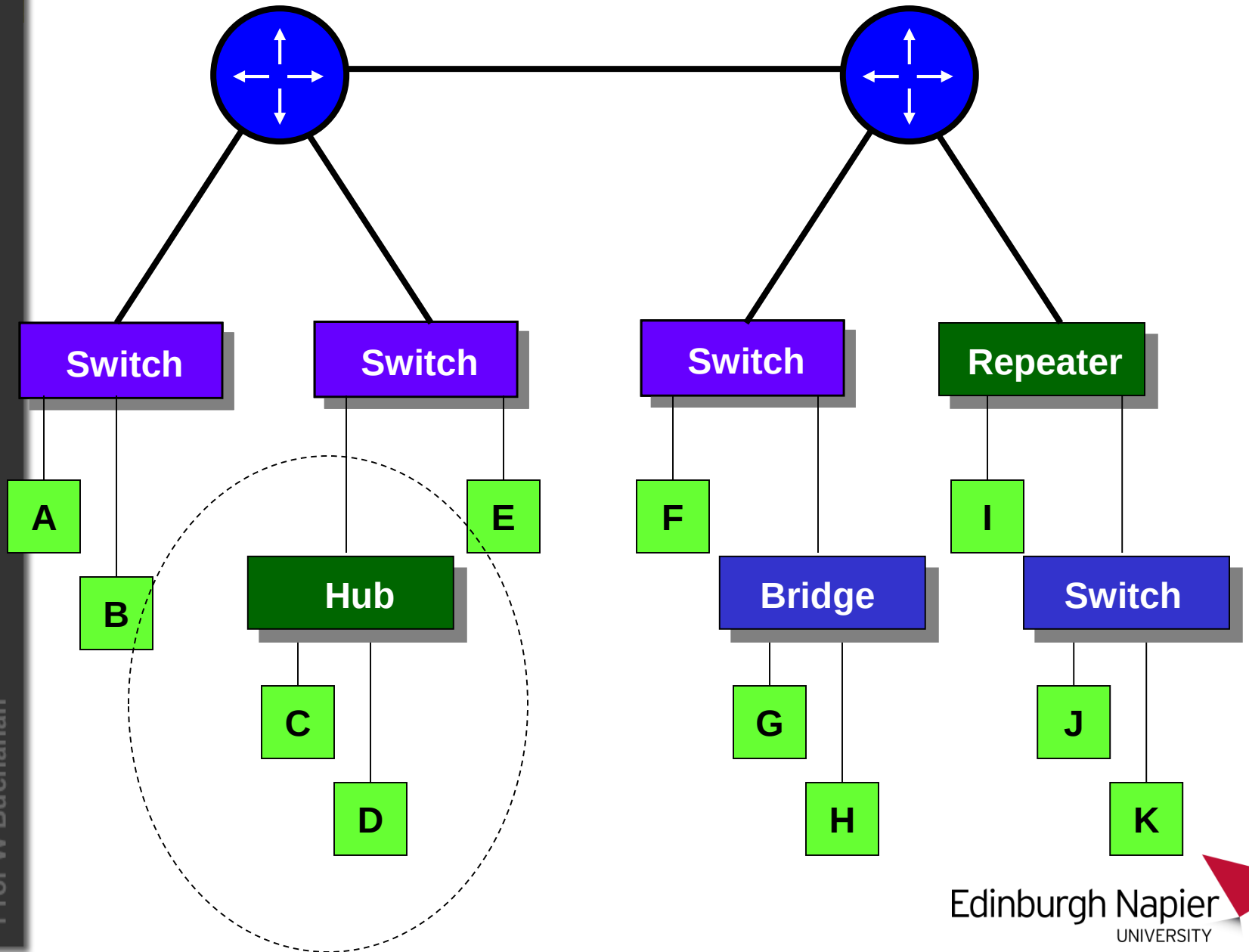
Broadcast domains

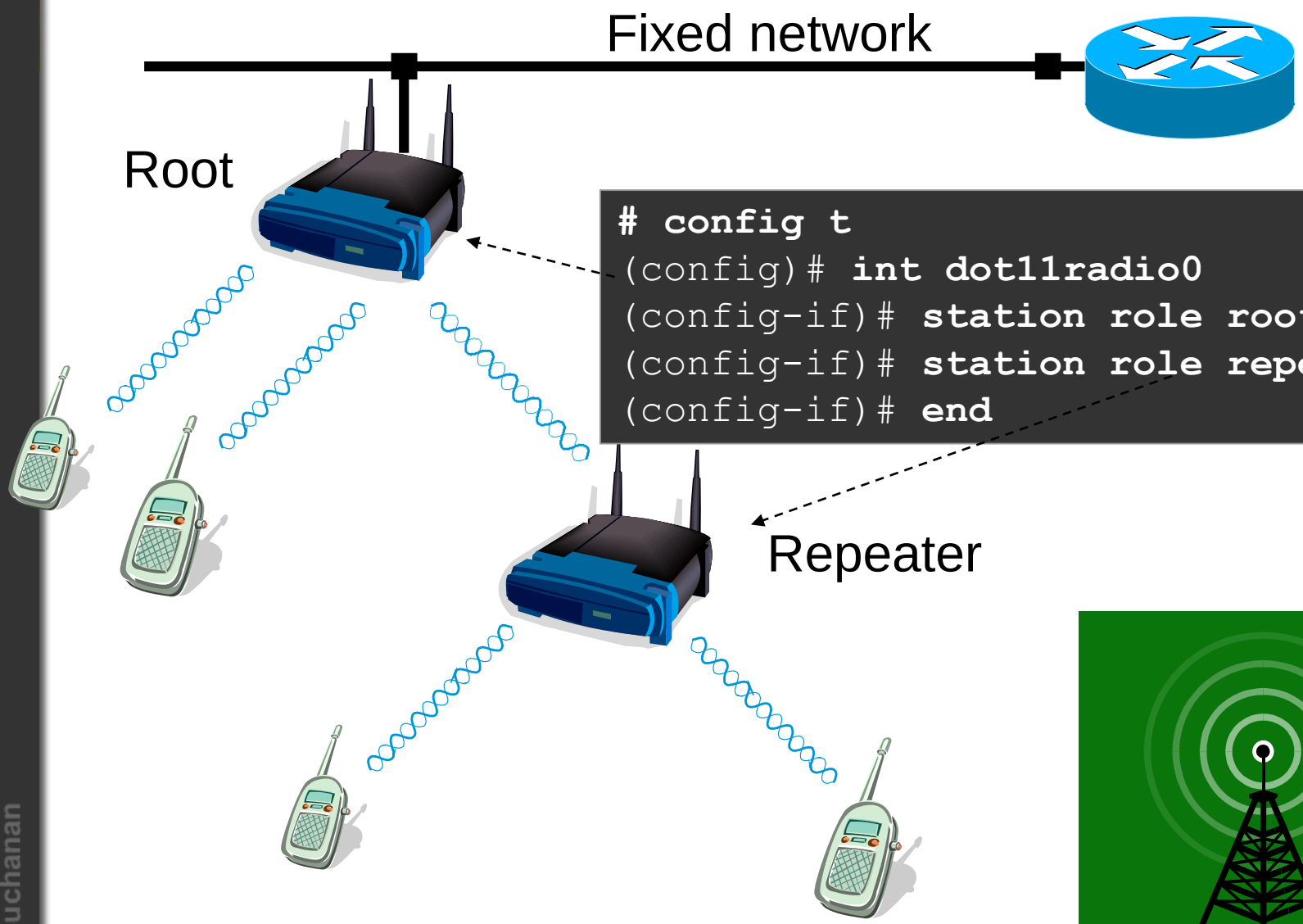


Broadcast domains

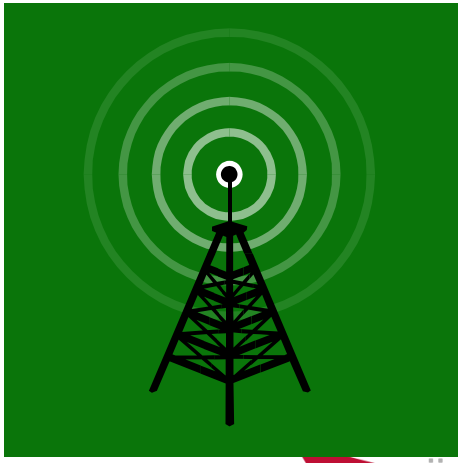


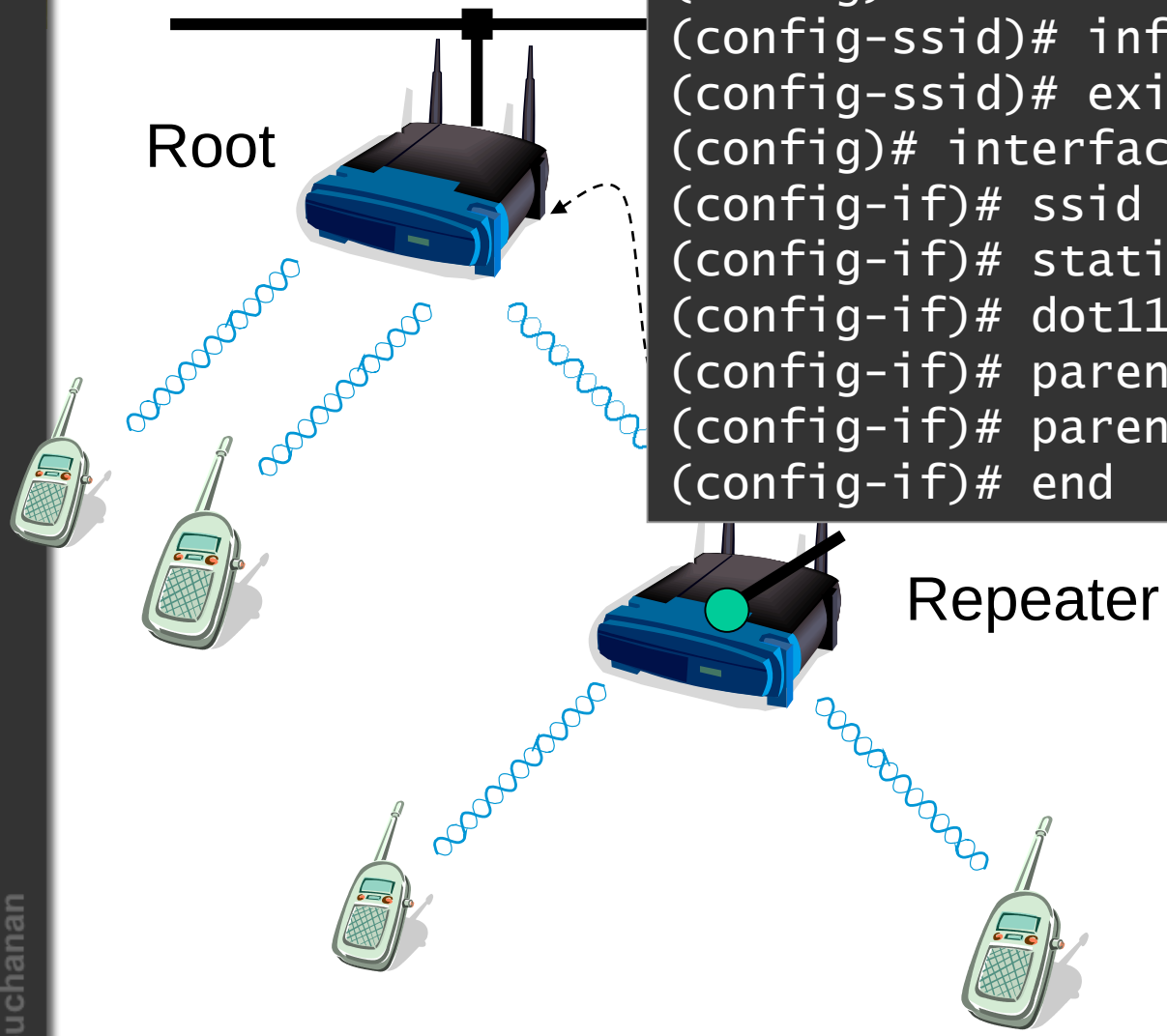
Collision domains



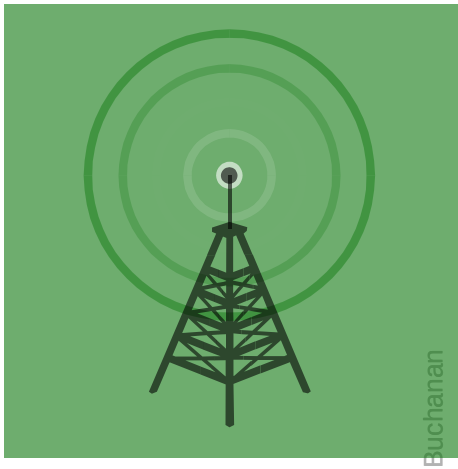


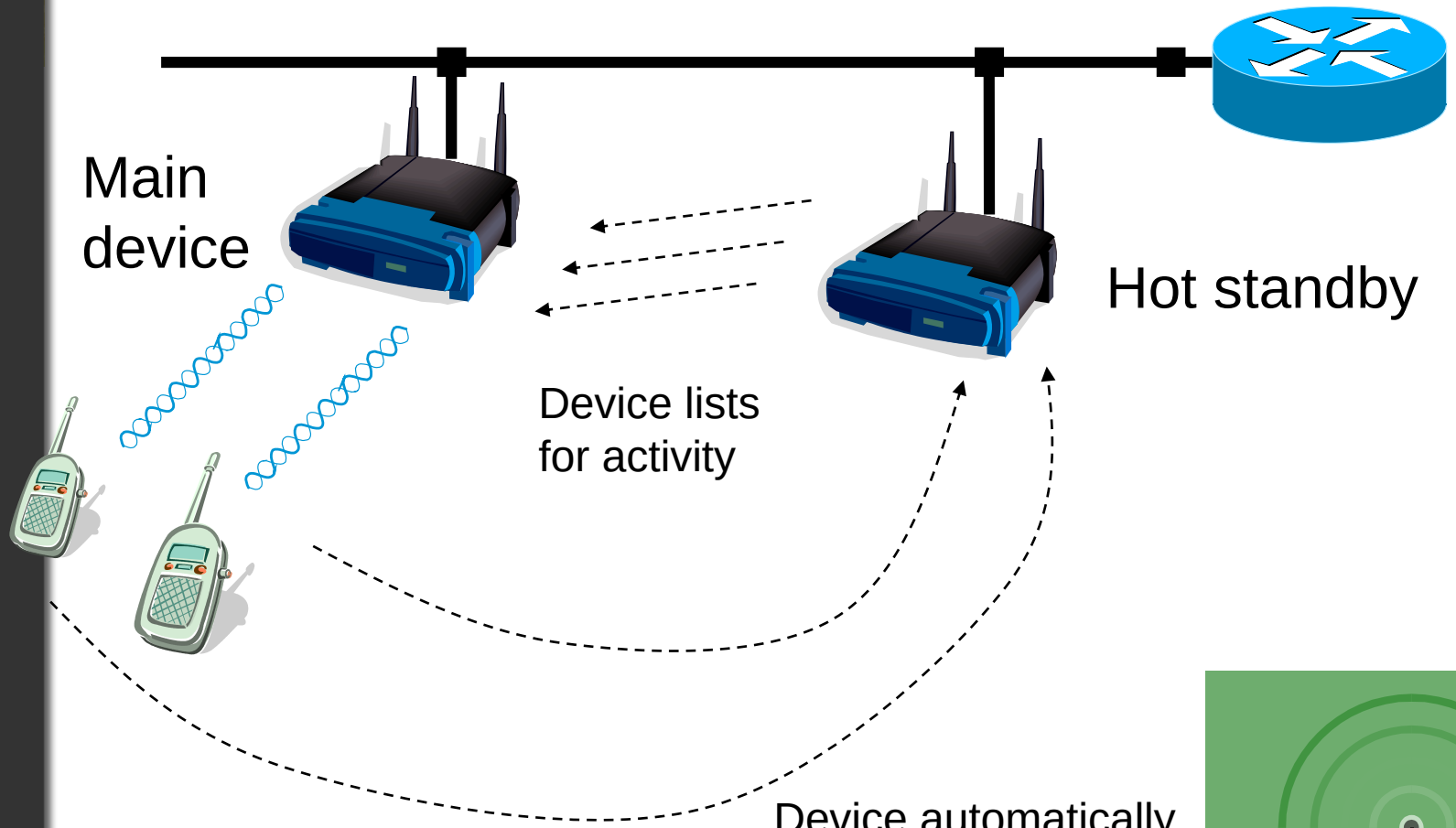

```
# config t
(config)# int dot11radio0
(config-if)# station role root
(config-if)# station role repeater
(config-if)# end
```

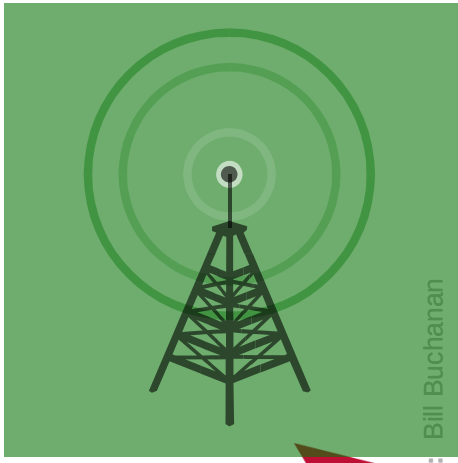


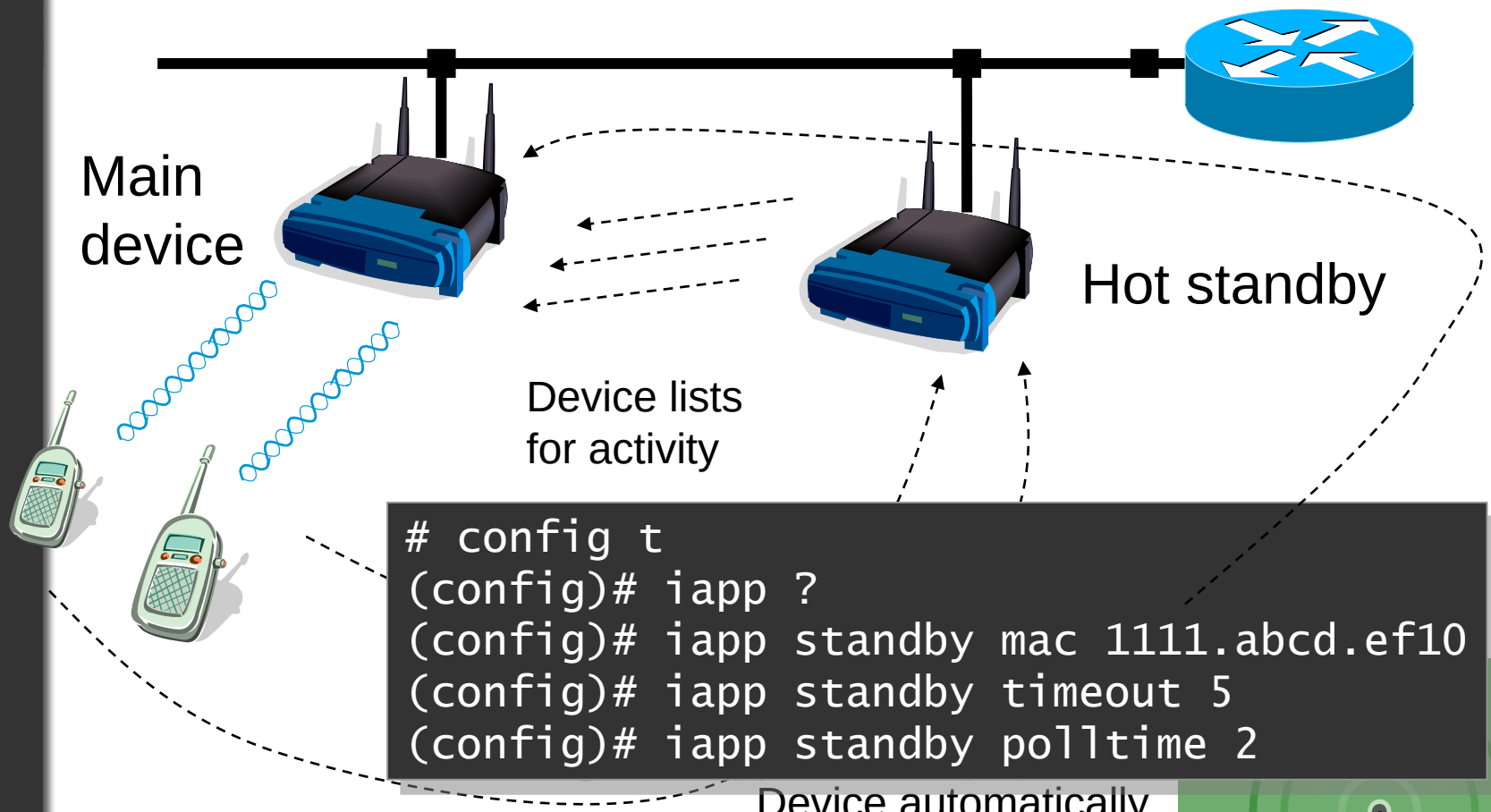



```
# config t
(config)# dot11 ssid napier
(config-ssid)# infrastructure-ssid
(config-ssid)# exit
(config)# interface d0
(config-if)# ssid napier
(config-if)# station-role repeater
(config-if)# dot11 extensions aironet
(config-if)# parent 1 1111.2222.3333
(config-if)# parent 2 2222.aaaa.bbbb
(config-if)# end
```




Main device
Hot standby
Device lists for activity
Device automatically associate with the standby device with the main one fails



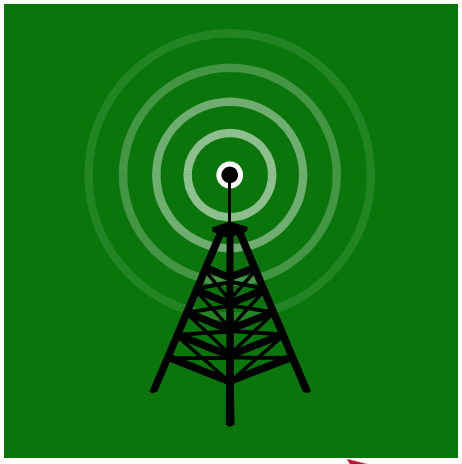



```
# config t
(config)# iapp ?
(config)# iapp standby mac 1111.abcd.ef10
(config)# iapp standby timeout 5
(config)# iapp standby polltime 2
```

Device automatically associate with the standby device with the main one fails

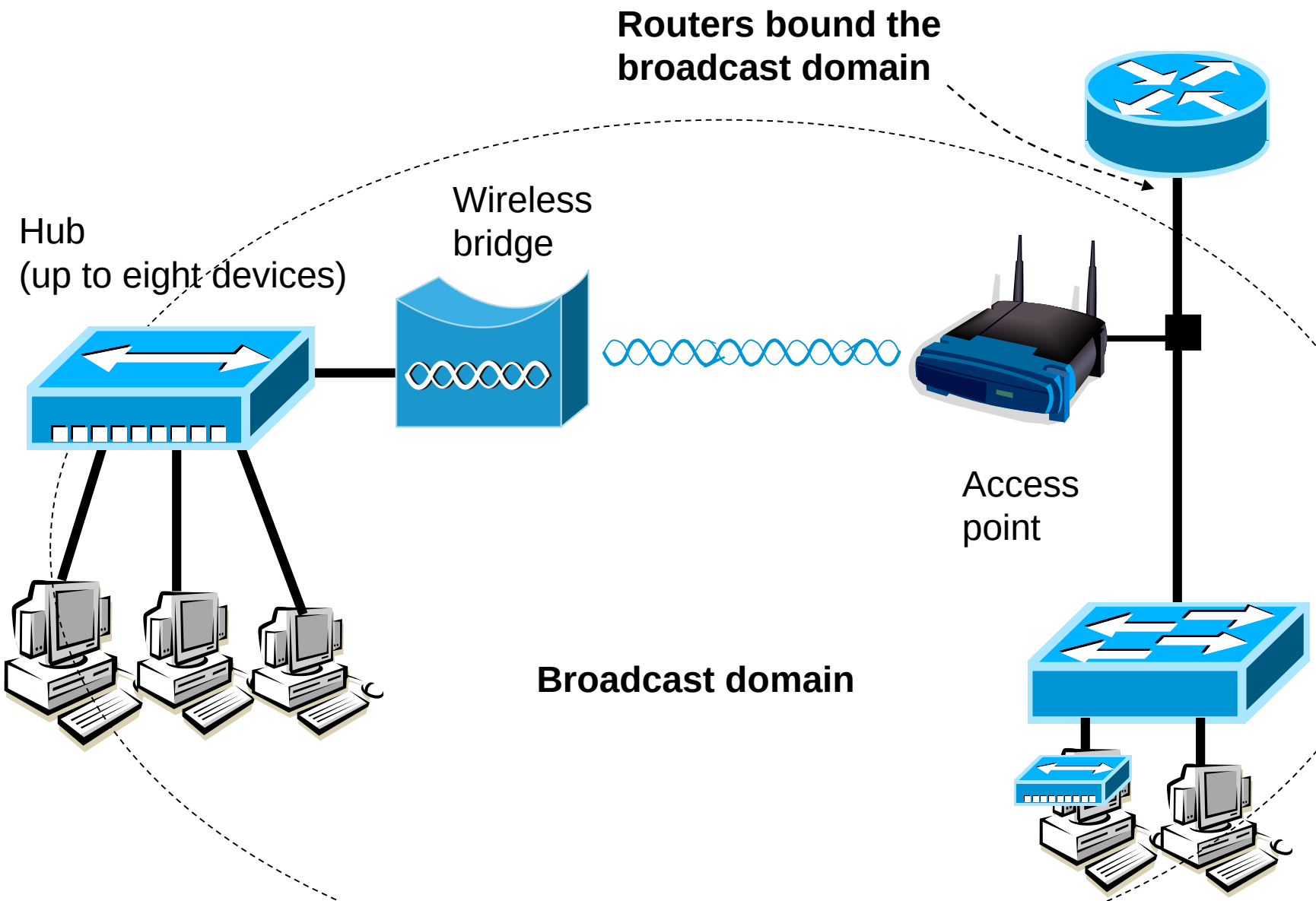
Wireless LAN

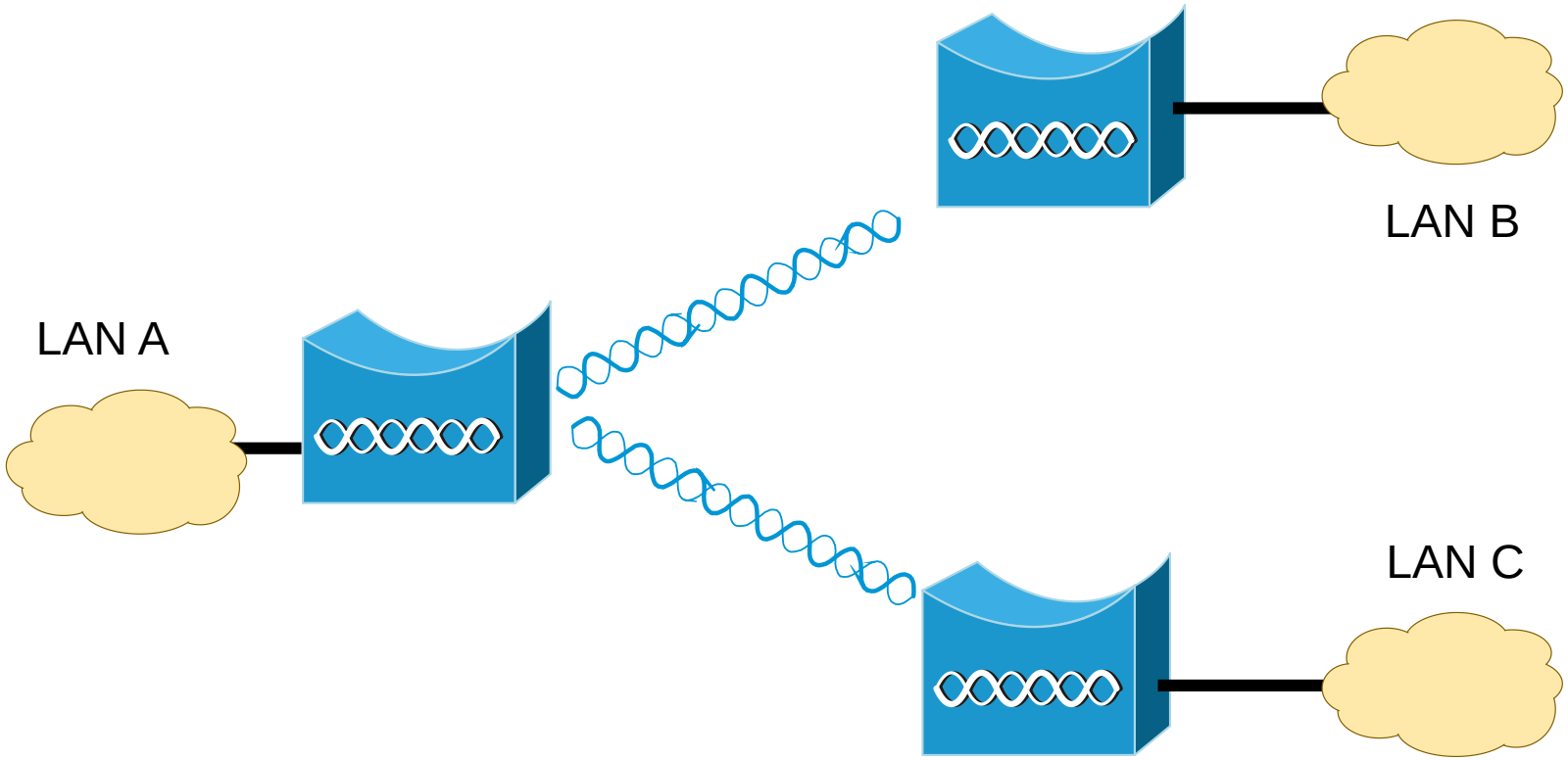
Wireless Bridging



Edinburgh Napier UNIVERSITY

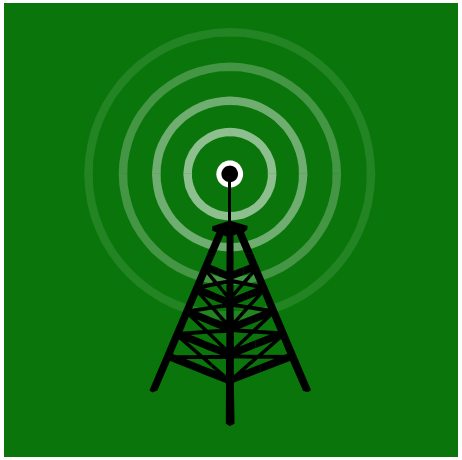
Author: Bill Buchanan


Routers bound the broadcast domain
Wireless bridge
Hub
(up to eight devices)
Access point
Broadcast domain


LAN A
LAN B
LAN C

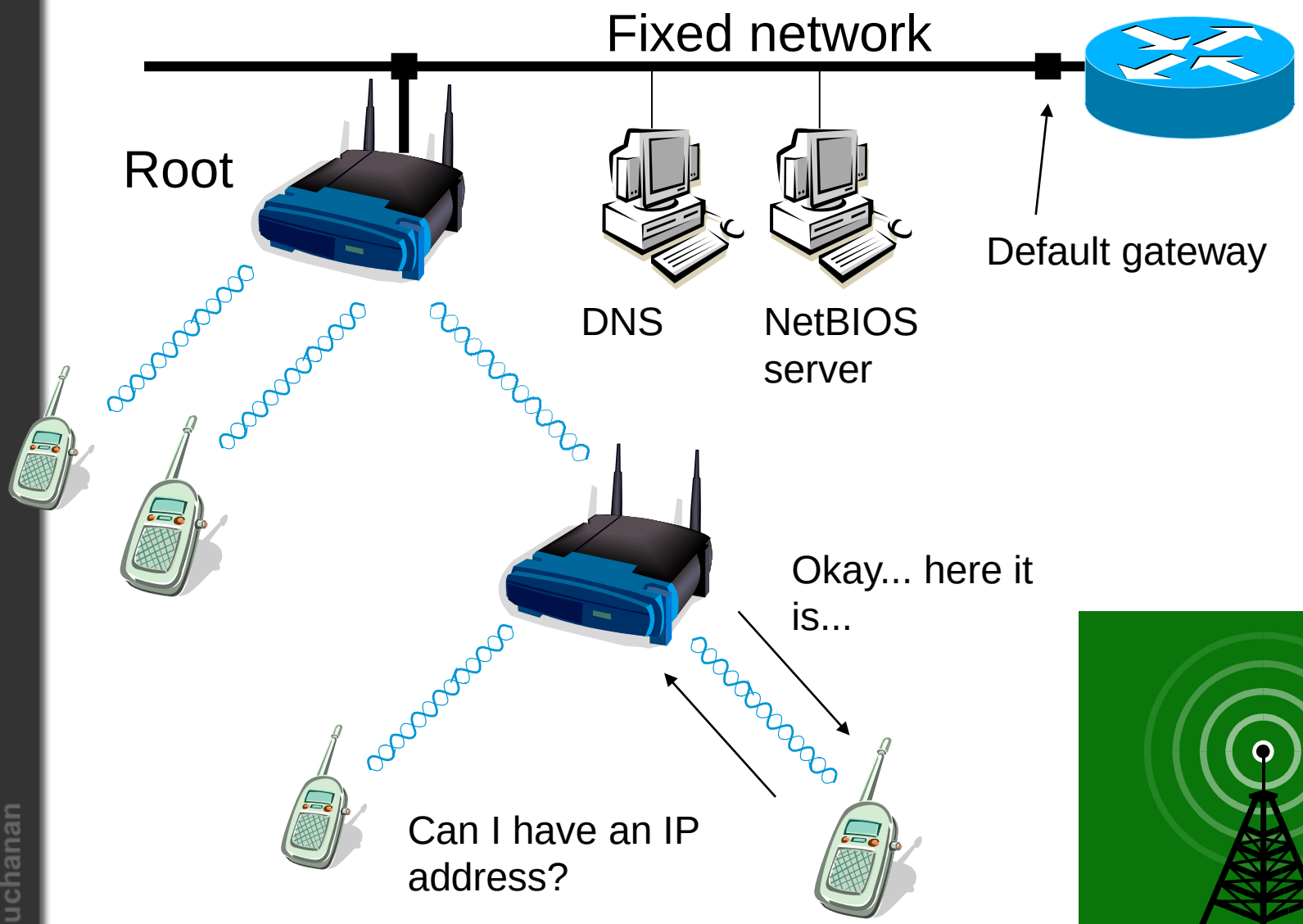
Wireless LAN

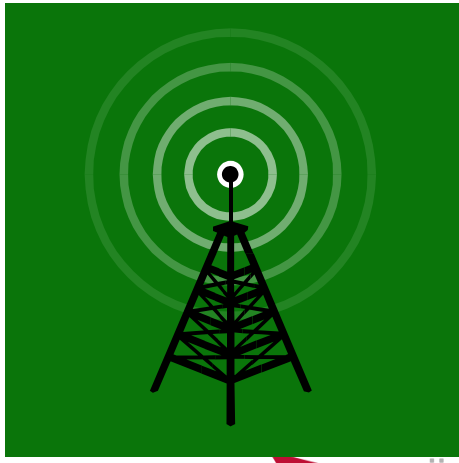
DHCP

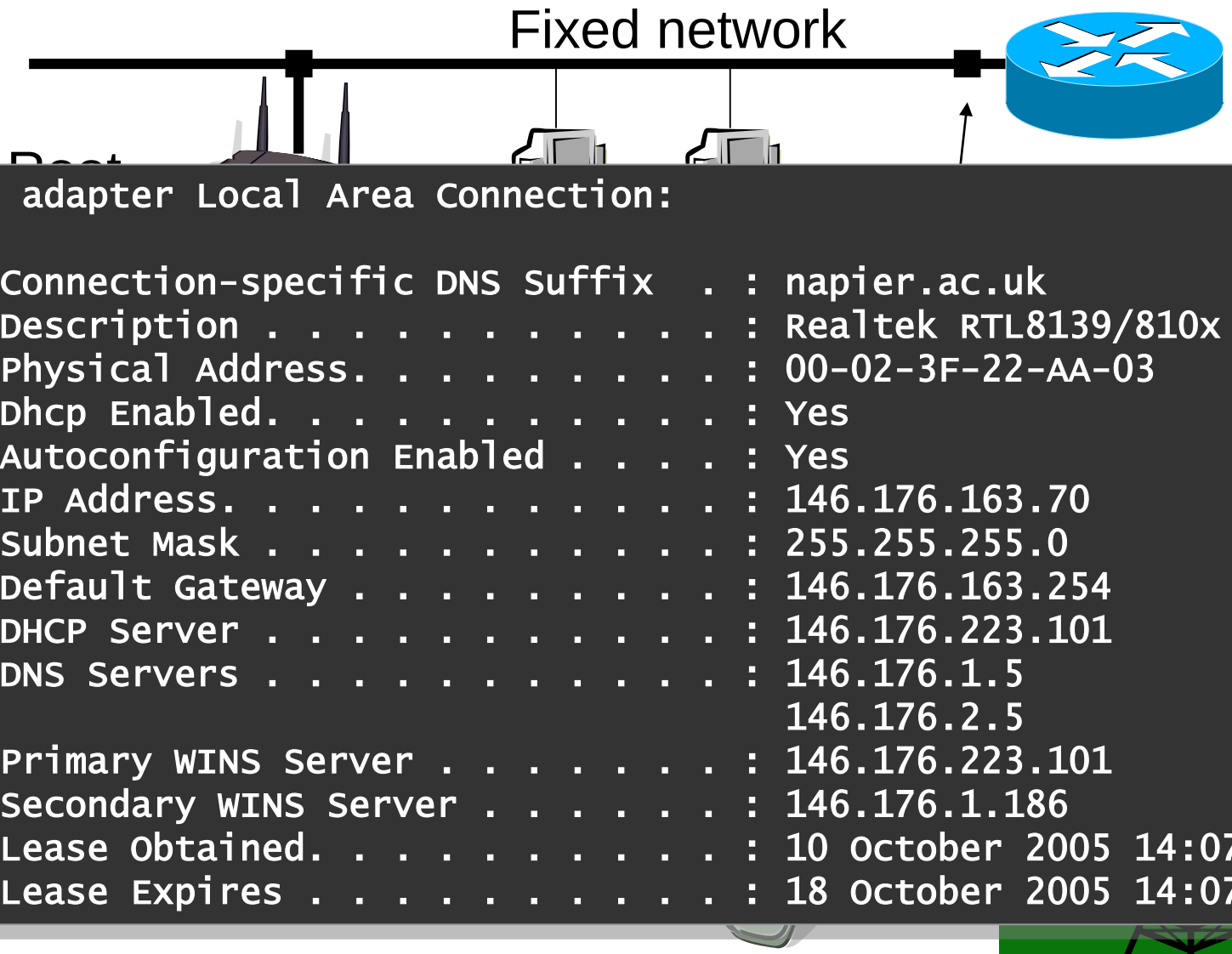


Edinburgh Napier UNIVERSITY

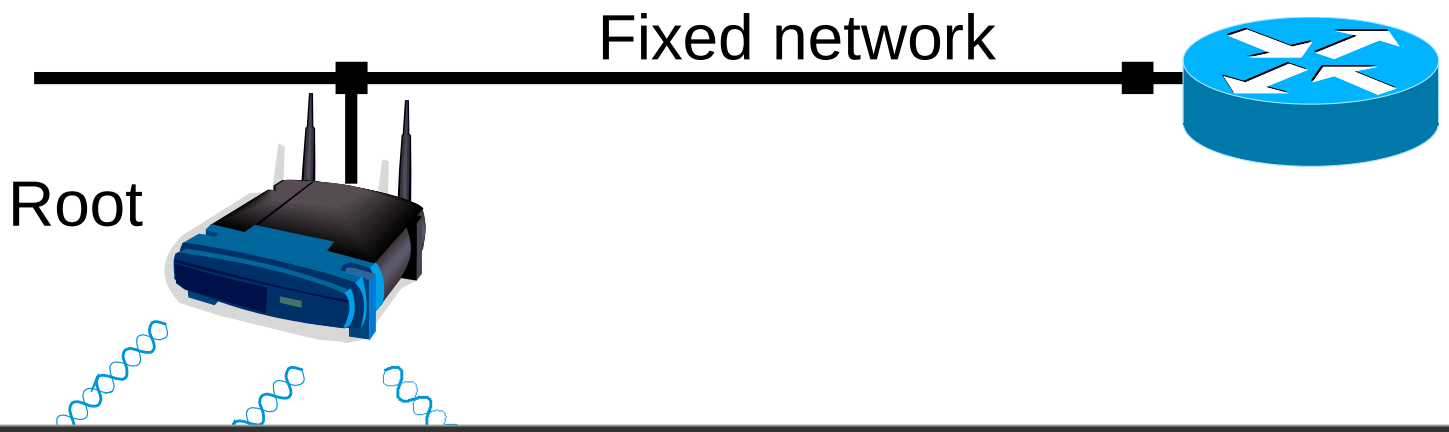
Author: Bill Buchanan


Fixed network
Root
DNS
NetBIOS server
Default gateway
Okay... here it is...
Can I have an IP address?





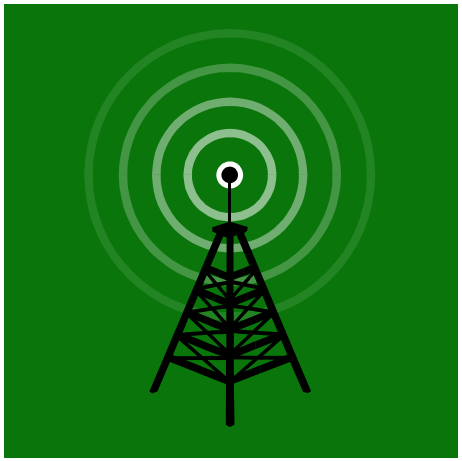

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : napier.ac.uk
        Description . . . . . . . . . . . : Realtek RTL8139/810x
        Physical Address. . . . . . . . . : 00-02-3F-22-AA-03
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 146.176.163.70
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 146.176.163.254
        DHCP Server . . . . . . . . . . . : 146.176.223.101
        DNS Servers . . . . . . . . . . . : 146.176.1.5
                                            146.176.2.5
        Primary WINS Server . . . . . . . : 146.176.223.101
        Secondary WINS Server . . . . . . : 146.176.1.186
        Lease Obtained. . . . . . . . . . : 10 October 2005 14:07:23
        Lease Expires . . . . . . . . . . : 18 October 2005 14:07:23
```




```
# config t
(config)# ip dhcp pool socpool
(config-dhcp)# network 192.168.0.0 255.255.255.0
(config-dhcp)# dns-server 10.0.0.1
(config-dhcp)# netbios-name-server 10.0.0.2
(config-dhcp)# domain-name xyz.com
(config-dhcp)# lease 10
(config-dhcp)# exit
(config)# ip dhcp excluded-address 192.168.0.10 192.168.0.12
(config)# ip dhcp ping timeout 400
# show running-config
```

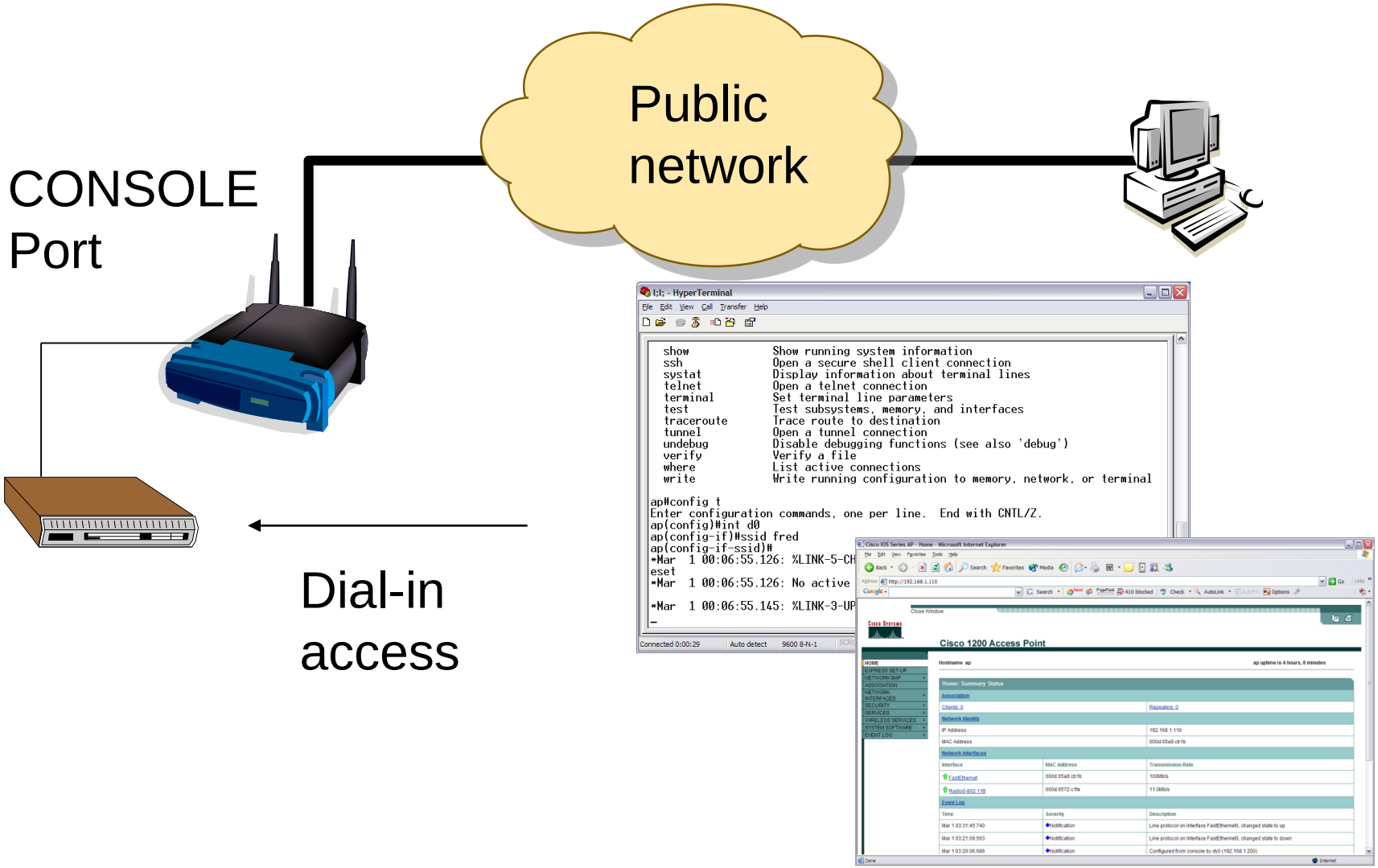
Wireless LAN

Remote Access



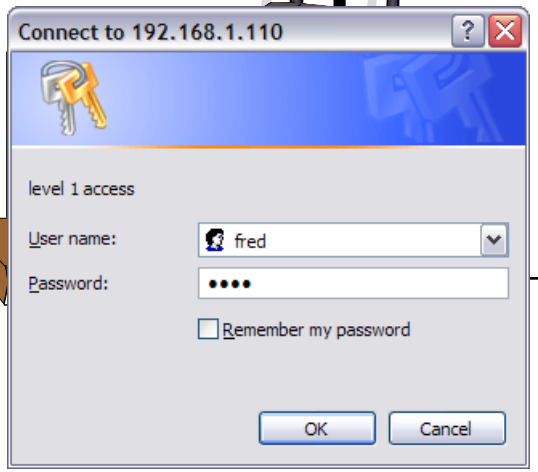
Edinburgh Napier UNIVERSITY

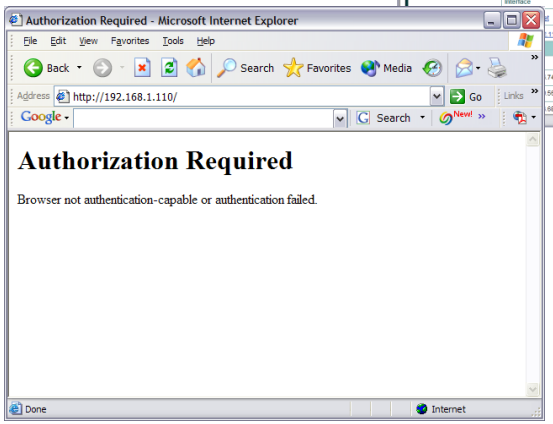
Author: Bill Buchanan

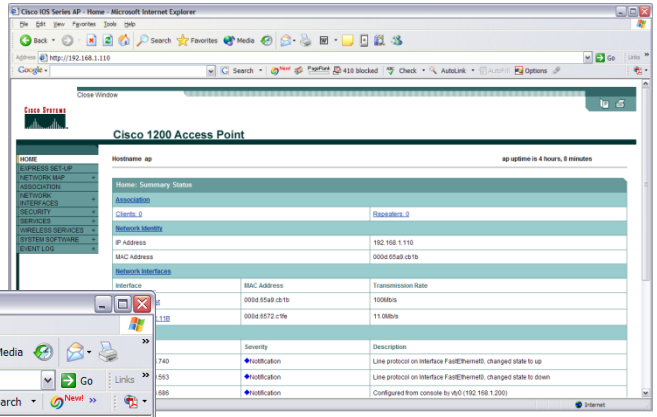

Public network
CONSOLE Port
Dial-in access
I:I; - HyperTerminal
File Edit View Call Transfer Help
show Show running system information
ssh Open a secure shell client connection
systat Display information about terminal lines
telnet Open a telnet connection
terminal Set terminal line parameters
test Test subsystems, memory, and interfaces
traceroute Trace route to destination
tunnel Open a tunnel connection
undebug Disable debugging functions (see also 'debug')
verify Verify a file
where List active connections
write Write running configuration to memory, network, or terminal
ap#config t
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid fred
ap(config-if-ssid)#
*Mar 1 00:06:55.126: %LINK-5-CH
eset
*Mar 1 00:06:55.126: No active
*Mar 1 00:06:55.145: %LINK-3-UP
Connected 0:00:29 Auto detect 9600 8-N-1
Cisco 1200 Access Point

CON
Port

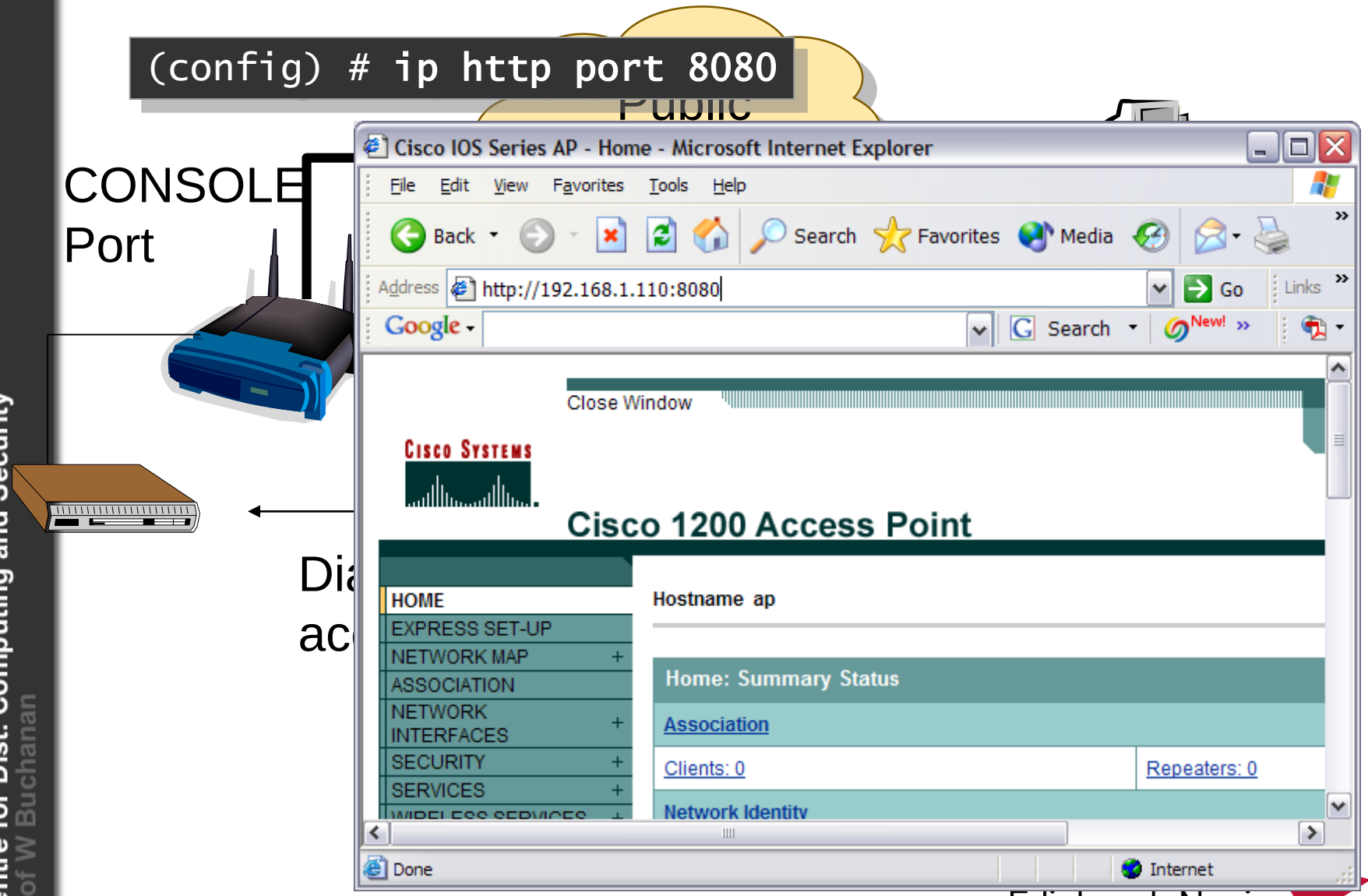
```
# config t
(config) # username fred password bert
(config) # ip http server
(config) # ip http authentication local
(config) # exit
```





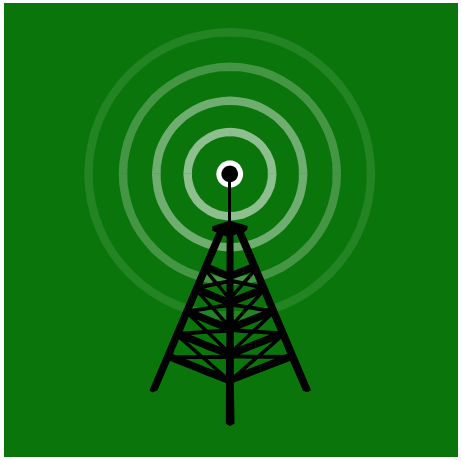


```
(config) # ip http port 8080
```



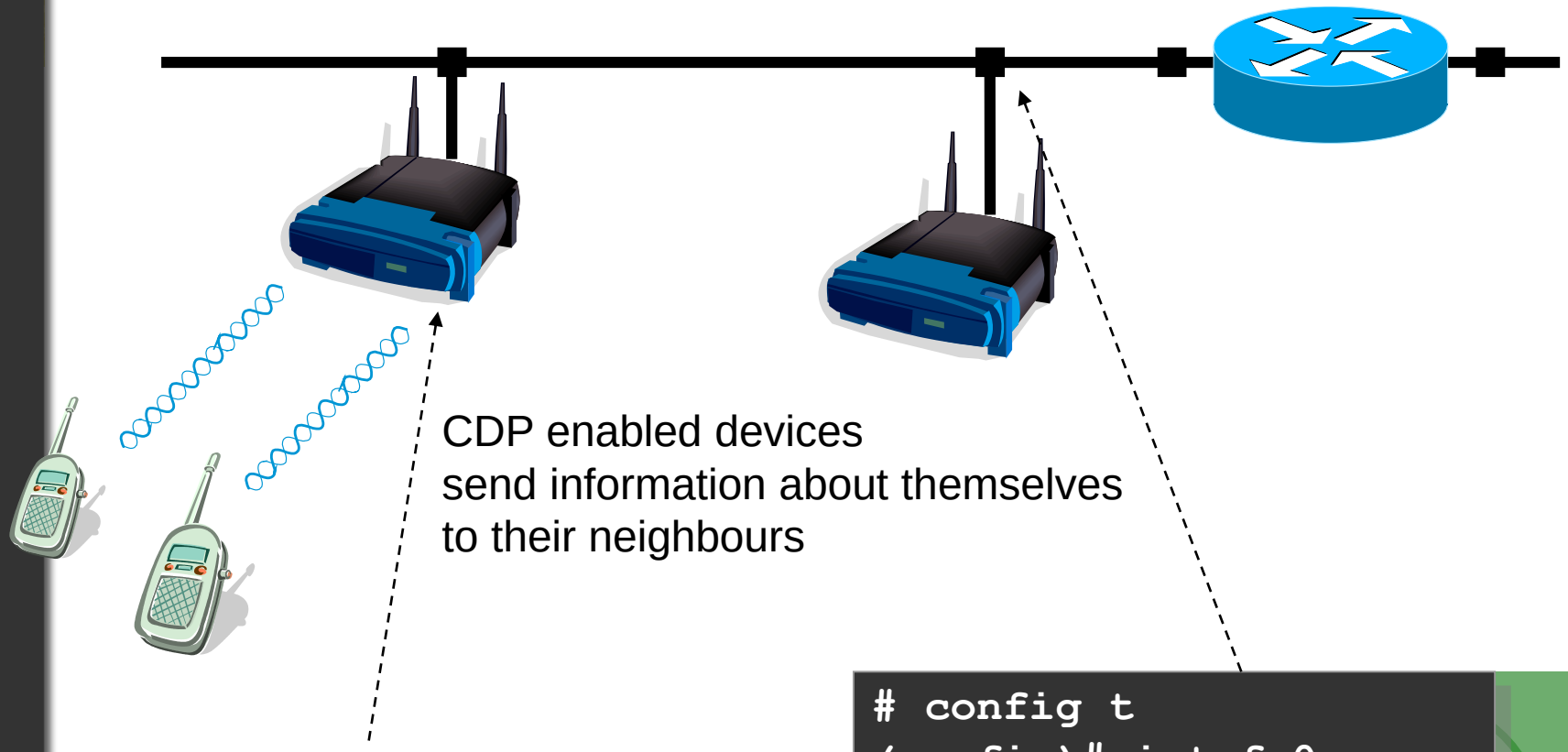
Wireless LAN

CDP



Edinburgh Napier UNIVERSITY

Author: Bill Buchanan



CDP enabled devices
send information about themselves
to their neighbours

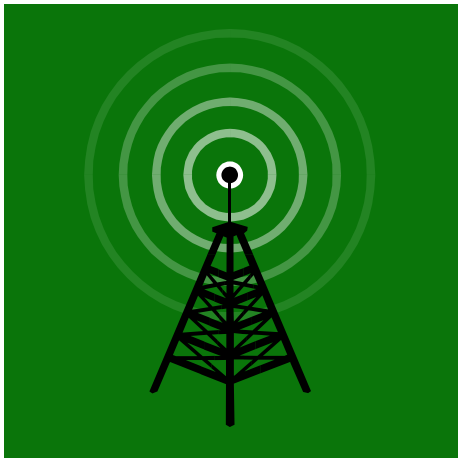
```
# config t
(config)# cdp holdtime 120
(config)# cdp timer 50
```

```
# config t
(config)# int fa0
(config-if)# cdp enable
(config-if)# end
```

```
# show cdp neighbors
# show cdp neighbors detail
# show cdp neighbors traffic
```

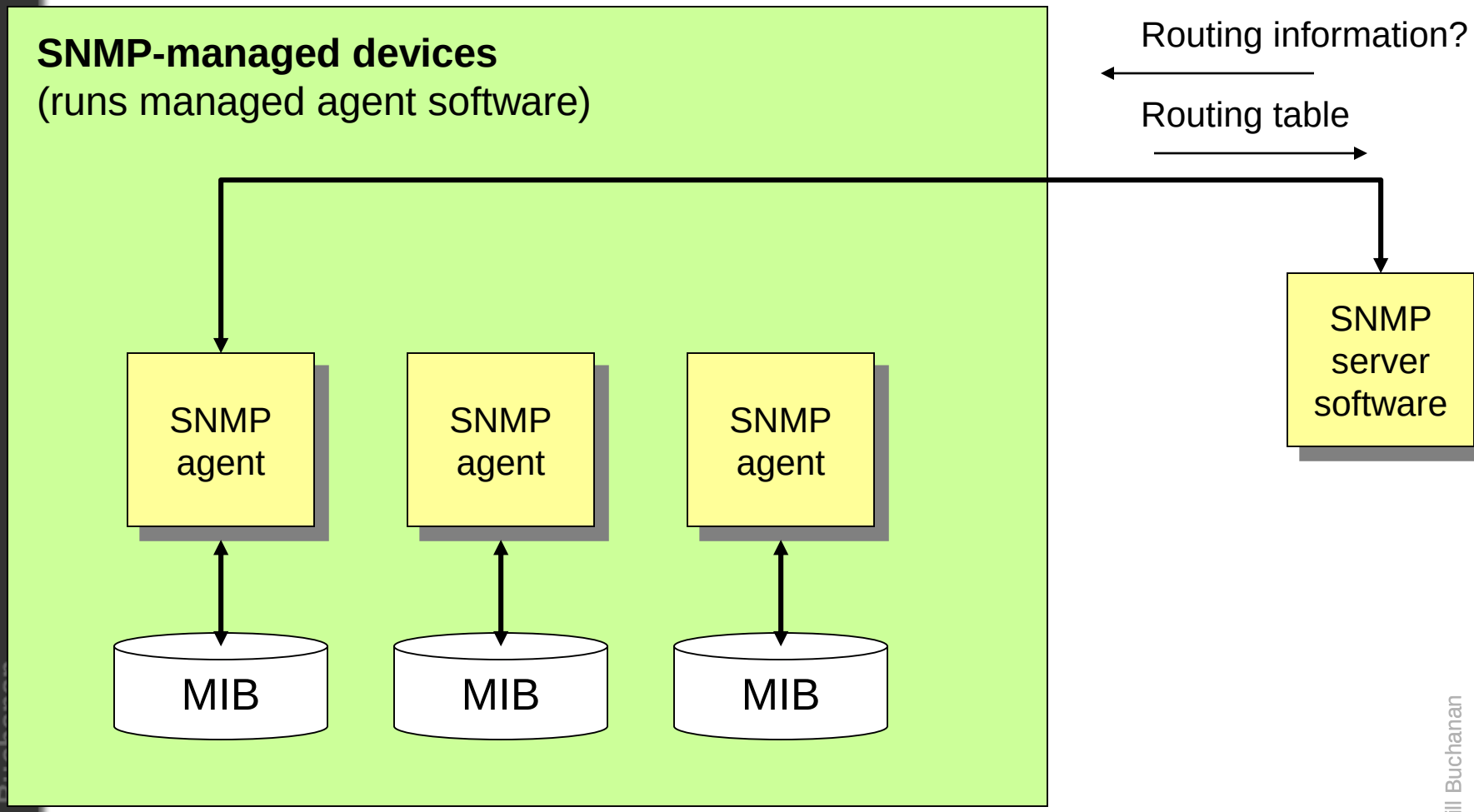
Wireless LAN

SNMP



Edinburgh Napier UNIVERSITY

Author: Bill Buchanan


SNMP-managed devices
(runs managed agent software)
Routing information?
Routing table
SNMP agent
SNMP agent
SNMP agent
MIB
MIB
MIB
SNMP server software

- The SNMP (Simple Network Management Protocol) protocol is initially based in the RFC1157 document.
- It defines a simple protocol which gives network element management information base (MIB).
- There are two types of MIB: MIB-1 and MIB-2. MIB-1 was defined in 1988 and has 114 table entries, divided into two groups. MIB-2 is a 1990 enhancement which has 171 entries organized into 10 groups (RFC 1213). Most devices are MIB-1 compliant and newer one with both MIB-1 and MIB-2.

Version	Authentication	Encryption
v1 Community	strings	None
!Trivial authentication.	Packets sent in clear-text.	
v2c Community	strings	None
!Trivial authentication.	Packets sent in clear-text.	
v3(noAuthNoPriv)	Username	None
!Trivial authentication.	Packets sent in clear-text.	
v3(authNoPriv) SHA or MD5	encrypted pass phrase	
None Strong authentication.	Packets sent in clear-text.	
v3(authPriv)	SHA or MD5	encrypted pass phrase

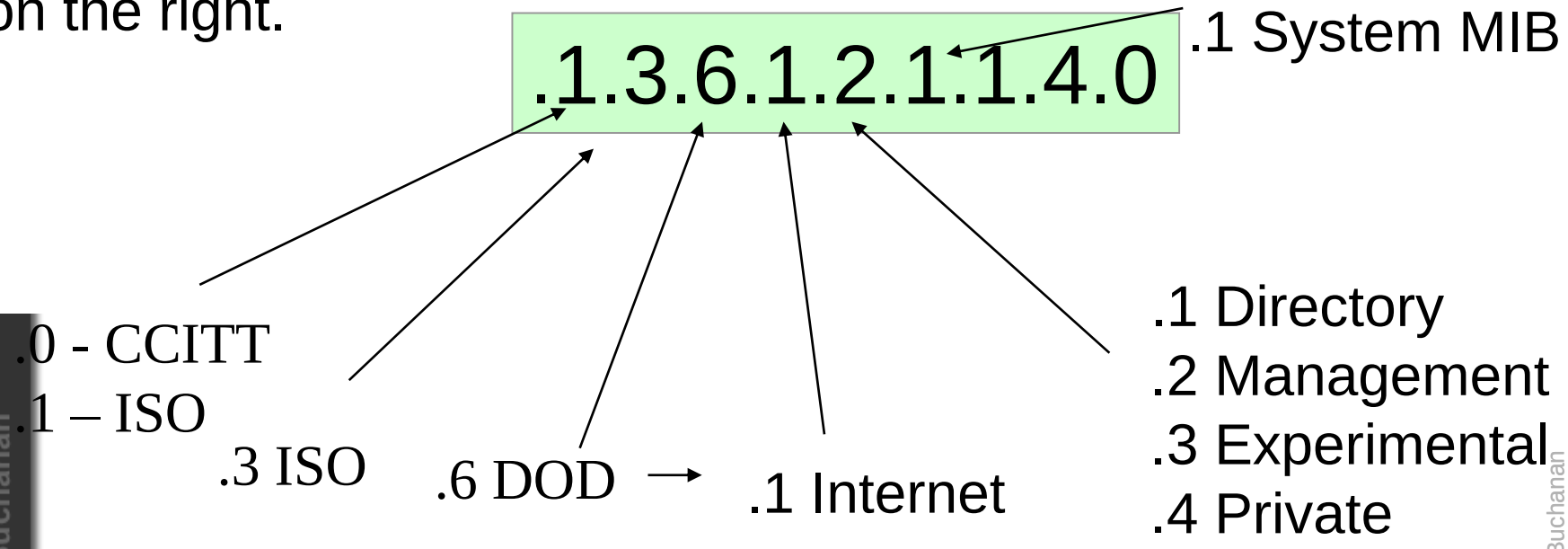
!DES Strong authentication. Packets are encrypted.

- **Object type**. Defines the name of the entry.
- **Syntax**. Gives the actual value (as string or an integer).
- **Access field**. Defines whether the value is read-only, read/write, write-only and not accessible.
- **Status field**. Contains an indication on whether the entry in the MIB is mandatory (the managed device must implement the entry), optional (the managed device may implement the entry) or obsolete (the entry is not used).

The network management protocol operates by inspecting or altering variables on an agent's MIB (management information base). They communicate by exchanging messages within UDP datagrams, with:

- A Version identifier (version). An integer value defining the version number.
- SNMP community name (community). An eight character string defining the community name.
- A protocol data unit (data). All SNMP implementations five PDUs: GetRequest-PDU, GetNextRequest-PDU, GetResponse-PDU, SetRequest-PDU, and Trap-PDU.

- The MIB tree structure is defined by a long sequence of numbers separated by dots, such as .1.3.6.1.2.1.1.4.0. This number is called an **Object Identifier** (OID).
- The OID is a numerical representation of the MIB tree structure. Each digit represents a node in this tree structure. The trunk of the tree is on the left; the leaves are on the right.



- The MIB tree structure is defined by a long sequence of numbers separated by dots, such as .1.3.6.1.2.1.1.4.0. This number is called an **Object Identifier** (OID).
- The OID is a numerical representation of the MIB tree structure. Each digit represents a node in this tree structure. The trunk of the tree is on the left; the leaves are on the right.

.1.3.6.1.2.1.1.4.0

sysDescr (1), *sysObjectID* (2),
sysUpTime (3), *sysContact* (4),
sysName (5), *sysLocation* (6),
sysServices (7),

Active SNMP - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://127.0.0.1:6611/ActiveSNMP.handler.Frames.class?sid=111508038292478136363131313434362e3137362e3136332e3730&regkey=&user=administrator&name=administrat

Customize Links Free Hotmail Windows Media Windows content.html

Active SNMP

THIS IS EVALUATION-ONLY VERSION OF ACTIVE SNMP. IT CAN BE USED ONLY FOR EVALUATION WHETHER TO PURCHASE AN ONGOING LICENSE.

Hosts | Browse | Commands | Graphs | MIBs | Options | Logout | About

- org
  - dod
    - internet
      - director
      - mgmt
      - experim
      - private
      - security
      - snmpV2

Browse

Help

Active SNMP - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://127.0.0.1:6611/ActiveSNMP.handler.Frames.class?sid=111508038292478136363131313434362e3137362e3136332e3730&regkey=&user=administrator&name=administrat

Customize Links Free Hotmail Windows Media Windows content.html

Active SNMP

THIS IS EVALUATION-ONLY VERSION OF ACTIVE SNMP. IT CAN BE USED ONLY FOR EVALUATION WHETHER TO PURCHASE AN ONGOING LICENSE.

Hosts | Browse | Commands | Graphs | MIBs | Options | Logout | About

- org
  - dod
    - internet
      - directory
      - mgmt
        - mib-2
          - system
          - interfaces
          - at
          - ip
          - icmp
          - tcp
          - udp
          - egp
          - transmission
          - snmp
          - ianaifType
      - experimental
      - private
      - security
      - snmpV2

Browse

Help

Host: 127.0.0.1 **address:** 127.0.0.1

Current node: iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).icmp(5).icmpInMsgs(1)

Name: icmpInMsgs [Find Name] [Get Next] [Walk]

Object ID: 1.3.6.1.2.1.5.1.0 [Find OID] [Get Next] [Walk]

MIB: RFC1213-MIB [file name: rfc1213.mib]

Description: The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

Value: 78

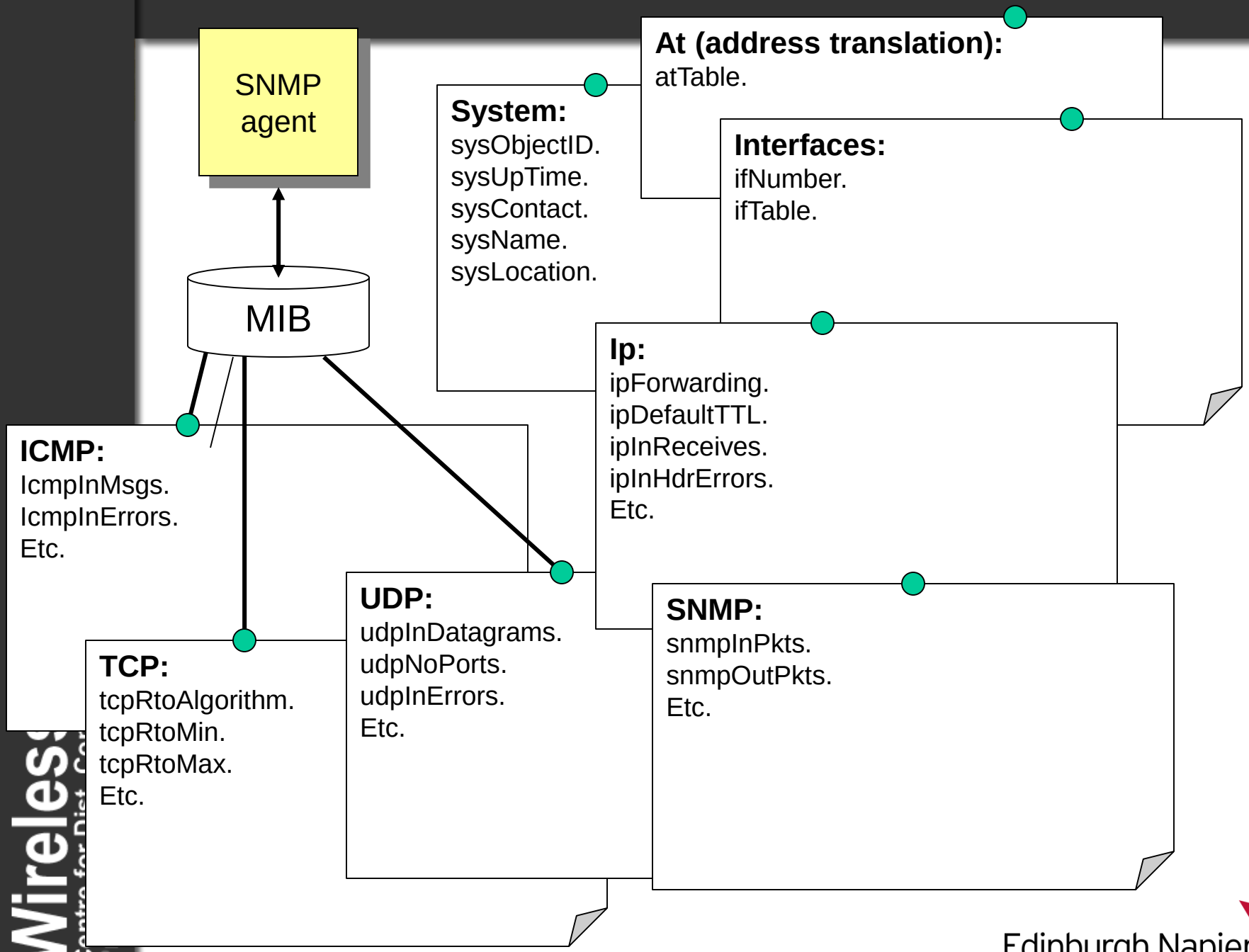
[Refresh] [Graph] [Back To Parent Node] [Commands]

Done

Node: 1.3.6.1.2.1.5.1.0

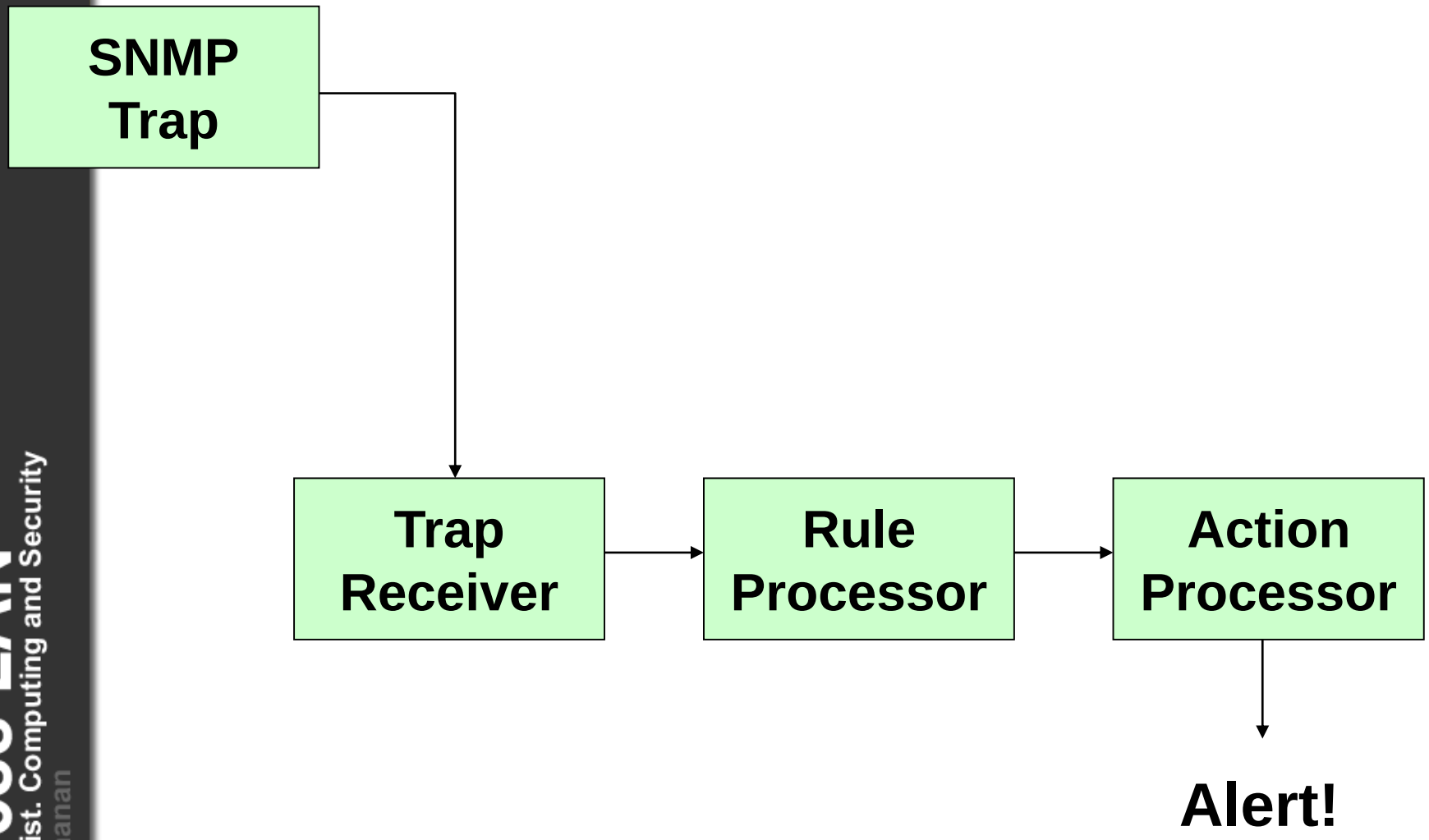
End of node

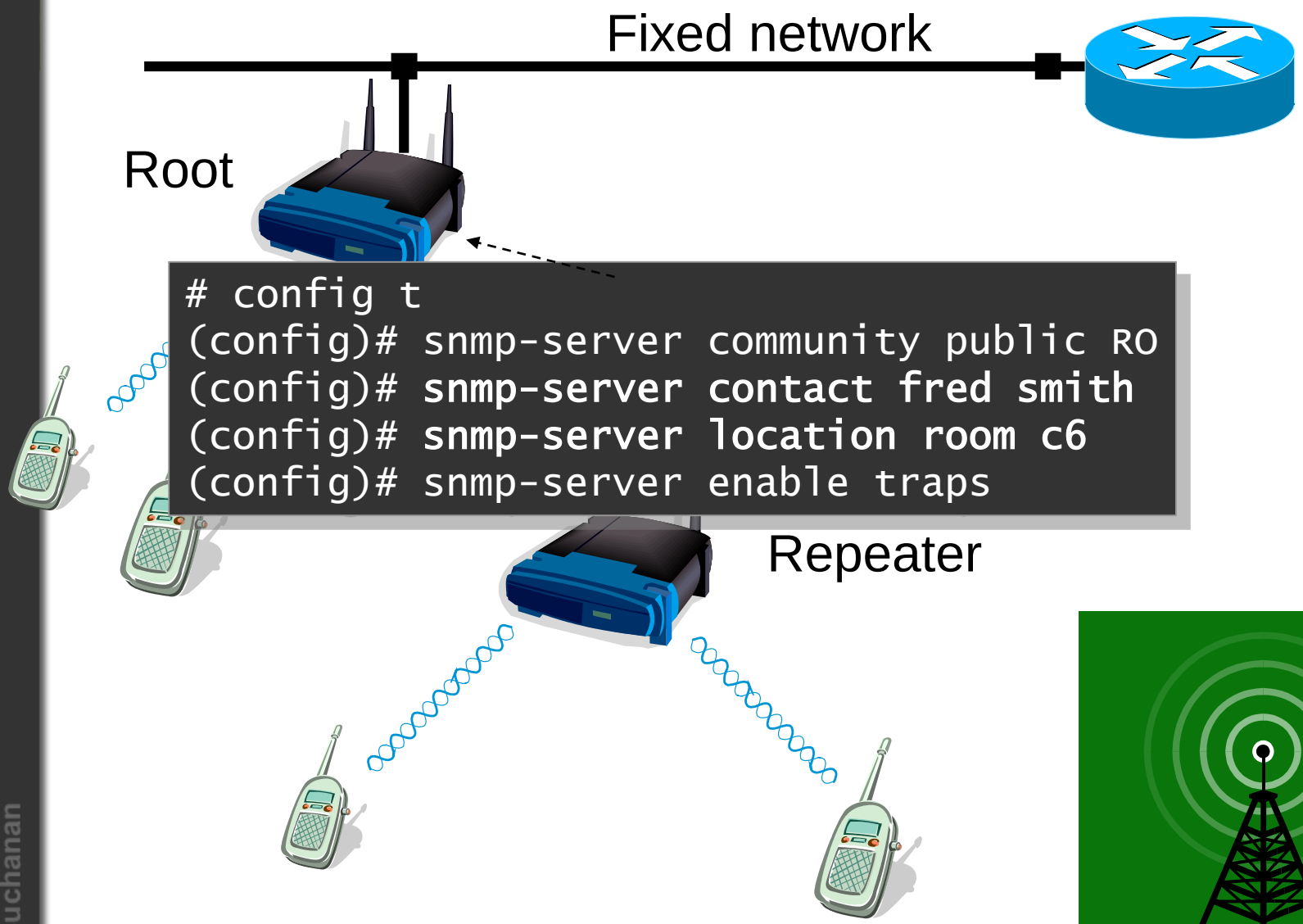
- iso(1).
- org(3).
- dod(6).
- internet(1).
- mgmt(2).
- mib-2(1).
- icmp(5).
- icmpInMsgs(1)


SNMP agent
MIB
At (address translation):
atTable.
System:
sysObjectID.
sysUpTime.
sysContact.
sysName.
sysLocation.
Interfaces:
ifNumber.
ifTable.
Ip:
ipForwarding.
ipDefaultTTL.
ipInReceives.
ipInHdrErrors.
Etc.
ICMP:
IcmpInMsgs.
IcmpInErrors.
Etc.
UDP:
udpInDatagrams.
udpNoPorts.
udpInErrors.
Etc.
SNMP:
snmpInPkts.
snmpOutPkts.
Etc.
TCP:
tcpRtoAlgorithm.
tcpRtoMin.
tcpRtoMax.
Etc.

- ifNumber. Number of interfaces.
- ifTable. List of interface entities:
  - ifIndex. Interface index value.
  - ifDescr. Interface description.
  - ifType. Interface type: other(1), regular1822(2), hdh1822(3), ddn-x25(4), rfc877-x25(5), ethernet-csmacd(6), iso88023-csmacd(7), iso88024-tokenBus(8), iso88025-tokenRing(9), iso88026-man(10), starLan(11), proteon-10Mbit(12), proteon-80Mbit(13), hyperchannel(14), fddi(15), lapb(16), sdlc(17), ds1(18), e1(19), basicISDN(20), primaryISDN(21), ppp(23), softwareLoopback(24), eon(25), ethernet-3Mbit(26))
  - ifSpeed. Speed of interface, in bits per second.
  - ifPhysAddress.
  - ifAdminStatus. Administration status is Up (1), down (2) or testing (3).
  - ifOperStatus. Operational status is Up (1), down (2) or testing (3).
  - ifLastChange. Time since last change.
  - ifInUcastPkts.
  - ifInNUcastPkts.
  - ifInDiscards.
  - ifInErrors.
  - …
  - ifOutErrors.
  - ifOutQLen.
  - ifSpecific.

- ipForwarding. Defines whether the node is a gateway or not. It can be set to: forwarding (for a gateway) or not-forwarding.
- ipDefaultTTL. IP Time-to-live.
- ipInReceives. The total number of IP packets (including ones in error).
- ipInHdrErrors. Discarded IP packets, due to header problems.
- ipInAddrErrors . Discarded IP packets, due to incorrect addresses (such as 0.0.0.0).
- ipForwDatagrams. Number of IP packets which were forwarded.
- ipInUnknownProtos. Number of IP packets with an unknown protocol.
- ipInDiscards. Discarded packets due to processing problems, such as lack of buffer memory.
- ipInDelivers. Number of successfully IP packets.
- ipOutRequests.
- ipOutDiscards.
- ipOutNoRoutes. Discarded IP packets, due to no router for the packets.
- ipFragOKs. Number of completed fragments.
- ipFragFails. Number of unsuccessful fragments.
- ipFragCreates. Number of fragments created.
- ipAddrTable.
- ipAddrEntry:
  - ipAdEntAddr. Network address.
  - ipAdEntIfIndex. Address index.
  - ipAdEntNetMask. Subnet mask.
  - ipAdEntBcastAddr. Broadcast address.
  - ipAdEntReasmMaxSize.
- ipRoutingTable:
  - ipRouteDest. Destination address. A value of 0.0.0.0 is defined as a default route.
  - ipRouteIfIndex Route index.
  - ipRouteMetric1. Route metric 1. If it is not using the value is set to -1.
  - ...


SNMP Trap
Trap Receiver
Rule Processor
Action Processor
Alert!




```
# config t
(config)# snmp-server community public RO
(config)# snmp-server contact fred smith
(config)# snmp-server location room c6
(config)# snmp-server enable traps
```

MIB name	Description	OID
• sysName	Hostname	.1.3.6.1.2.1.1.5.0
• sysUpTime	Uptime	.1.3.6.1.2.1.1.3.0
• sysDescr	System Description	.1.3.6.1.2.1.1.1.0
• sysContact	System Contact	.1.3.6.1.2.1.1.4.0
• sysLocation	System Location	.1.3.6.1.2.1.1.6.0
• ciscoImageString.5	IOS Version	.1.3.6.1.4.1.9.9.25.1.1.1.2.5
• avgBusy1	1-Minute CPU Util.	.1.3.6.1.4.1.9.2.1.57.0
• avgBusy5	5-Minute CPU Util.	.1.3.6.1.4.1.9.2.1.58.0
• freeMem	Free memory	.1.3.6.1.4.1.9.2.1.8.0
• ciscoImageString.4	IOS feature set	.1.3.6.1.4.1.9.9.25.1.1.1.2.4

Keyword	Description
• internet	Entire MIB tree
• mib-2	Entire MIB-II tree
• system	System branch of the MIB-II tree
• interfaces	Interface branch of the MIB-II tree
• at	ARP table branch of the MIB-II tree
• ip	IP routing table branch of the MIB-II tree
• icmp	ICMP statistics branch of the MIB-II tree
• tcp	TCP statistics branch of the MIB-II tree
• udp	UDP statistics branch of the MIB-II tree
• transmission	Transmission statistics of the MIB-II tree
• snmp	SNMP statistics branch of the MIB-II tree
• ospf	OSPF MIB
• bgp	BGP MIB
• rmon	RMON MIB
• cisco	Cisco's enterprise MIB tree
• x25	X.25 MIB
• ifEntry	Interface statistics MIB objects
• lsystem	Cisco's system MIB

Keyword	Description
• bgp	Allow BGP state change traps
• bstun	Allow bstun event traps
• config	Allow SNMP configuration traps
• dlsw	Allow DLSw traps
• dsp	Allow SNMP DSP traps
• dspu	Allow dspu event traps
• entity	Allow SNMP entity traps
• envmon	Allow environmental monitor traps
• frame-relay	Allow SNMP Frame Relay traps
• hsrp	Allow SNMP HSRP traps
• ipmulticast	Allow SNMP IP multicast traps
• isdn	Allow SNMP ISDN trap
• msdp	Allow SNMP MSDP traps
• rsrb	Allow rsrb event traps
• rsvp	Allow RSVP flow change traps
• rtr	Allow SNMP Response Time Reporter (RTR) traps
• sdlc	Allow SDLC event traps
• sdllc	Allow SDLLC event traps
• snmp	Allow SNMP-type notifications
• stun	Allow stun event traps

FreeSnmp

Pro version is available in Nsauditor...Over 35 network tools in one program for scanning, sniffing, enumerating... Download Here...

IP Addr: 192 . 168 . 1 . 110 Description: System

OID: .1.3.6.1.2.1.1 Walk

```
Variable = system.sysDescr.0
Value  = Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(11)JA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 23-May-
Variable = system.sysObjectID.0
Value  = 1.3.6.1.4.1.9.1.525
Variable = system.sysUpTime.0
Value  = 183076
Variable = system.sysContact.0
Value  =
Variable = system.sysName.0
Value  = ap
Variable = system.sysLocation.0
Value  =
Variable = system.sysServices.0
Value  = 2
Variable = system.8.0
Value  = 0
```

FreeSnmp

Pro version is available in Nsauditor...Over 35 network tools in one program for scanning, sniffing, enumerating... Download Here...

IP Addr: 192 . 168 . 1 . 110 Description: Interfaces

OID: .1.3.6.1.2.1.2 Walk

```
Variable = interfaces.ifNumber.0
Value  = 5
Variable = interfaces.ifTable.ifEntry.ifIndex.1
Value  = 1
Variable = interfaces.ifTable.ifEntry.ifIndex.2
Value  = 2
Variable = interfaces.ifTable.ifEntry.ifIndex.3
Value  = 3
Variable = interfaces.ifTable.ifEntry.ifIndex.4
Value  = 4
Variable = interfaces.ifTable.ifEntry.ifIndex.5
Value  = 5
Variable = interfaces.ifTable.ifEntry.ifDescr.1
Value  = Dot11Radio0
Variable = interfaces.ifTable.ifEntry.ifDescr.2
Value  = FastEthernet0
Variable = interfaces.ifTable.ifEntry.ifDescr.3
Value  = Null0
Variable = interfaces.ifTable.ifEntry.ifDescr.4
Value  = BVI1
Variable = interfaces.ifTable.ifEntry.ifDescr.5
Value  = Virtual-Dot11Radio0
Variable = interfaces.ifTable.ifEntry.ifType.1
```

Variable = system.sysDescr.0
Value = Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(11)JA, EARLY DEPLOYMENT RELEASE SOFTWARE (fc2)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 23-May-
Variable = interfaces.ifNumber.0, Value = 5
Variable = interfaces.ifTable.ifEntry.ifIndex.1, Value = 1
Variable = interfaces.ifTable.ifEntry.ifIndex.2, Value = 2
Variable = interfaces.ifTable.ifEntry.ifIndex.3, Value = 3
Variable = interfaces.ifTable.ifEntry.ifIndex.4, Value = 4
Variable = interfaces.ifTable.ifEntry.ifIndex.5, Value = 5
Variable = interfaces.ifTable.ifEntry.ifDescr.1, Value = Dot11Radio0
Variable = interfaces.ifTable.ifEntry.ifDescr.2, Value = FastEthernet0
Variable = interfaces.ifTable.ifEntry.ifDescr.3, Value = Null0
Variable = interfaces.ifTable.ifEntry.ifDescr.4, Value = BVI1
Variable = interfaces.ifTable.ifEntry.ifDescr.5, Value = Virtual-Dot11Radio0