Techtronica

NETWORKING (ROUTERS AND SWITCHES)

Presented by- Priyanshi Bansal

Aviral Kulshrestha

INDEX

- Basics of Networking
- IP address/MAC address
- OSI model
- Router/Switch
- How internet works ?
- Packet Flow
- Basics of WIRELESS Technology
- Requirement to create wireless network
- Radio Frequency Signal
- Basics of Cloud
- Cloud Structures

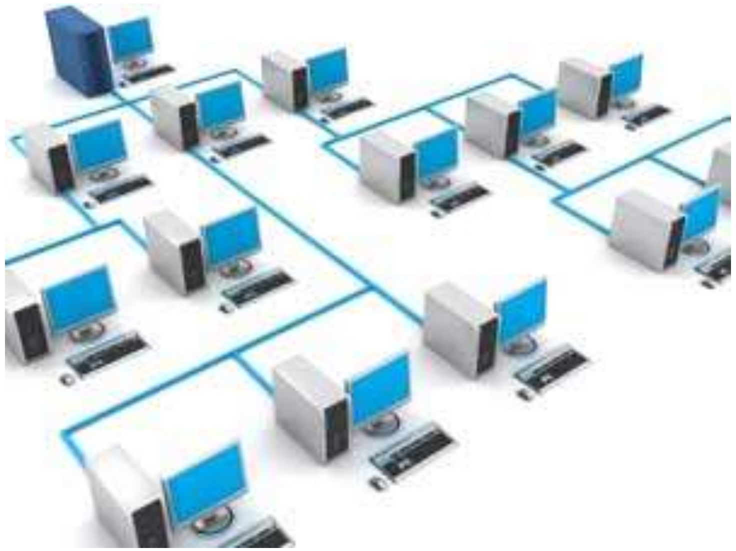
WHAT IS NETWORK ?

- It is a practice of connecting multiple computing devices .
- Here , devices can be – desktop/mobile ,

  laptop , servers etc.
- Connected either through wired or wireless medium .
- To allow sharing resourcing, exchanging files or allow

  communication .
- Example – internet which connects millions of

  people all over the world.



Techtronica

where ideas flow without resistance

WHY DO WE NEED NETWORK ?

- **Older ways to communicate –**

Floppy disk

- **Problem –**

  - Time consuming

  -No security

  -Storage

  -High cost

Floppy disk

ADVANTAGES :

- Fast
- Security
- Acknowledgement
- Boost Storage Capacity
- Saves Resources

Techtronica

Types of Networking

On the basis of area of they cover

- **PAN (personal area network)** :

  uses wireless technology ex. Bluetooth , Hotspots etc. and also be connected through USB cables.

- **LAN (Local Area Network)** :

  Connected devices that are located in a schools , homes and colleges etc .

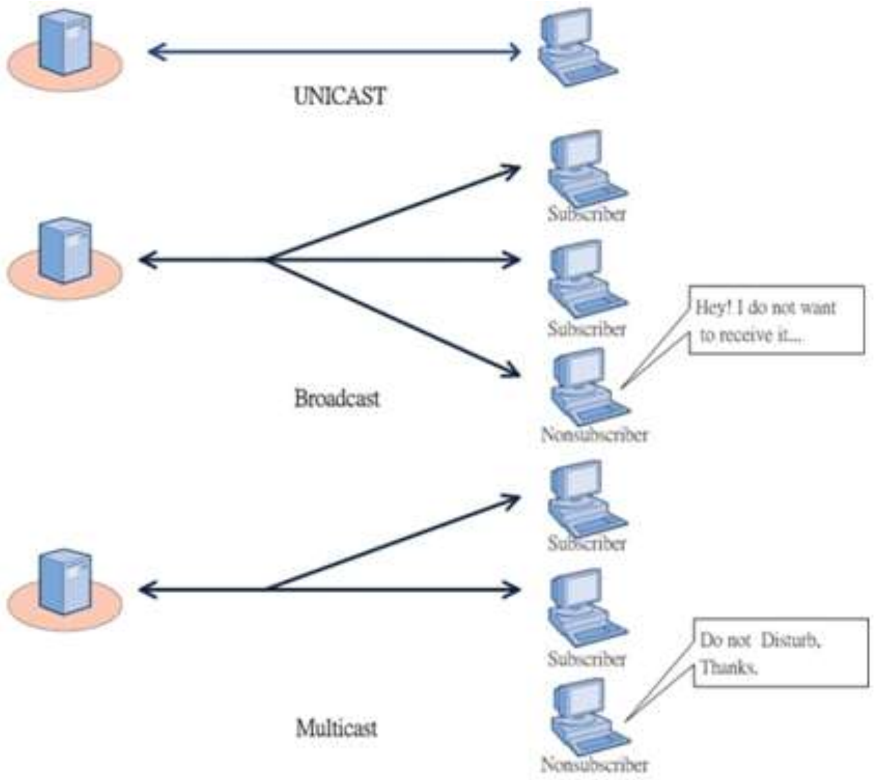
- **WAN (Wide Area Network) :**

  Connects smaller networks across long distances .

Types Of Communication

- **Unicast** : one to one communication .
- **Multicast :** one to many communication.
- **Broadcast :** one to all communication

  but within the network.



Modes Of Communication

- **Simplex** : One way communication.

  Ex – radio, broadcasting , TV broadcasting etc.

- **Half Duplex** : Two way Communication .

  Ex- wacky tacky etc.

- **Full Duplex** : Two way communication at a same time .

  Ex – Mobile phones etc.

Techtronica

IP ADDRESS
(Internet Protocol address)

- An IP address is numerical representation that uniquely identifies a specific interface on the network .
- It is 32 bit long i.e. 192.162.58.1
- It is unique address
- Two types of Networking :

- IPV4 (32 bit long)

- IPV6 (128 bit long)

- IP address is a logical address .

MAC ADDRESS
(Media Access Control Address)

- It is device identity which is given when it is manufactured .
- MAC address are primarily assigned by device manufacturers
- It is 48 bit long (written in hexadecimal form)
- "Burned-in address or Ethernet hardware address , hardware address and physical address"

OSI MODEL
(Open System Interconnection)

- Any data transmitted from any source passes through

  Seven different layers(steps) to reach at the destination (developed by ISO)

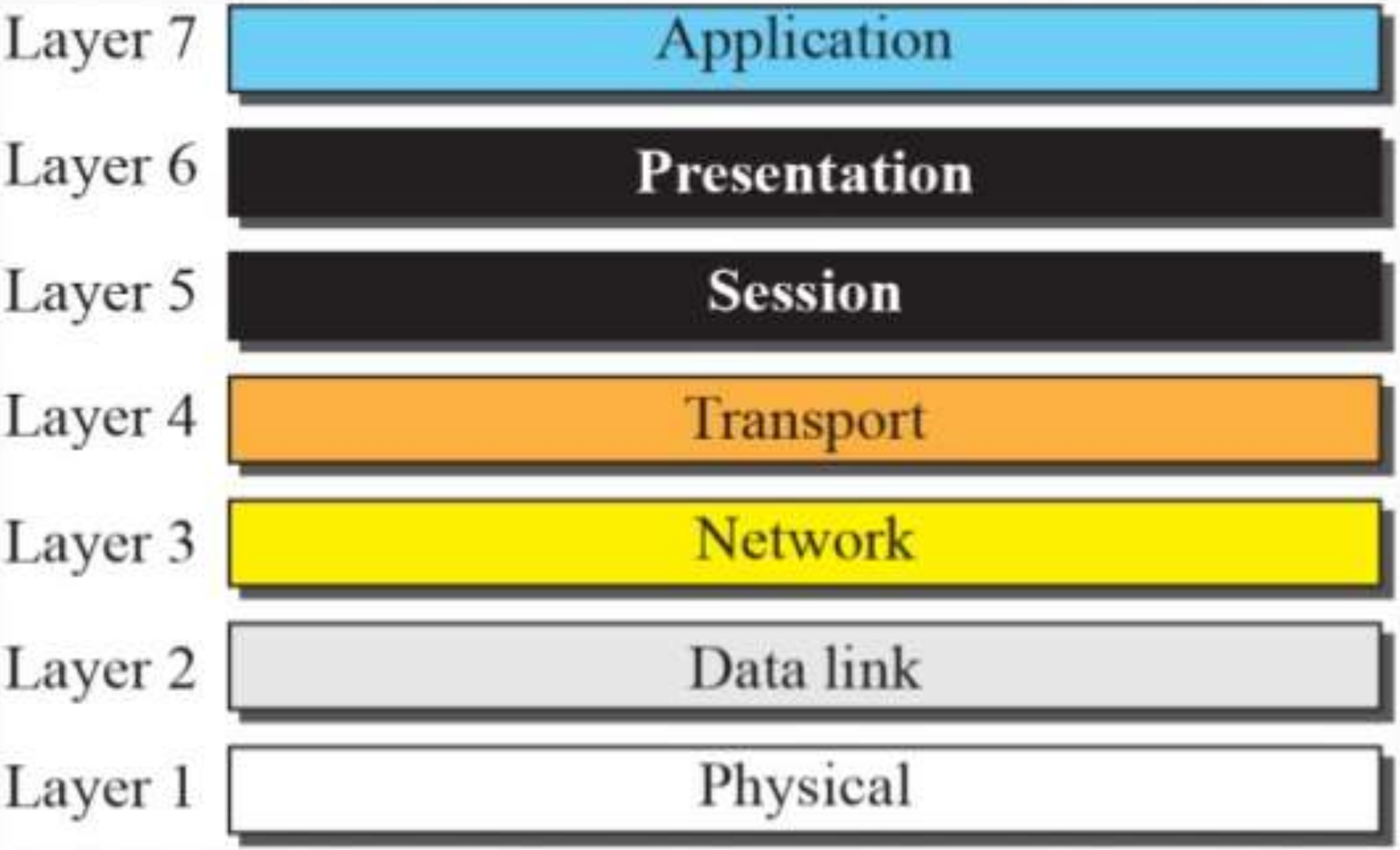
- The sum of these seven layers is called OSI model .

NEED OF OSI MODEL

Interoperability

- OSI Model came into existence in order to communicate with different Operating System .

Seven layers of the OSI model:



Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

Layer 2 Data link

Layer 1 Physical

LAYER 7 : Application Layer

- It provide user interface .

  - Ex. When we try to connect through any website like HDFC bank .

- Provoke application layer protocol .

  - Ex - will automatically call https protocol .

- Some other protocol :

  -FTP (File Transfer Protocol)

  -DHCP (Dynamic Host Configuration Protocol)

  -DNS (Domain Name System)

  and many more

Techtronica
where ideas flow without resistance

LAYER 6 : Presentation Layer

- It present the data into an standard format .
- Encryption - plain text into cipher text .
- Decryption - cipher text into plain text .
- Compress - like creating a zip file .
- Decompress – act of expanding a file back into its original form .

Source

Destination

Techtronica

LAYER 5 : Session layer

- It is responsible for

  - creating

  - managing

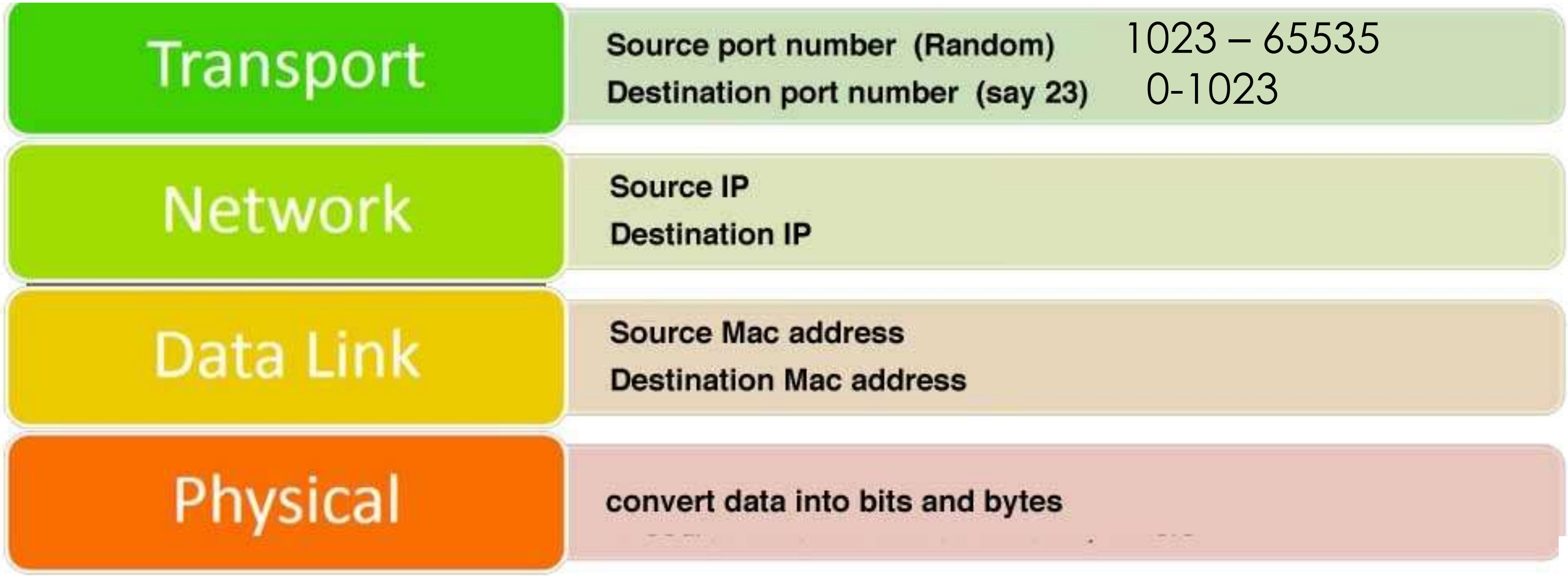
  -termination

  of the session .

- Example – In any bank website

  -authentication timeout

  - session timeout

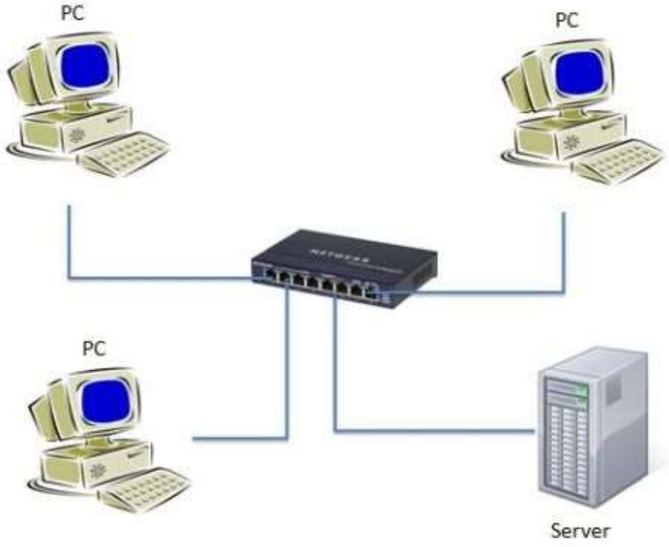


LAYER 4	Transport	Source port number (Random) Destination port number (say 23)	1023 – 65535 0-1023
LAYER 3 :	Network	Source IP Destination IP	
LAYER 2 :	Data Link	Source Mac address Destination Mac address	
LAYER 1 :	Physical	convert data into bits and bytes	

Techtronica

Switch

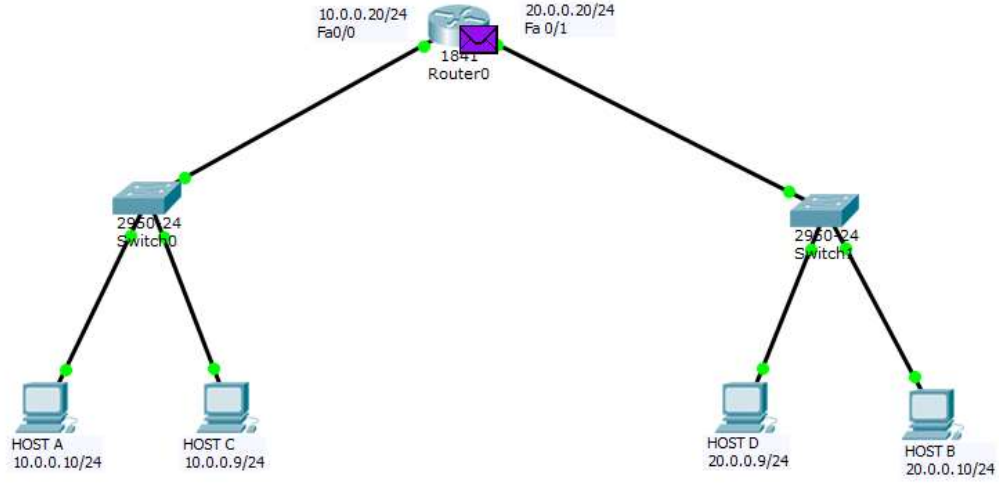
- A switch is a device in a computer network that connects other devices together.
- It is used to extend the number of ports available on your router.
- It is a full duplex device .
- It works on Mac- address i.e. makes table for different Mac-address (layer 2)



Techtronica

ROUTER

- Use to communicate with one network with different network .
- It takes packet forwarding decision on the basis of IP network .
- It works on "LAYER 3" i.e. Network Layer
- Routing : It is process of taking out the packet from one IP network to different IP network .
- Routing Table : Table stored in a router or a network or a That list the routes to particular network



Techtronica
where ideas flow without resistance

WIRELESS NETWORKING

Techtronica
where ideas flow without resistance

Problems with Wired Network

- No mobility
- Expensive to install
- More prone to damage
- Need of special connectors
- Absence of ports in small devices

Wireless Networking

- Wireless networking is used to transfer data from one device to another without any physical connection between them , i.e. without the use of any cables or wires.
- This technology is flexible , intangible and easy to access.
- It is cost effective.
- There is no need of connectors
- RF signal is used to setup connection.

Techtronica
where ideas flow without resistance

Radio frequency signal(RF Signal)

- Range : 30 kHz to 300 Ghz
- The medium of transmission is air.
- This signal falls under the category of EM waves as they only can propagate in air.
- Uses-

1- They provide the means for carrying music to FM radios and video to televisions.

2- It is used in medical treatments such as cosmetic treatments that tighten skin, reduce fat or promote healing.

3- MRI

4- Destroying cancer cells

And many more

Techtronica

Requirement to create wireless network

- Network Interface Card(NIC) is used for wireless networks.
- Access points for generating signal and establishing connection between devices.
- Device which has a wireless signal adapter.

Modes of wireless communication

- The network connection can happen in two modes-

1- Half Duplex mode-

When both parties transmit and receive on same frequencies then the network operates in half duplex mode.

2- Full Duplex mode-

When both parties use individual frequency to transmit and receive then the network operates in full duplex mode.

Techtronica

Terminologies in wireless networking

- SSID - A service set identifier (SSID) is a sequence of characters that uniquely names a wireless network.
- BSSID- The BSSID is the MAC address associated with SSID.
- AP- Access Point (AP) is a centralized device which connects multiple deices through the wireless network.
- 802.11 standard- 802.11 is a standard that was developed by the Institute of Electrical and Electronic Engineers (IEEE). It is the original wireless specification.

Basic Service Set

- The Basic Service Set is a term used to describe the collection of Stations which may communicate together within an 802.11 network.
- At the heart of every BSS is a wireless *access point* (AP)
- The AP and the members of the BSS must all use the same channel to communicate properly.
- BSSID as a machine-readable name tag that uniquely identifies the access point.
- Membership with the BSS is called an *association*.
- If clients are allowed to communicate directly, then the whole idea of organizing and managing a BSS is disputive. By sending data through the AP first, the BSS remains stable and under control.

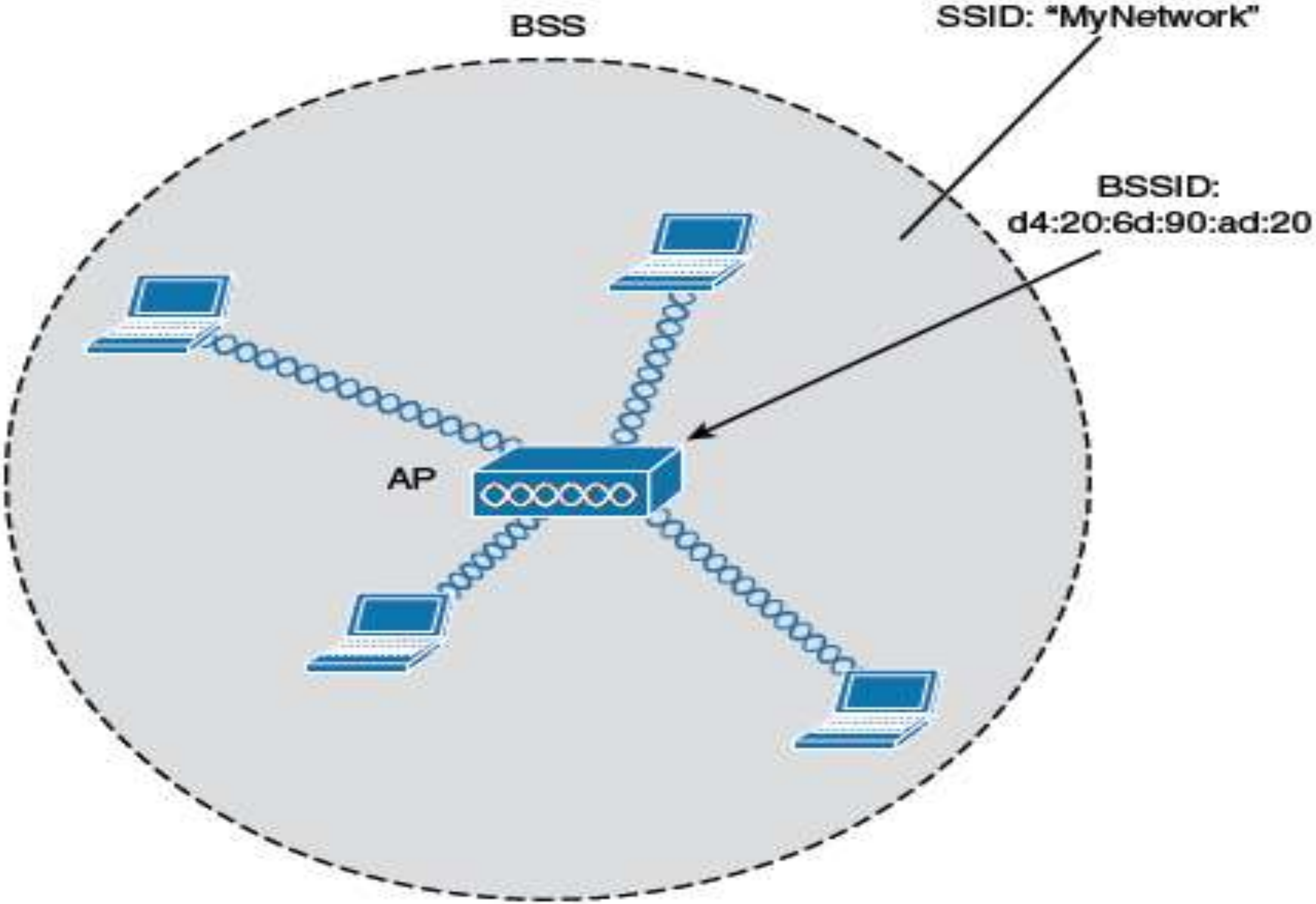


Figure 26-4 *802.11 Basic Service Set*

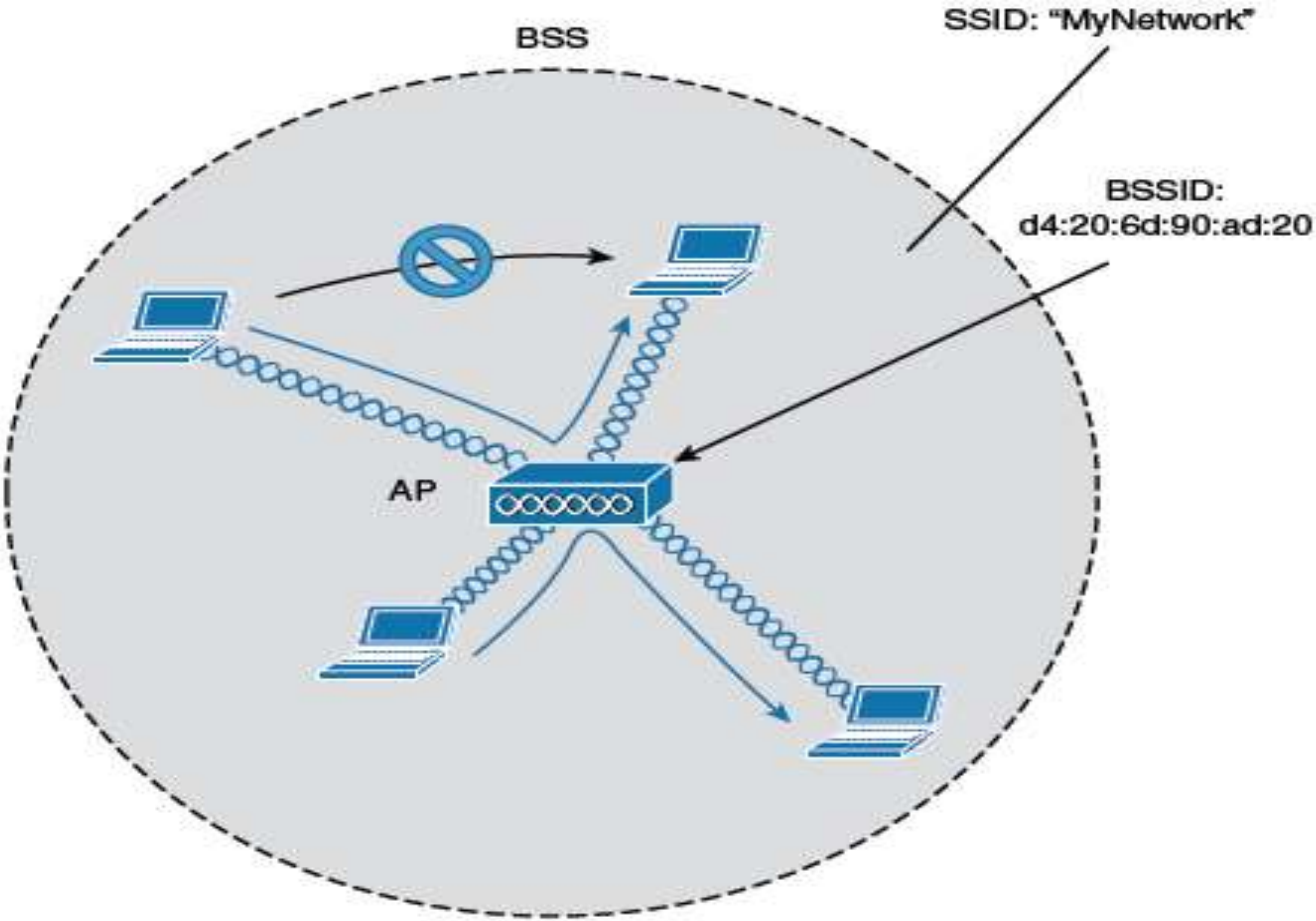


Figure 26-5 *Traffic Flows Within a BSS*

Distributed System

- A distributed system contains multiple nodes that are physically separate but linked together using the network.
- An AP can also uplink into an Ethernet network because it has both wireless and wired capabilities.
- The 802.11 standard refers to the upstream wired Ethernet as the *distribution system* (DS).
- AP as a translational bridge, where frames from two dissimilar media (wireless and wired) are translated.
- This concept can be extended so that multiple VLANs are mapped to multiple SSIDs. To do this, the AP must be connected to the switch by a trunk link that carries the VLANs.

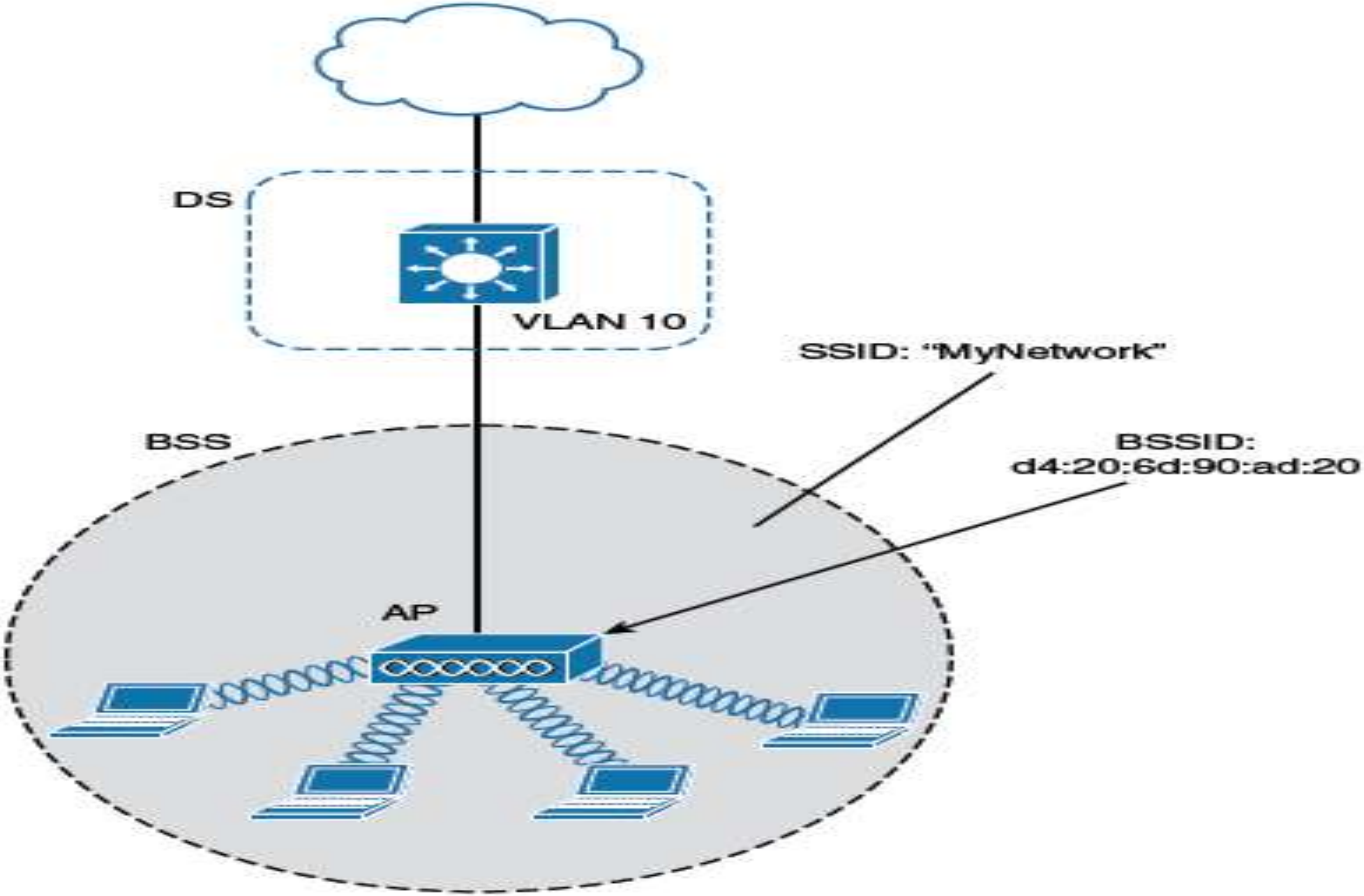


Figure 26-6 *Distribution System Supporting a BSS*

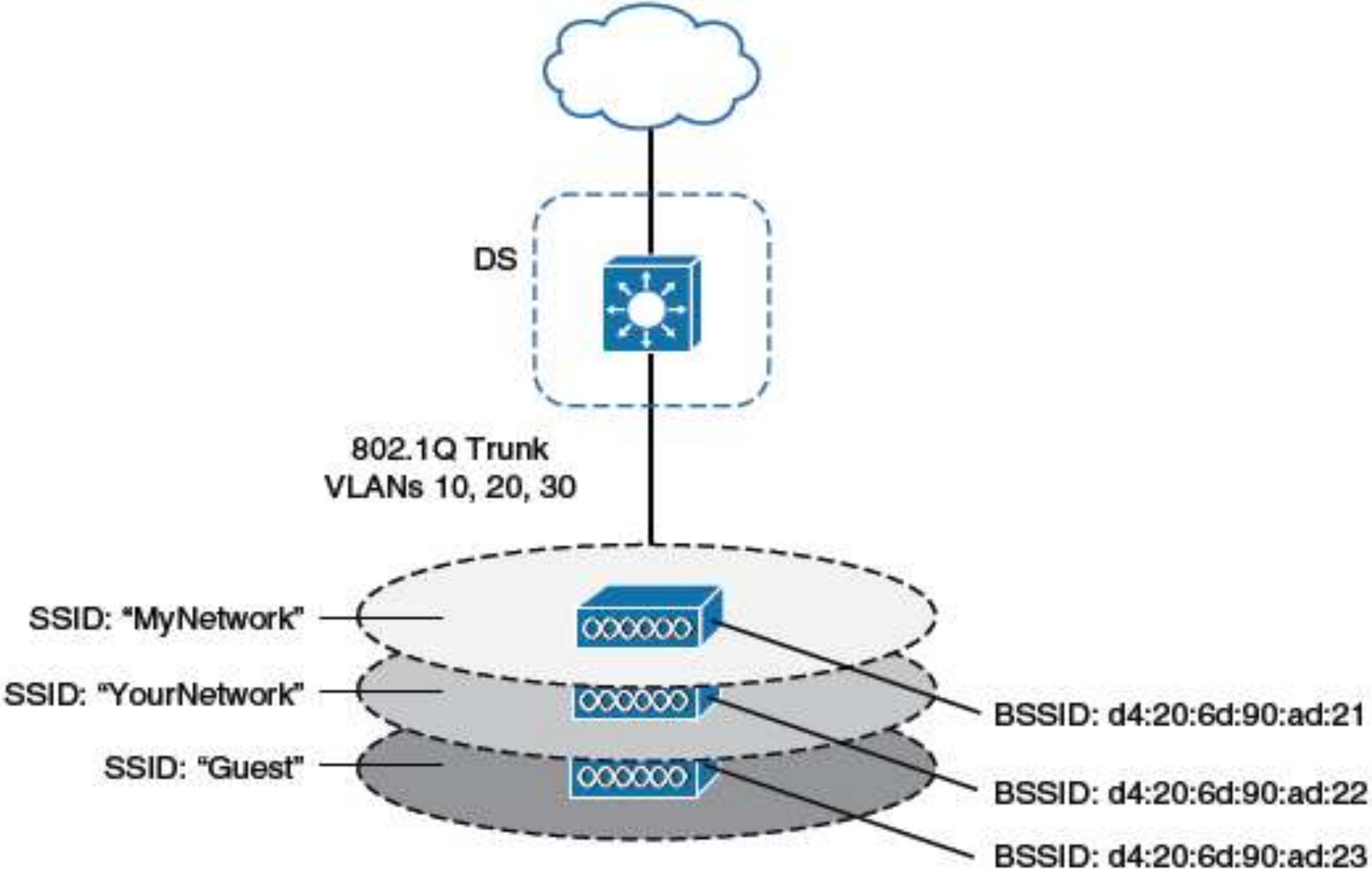


Figure 26-7 *Supporting Multiple SSIDs on One AP*

Extended Service Set

- An extended service set (ESS) is one or more interconnected basic service sets (BSSs) and their associated LANs.
- Each BSS consists of a single access point (AP) together with all wireless client devices (stations, also called STAs) creating a local or enterprise 802.11 wireless LAN
- The idea is to make multiple APs cooperate so that the wireless service is consistent and seamless from the client’s perspective.
- Ideally, any SSIDs that are defined on one AP should be defined on all the APs in an ESS.
- Each cell in has a unique BSSID, but both cells share one common SSID

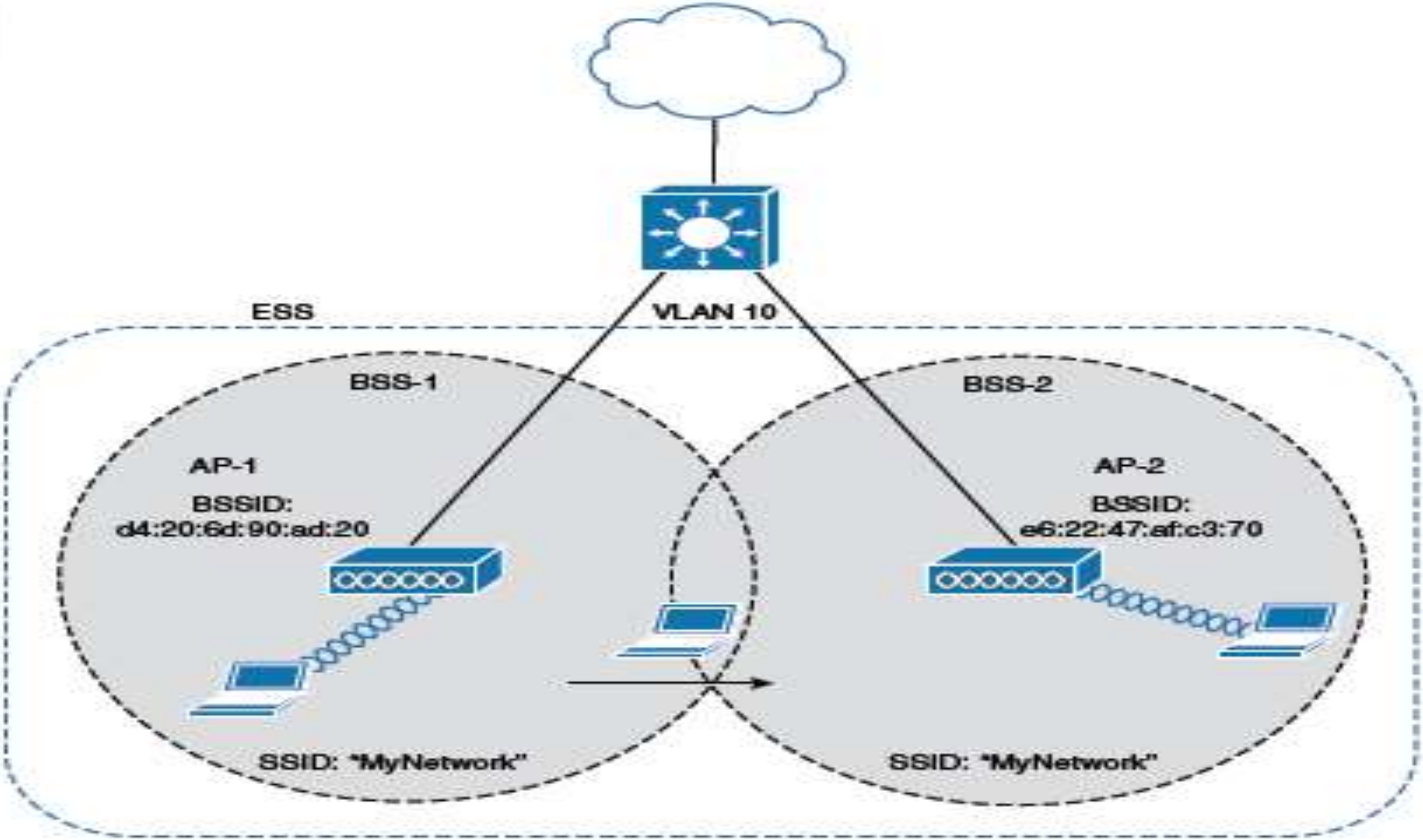


Figure 26-8 *Scaling Wireless Coverage with an 802.11 Extended Service Set*

Wireless topologies

- **Repeater-** In some scenarios, it is not possible to run a wired connection to a new AP because the cable distance is too great to support Ethernet communication.In that case, an additional AP that is configured for *repeater mode*.
- A repeater takes the area around the rep

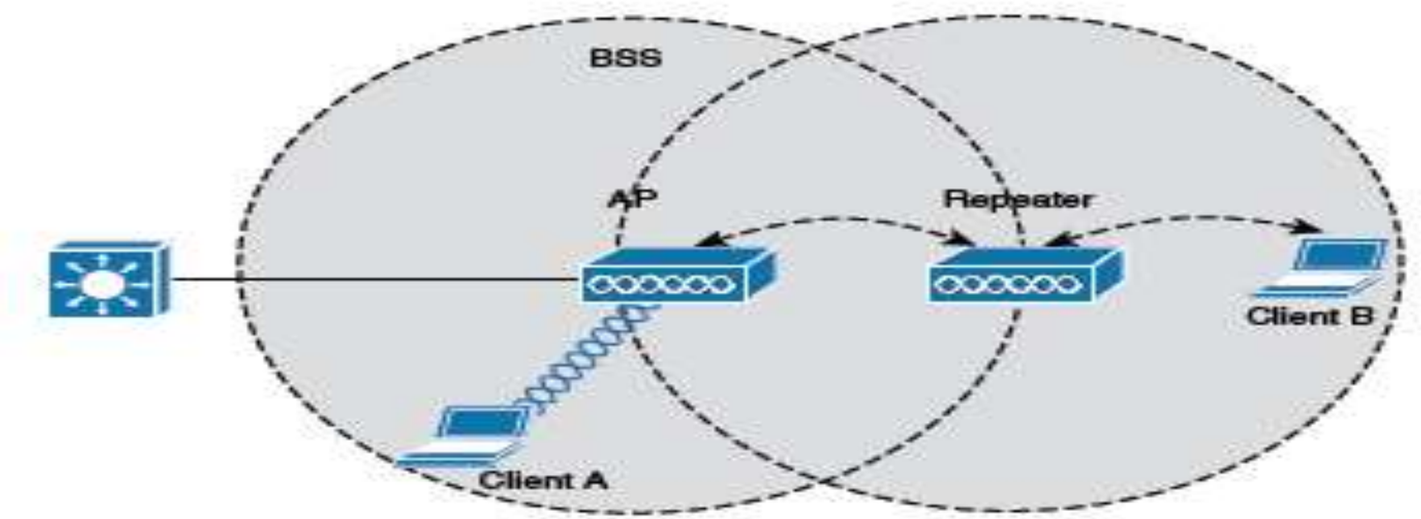


Figure 26-10 *Extending the Range of an AP with a Wireless Repeater*

Workgroup Bridge

- A work group bridge (WGB) is used to connect the device’s wired network adapter to a wireless network.
- WGB acts as an external wireless network adapter for a device that has none.

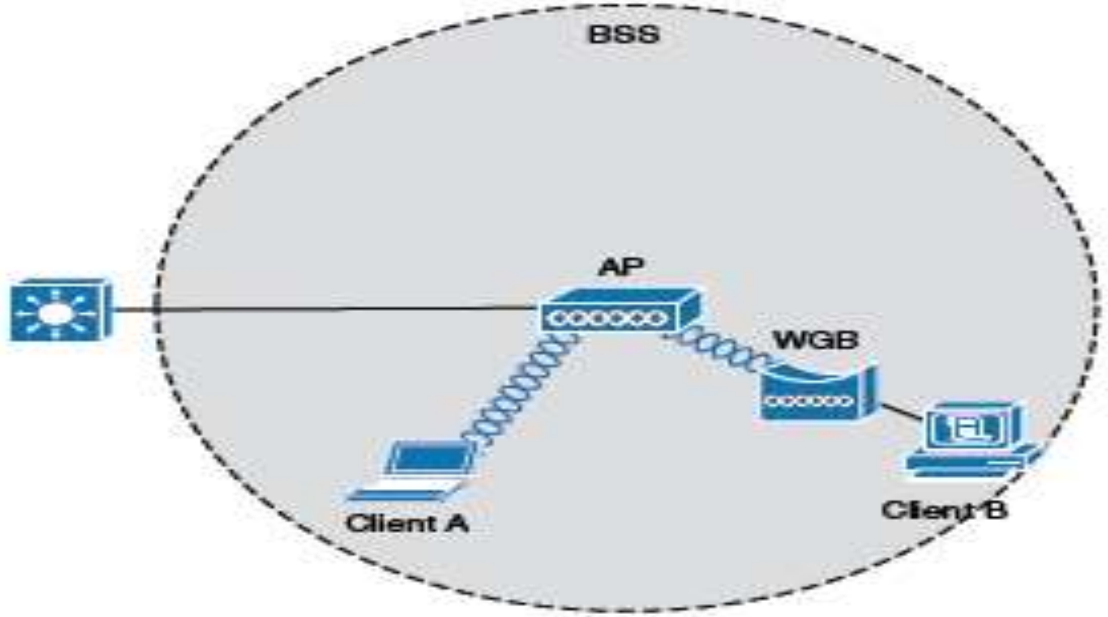


Figure 26-11 *Nonwireless Device Connecting Through a Workgroup Bridge*

Techtronica

Outdoor Bridge

- An AP can be configured to act as a bridge to form a single wireless link from one LAN to another over a long distance.
- Outdoor bridged links are commonly used for connectivity between buildings or between cities.
- If the LANs at two locations need to be bridged, a point-to-point bridged link can be used.

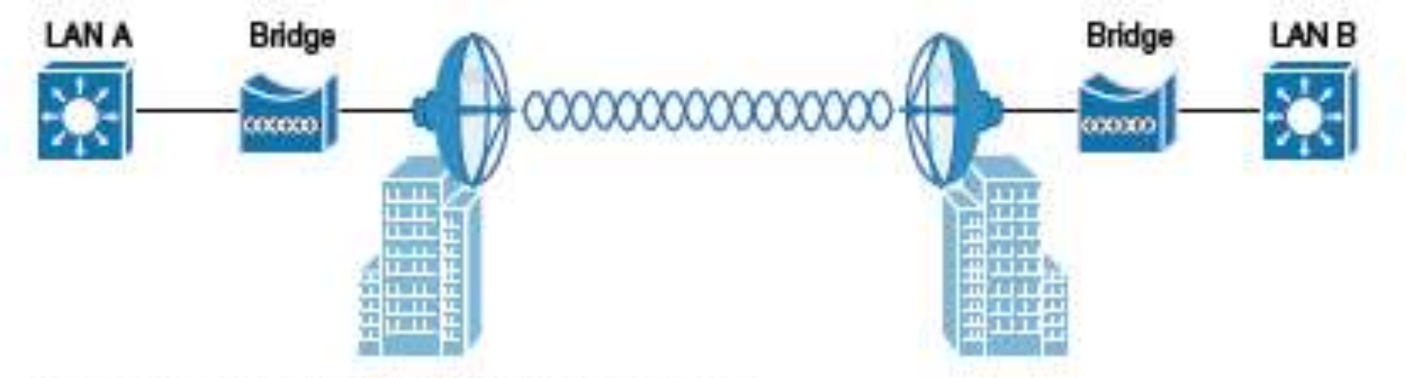


Figure 26-12 *Point-to-Point Outdoor Bridge*

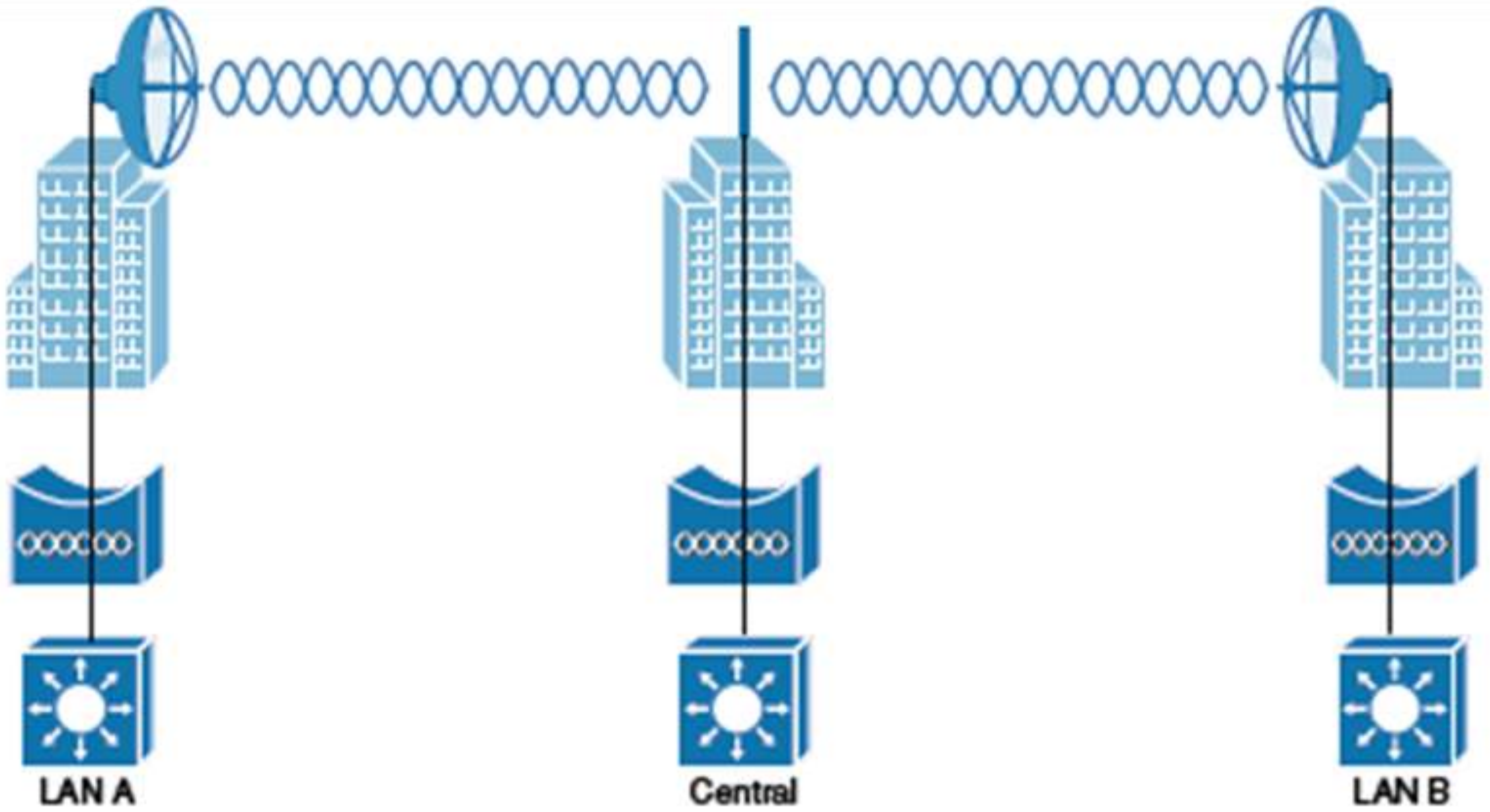


Figure 26-13 *Point-to-Multipoint Outdoor Bridge*

Sometimes the LANs at multiple sites need to be bridged together. A point-to-multipoint bridged link allows a central site to be bridged to several other sites. The central site bridge is connected to an omnidirectional antenna, such that its signal is transmitted equally in all directions so that it can reach the other sites simultaneously

Mesh Network

- In a mesh topology, wireless traffic is bridged from AP to AP, in a daisy-chain fashion, using another wireless channel.
- The mesh network runs its own dynamic routing protocol to work out the best path for backhaul traffic to take across the mesh APs.

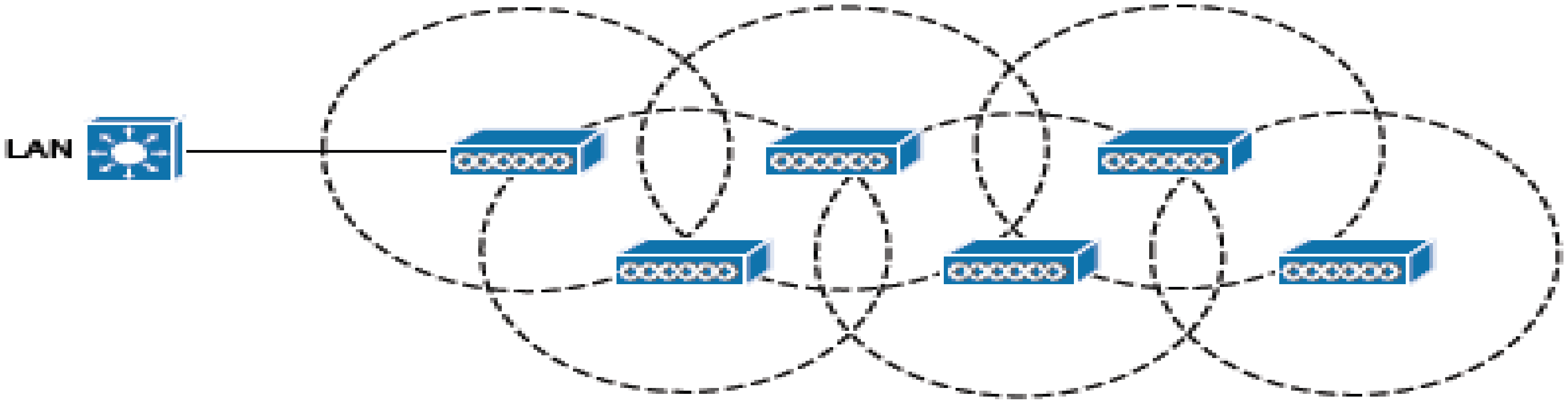


Figure 26-14 *Typical Wireless Mesh Network*

Autonomous AP Architecture

- In an autonomous architecture, access points (APs) are stand-alone (sometimes called "fat") APs that contain all the necessary features and capabilities to operate without any reliance on another device.
- An *autonomous AP* is self-contained; it is equipped with both wired and wireless hardware so that the wireless client associations can be terminated onto a wired connection locally at the AP

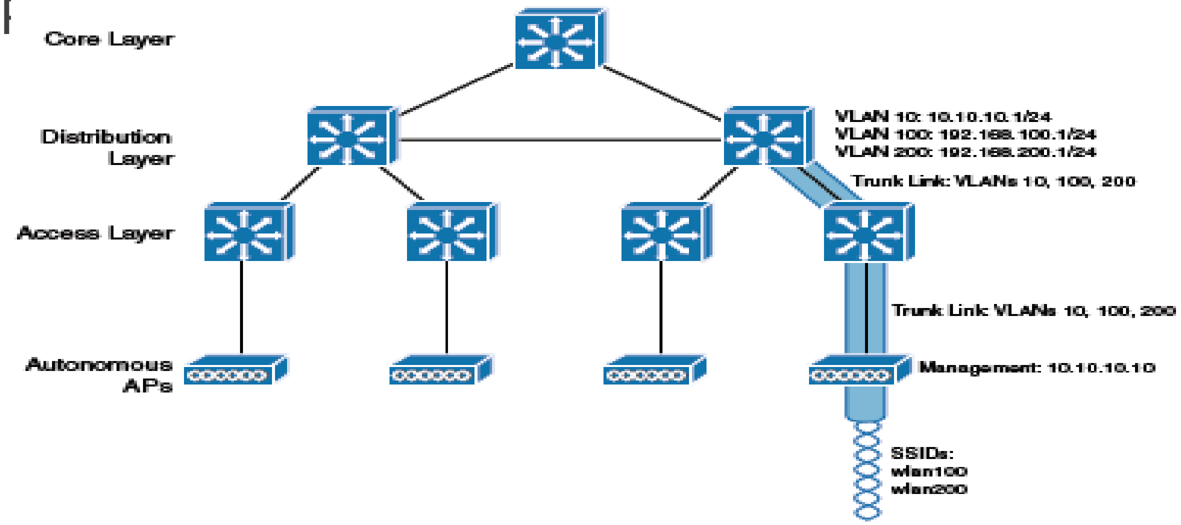


Figure 27-1 *Wireless Network Architecture with Autonomous APs*

Cloud-based AP Architecture

- A simpler approach is a cloud-based AP architecture, where the AP management function is pushed out of the enterprise and into the Internet cloud. Cisco Meraki is cloud-based and offers centralized management of wireless, switched, and security networks built from Meraki products.

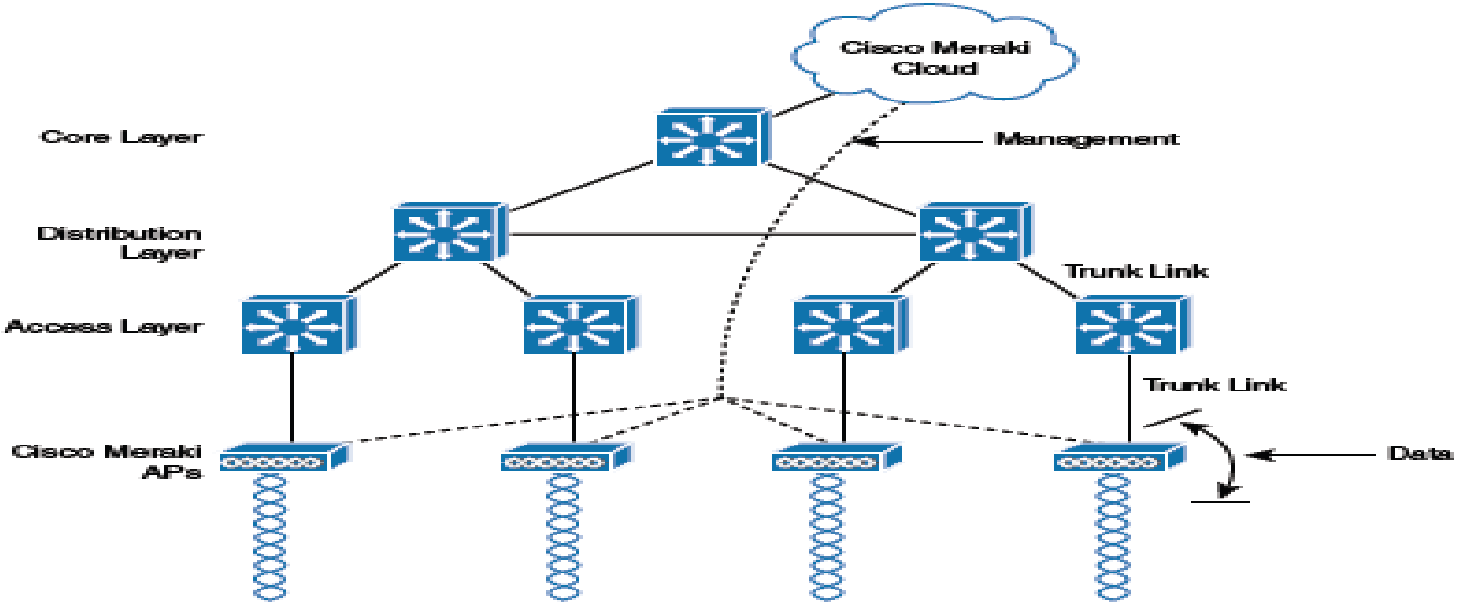


Figure 27-3 *Cisco Meraki Cloud-Based Wireless Network Architecture*

Lightweight Access Point

Lightweight Access Point is the name of a access point that can control multiple Wi-Fi wireless access points at once.

This can reduce the amount of time spent on configuring, monitoring or troubleshooting a large network.

The system will also allow network administrators to closely analyze the network.

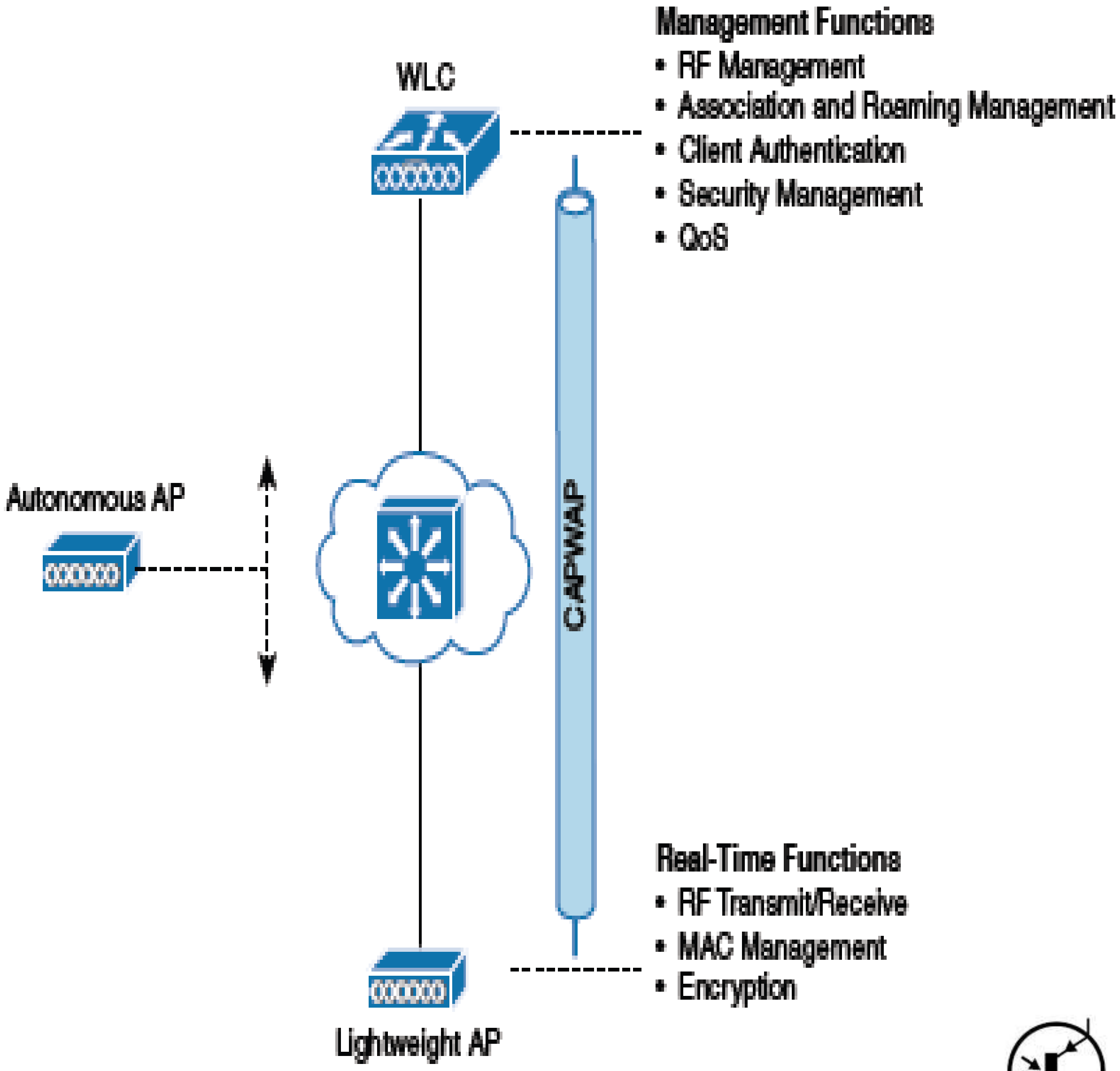


Figure 27-4 *Autonomous Versus Lightweight Access Point*

Techtronica

Security options in wireless networks-

Data can be easily hacked in wireless network if proper security is not used.

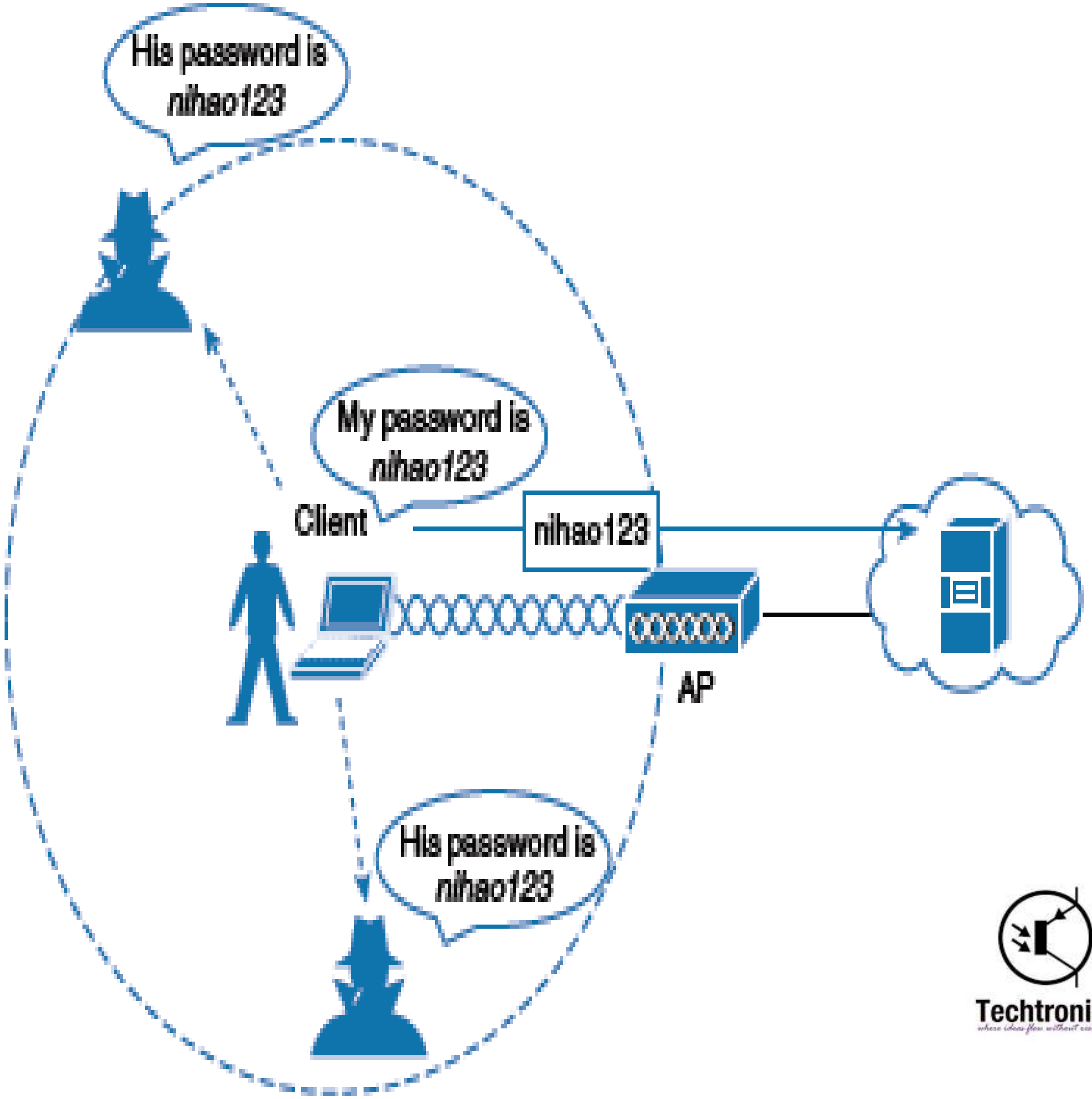
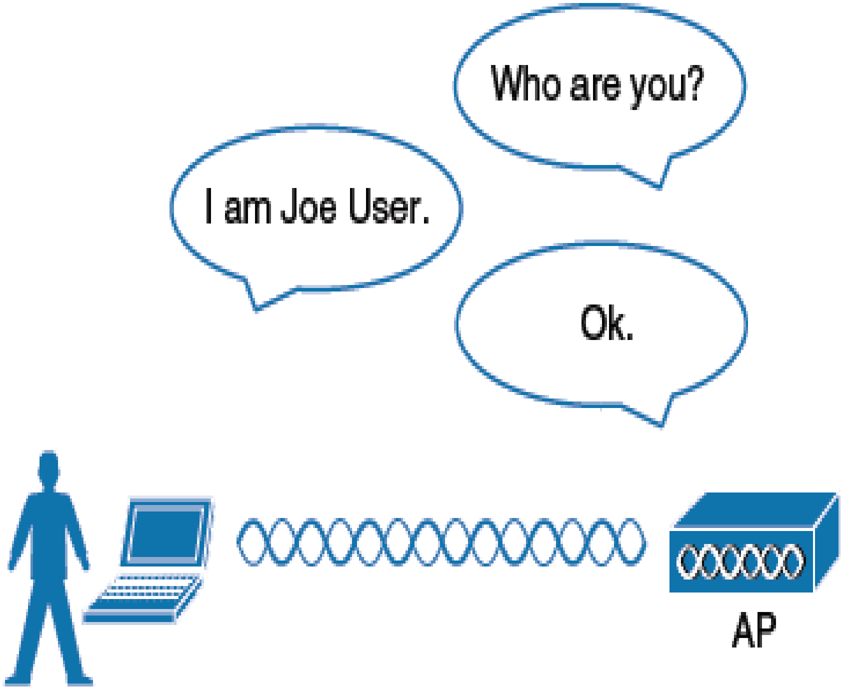
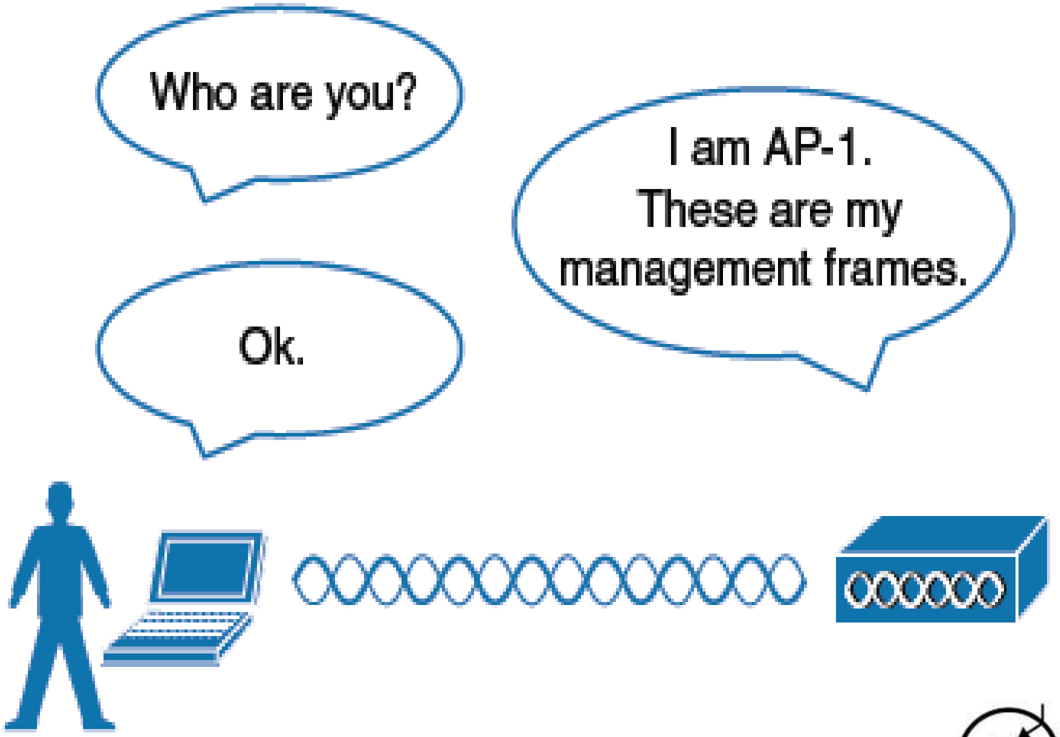


Figure 28-1 *Wireless Transmissions Reaching Unintended Recipients*

Authentication





Message Privacy

- The idea is to use an encryption method that the transmitter and receiver share, so the data can be encrypted and decrypted successfully.
- Ideally, the AP and a client are the only two devices that have the encryption keys in common so that they can understand each other's data. No other device

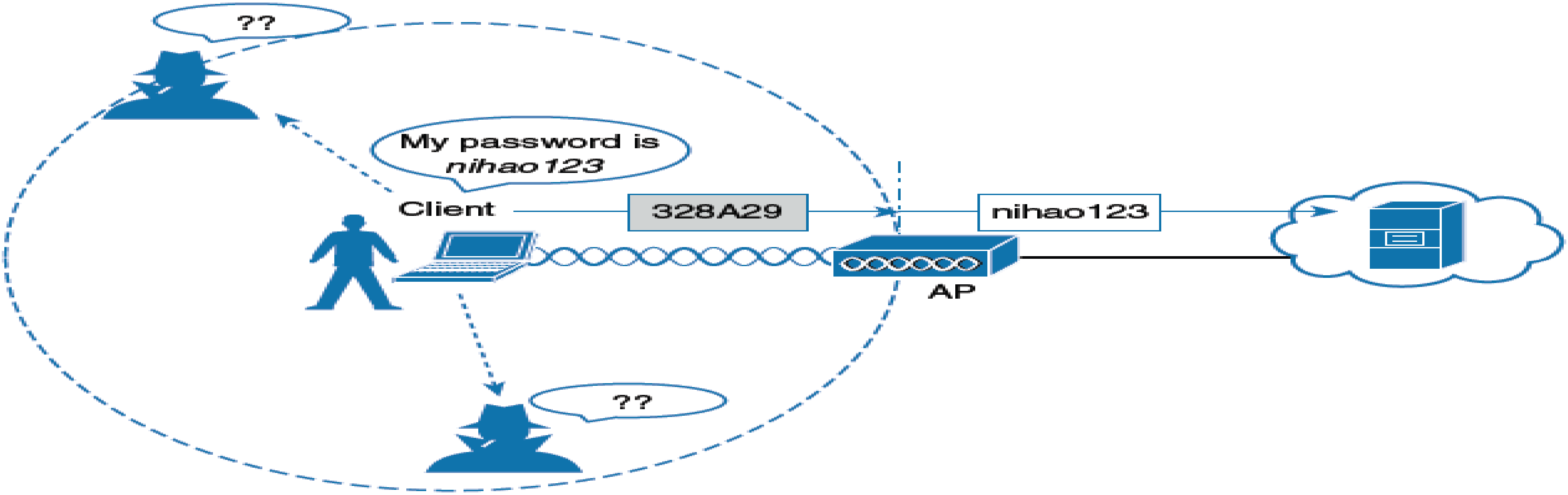


Figure 28-4 *Encrypting Wireless Data to Protect Data Privacy*

Techtronica

Wireless Client Authentication Methods

- You can use many different methods to authenticate wireless clients as they try to associate with the network.
- The methods have been introduced over time and have evolved as security weaknesses have been exposed and wireless hardware has advanced.

Open Authentication

- Open authentication is true to its name; it offers open access to a network.
- No security is there ; data is public.
- Anyone can breach the data

WEP

- It stands for Wired Equivalent Privacy.
- WEP uses the RC4 cipher algorithm to make every wireless data frame private and hidden from eavesdroppers.

WPA

- Wi-Fi Protected Access (WPA) is a security standard for users of computing devices equipped with wireless internet connections
- It required firmware upgradation instead of changing any hardware component.
- Uses TKIP(Temporal key integrity protocol)
- Better security than WEP.

WPA2

- WPA2 is the security method added to WPA for wireless networks that provides stronger data protection and network access control.
- It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.
- It has advanced security features.
- Advances Encryption Standard(AES) algorithm is used.

Cloud

- Instead of being stored directly on your own personal device (the hard drive on your laptop, for example, or your phone), cloud-based data is stored elsewhere — on servers owned by big companies, usually — and is made accessible to you via the internet.
- Cloud storage involves at least one data server that a user connects to via the internet. The user sends files manually or in an automated fashion over the Internet to the data server which forwards the information to multiple servers. The stored data is then accessible through a web-based interface.

Deployment models of cloud

There are 3 deployment models of cloud-

- Public cloud
- Private cloud
- Hybrid cloud

Public cloud

- The **public cloud** is defined as computing services offered by third-party providers over the **public** Internet, making them available to anyone who wants to use or purchase them.
- They may be free or sold on-demand, allowing customers to pay only per usage for the CPU cycles, storage, or bandwidth they consume.

Private cloud

- A private cloud is a single-tenant environment, meaning the organization using it (the tenant) does not share resources with other users.
- A private cloud is dedicated to the needs and goals of a single organization.

Hybrid Cloud

- Hybrid cloud is a solution that combines a private cloud with one or more public cloud services, with proprietary software enabling communication between each distinct service
- Hybrid cloud services are powerful because they give businesses greater control over their private data.

Service models of cloud

- There are 3 service models of the cloud-

  1- PaaS

  2- SaaS

  3- IaaS

SaaS: Software as a Service

- Software as a Service, also known as cloud application services, represents the most commonly utilized option for businesses in the cloud market. SaaS utilizes the internet to deliver applications, which are managed by a third-party vendor, to its users. A majority of SaaS applications run directly through your web browser, which means they do not require any downloads or installations on the client side.

PaaS: Platform as a Service

- Cloud platform services, also known as Platform as a Service (PaaS), provide cloud components to certain software while being used mainly for applications. PaaS delivers a framework for developers that they can build upon and use to create customized applications. All servers, storage, and networking can be managed by the enterprise or a third-party provider while the developers can maintain management of the applications.

IaaS: Infrastructure as a Service

- Cloud infrastructure services, known as Infrastructure as a Service (IaaS), are made of highly scalable and automated compute resources. IaaS is fully self-service for accessing and monitoring computers, networking, storage, and other services. IaaS allows businesses to purchase resources on-demand and as-needed instead of having to buy hardware outright.

Thank You!