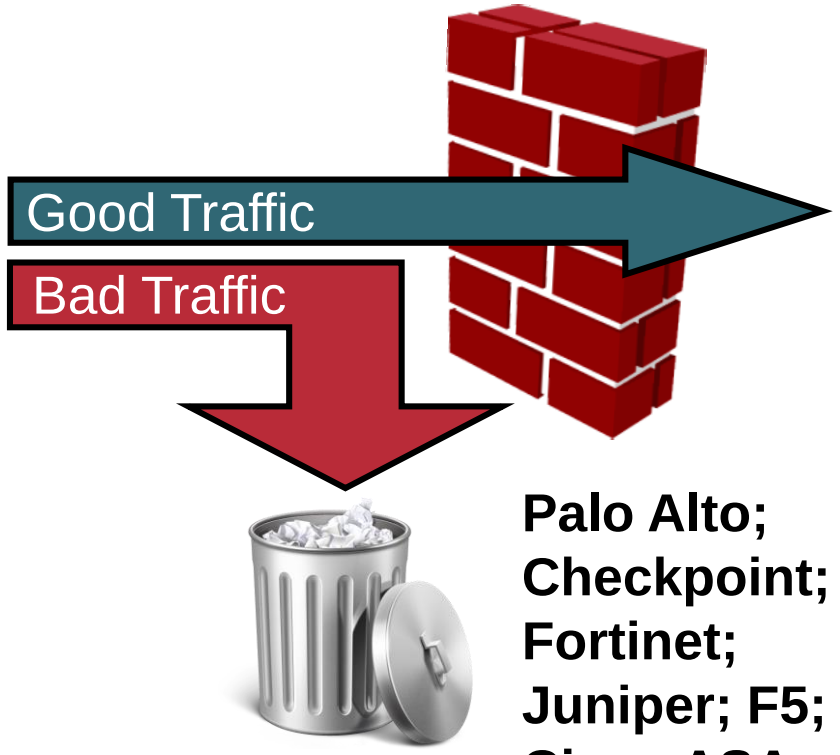
Introducing
Firewall, Access Point, Wireless Controller

What Is a Firewall?

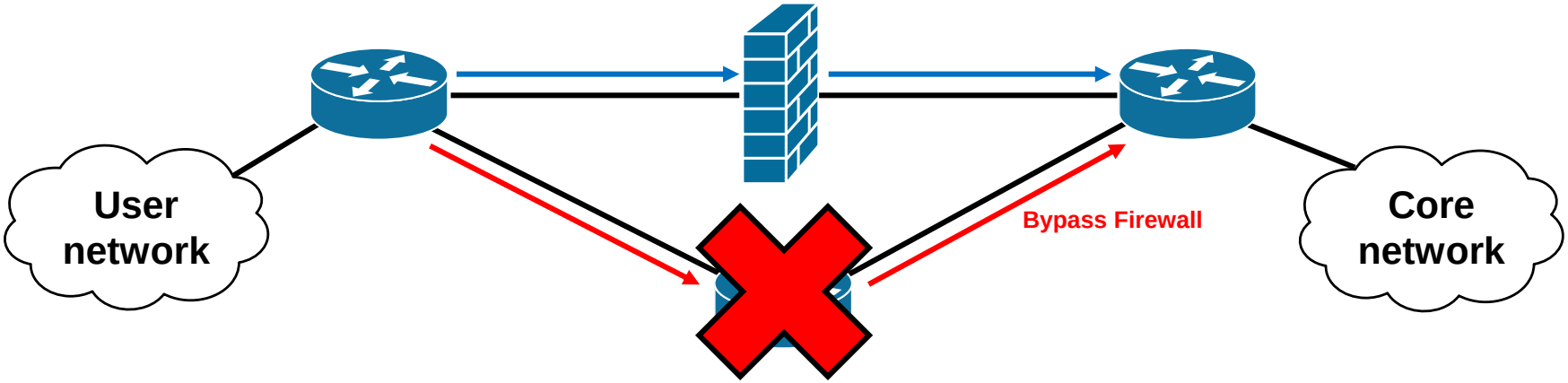
- **A firewall is a system or group of systems that enforce an access control policy between two networks.**
- **This definition is so loose that almost anything can be a firewall:**
  - A packet filtering router
  - A switch with two VLANs
  - Multiple hosts with firewalling software



Palo Alto; Checkpoint; Fortinet; Juniper; F5; Cisco ASA; McAfee, ...

Expanding on the Definition

- **Firewalls are different things to different people and organizations.**
- **All firewalls are supposed to share some common properties:**
  - The firewall itself is resistant to attacks.
  - The firewall is the only transit point between networks (all traffic flows through the firewall).
  - The firewall enforces the access control policy.



Firewall Benefits

- **A firewall can protect against**
  - Exposure of sensitive hosts and applications to untrusted users
  - Exploitation of protocol flaws by sanitizing protocol flow
  - Malicious data being sent to servers and clients
- **If properly designed, enforcement of policies is simple, scalable, and robust.**
- **A firewall reduces the complexity of security management by offloading most of the network access control to a couple of points in the network.**

Firewall Limitations

- **Misconfiguration of a firewall can have serious consequences (single point of failure).**
- **Many applications cannot be securely passed over firewalls.**
- **When a user is frustrated by a firewall, they may find ways around the firewall.**
- **A firewall can cause performance bottlenecks.**
- **Unauthorized traffic can be tunneled (covert channels).**

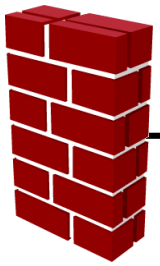
Firewalls in a Layered Defense Strategy

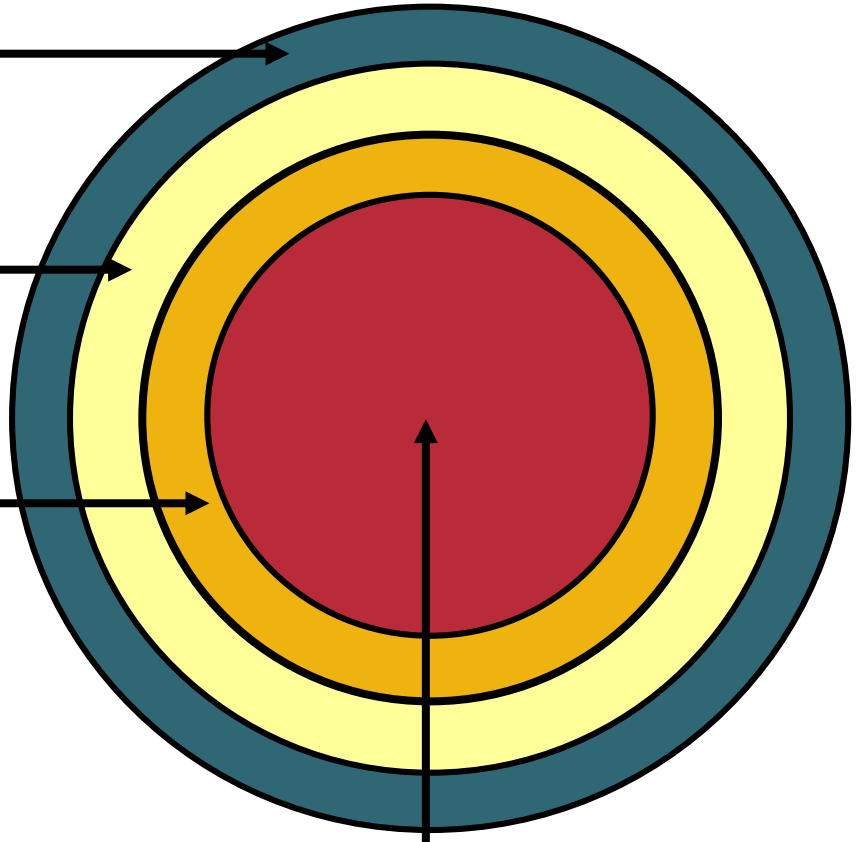
Perimeter security
Secures boundaries between zones

Communications security
Provides information assurance

Core network security
Protects against malicious software and traffic anomalies, enforces network policies, and ensures survivability

Endpoint security
Provides identity and device security policy compliance

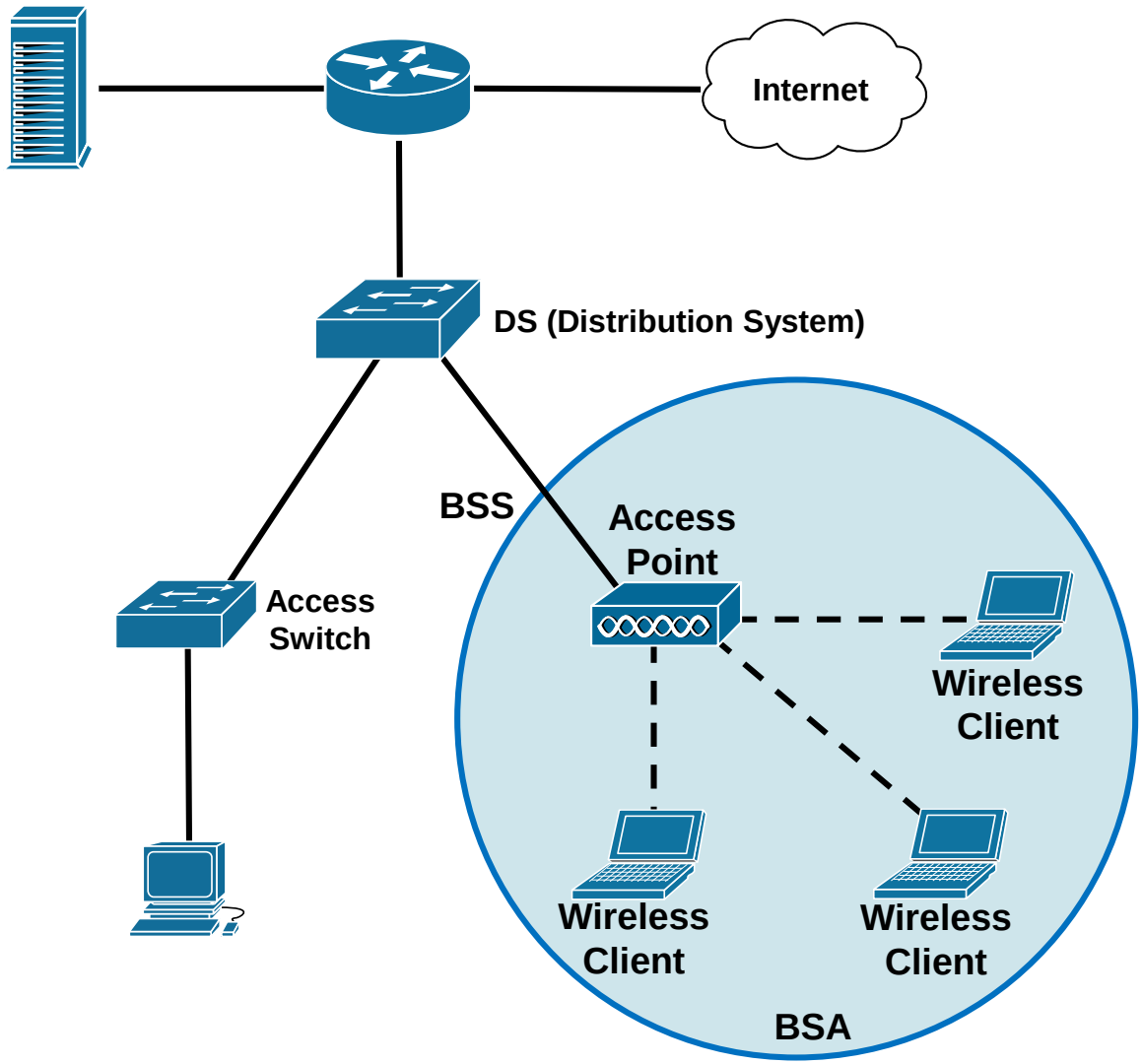




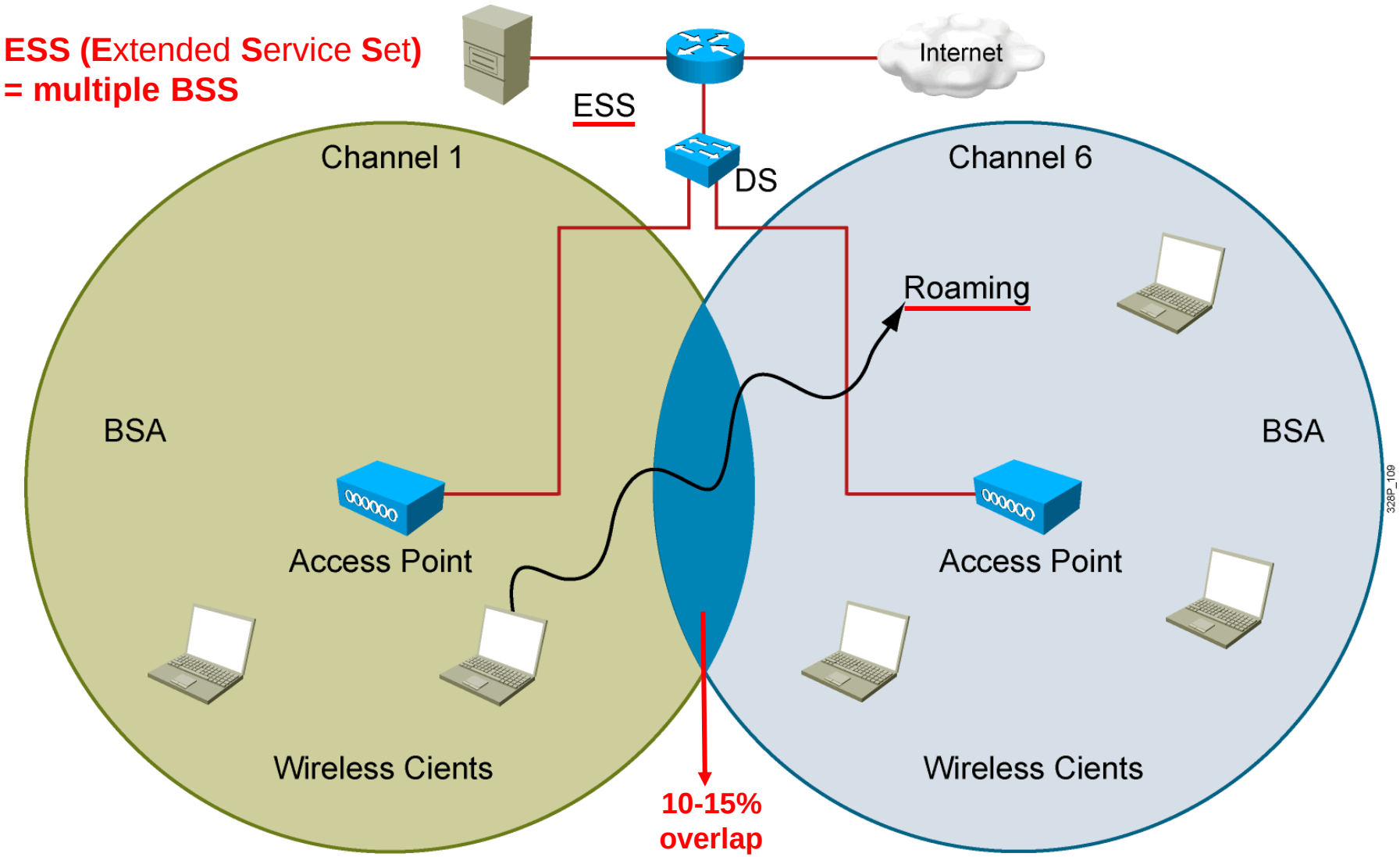
Disaster recovery
Offsite storage and redundant architecture

Access Point

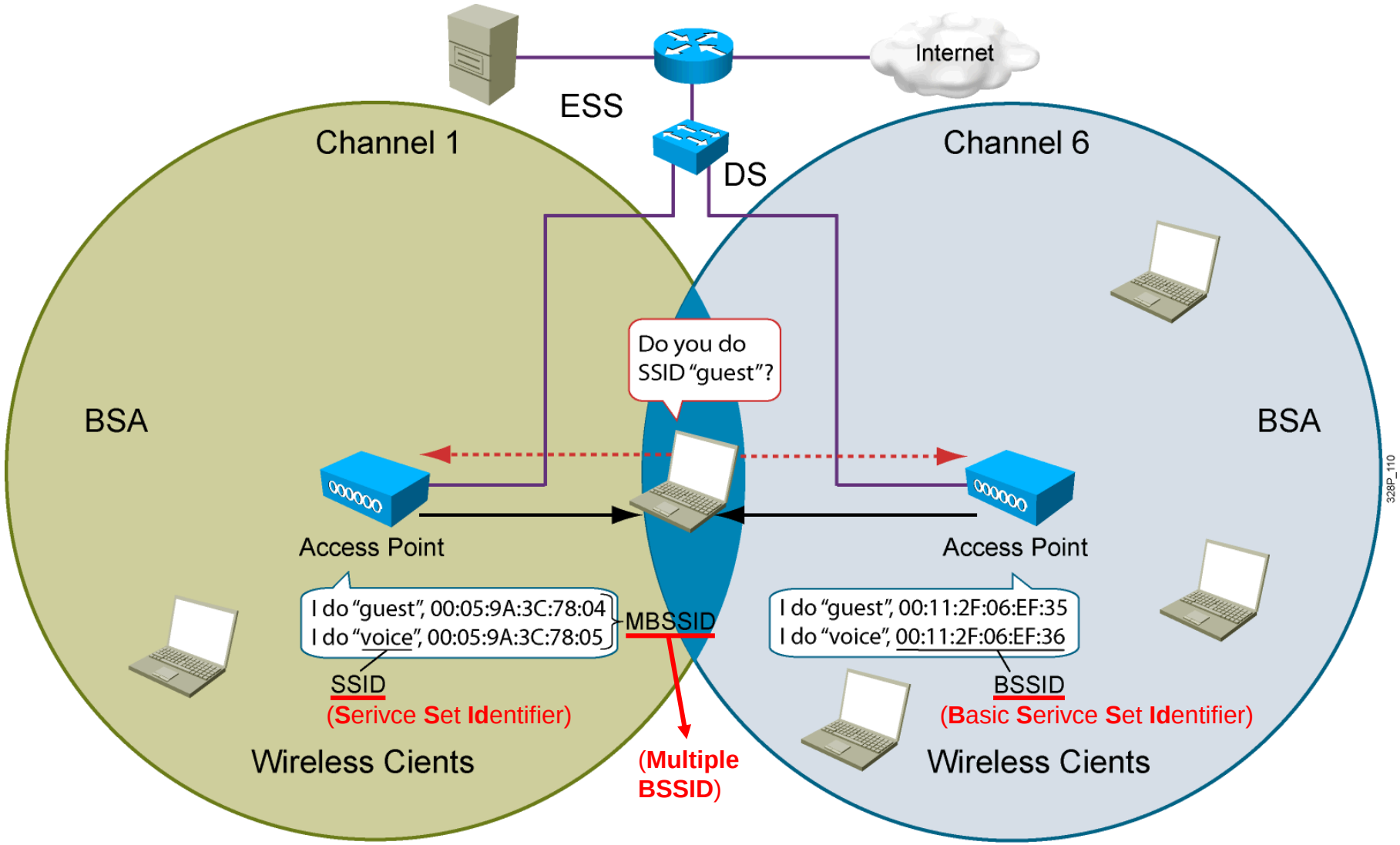
- **WLAN = Wireless LAN**
- **The AP functions as a translational bridge between 802.3 wired media and 802.11 wireless media.**
- **Wireless is a half-duplex environment.**
- **BSA (**Basic **S**ervice **A**rea**) = wireless cell.**
- **BSS (**Basic **S**ervice **S**et**) = AP + associated stations.**



Access Point (Cont.)

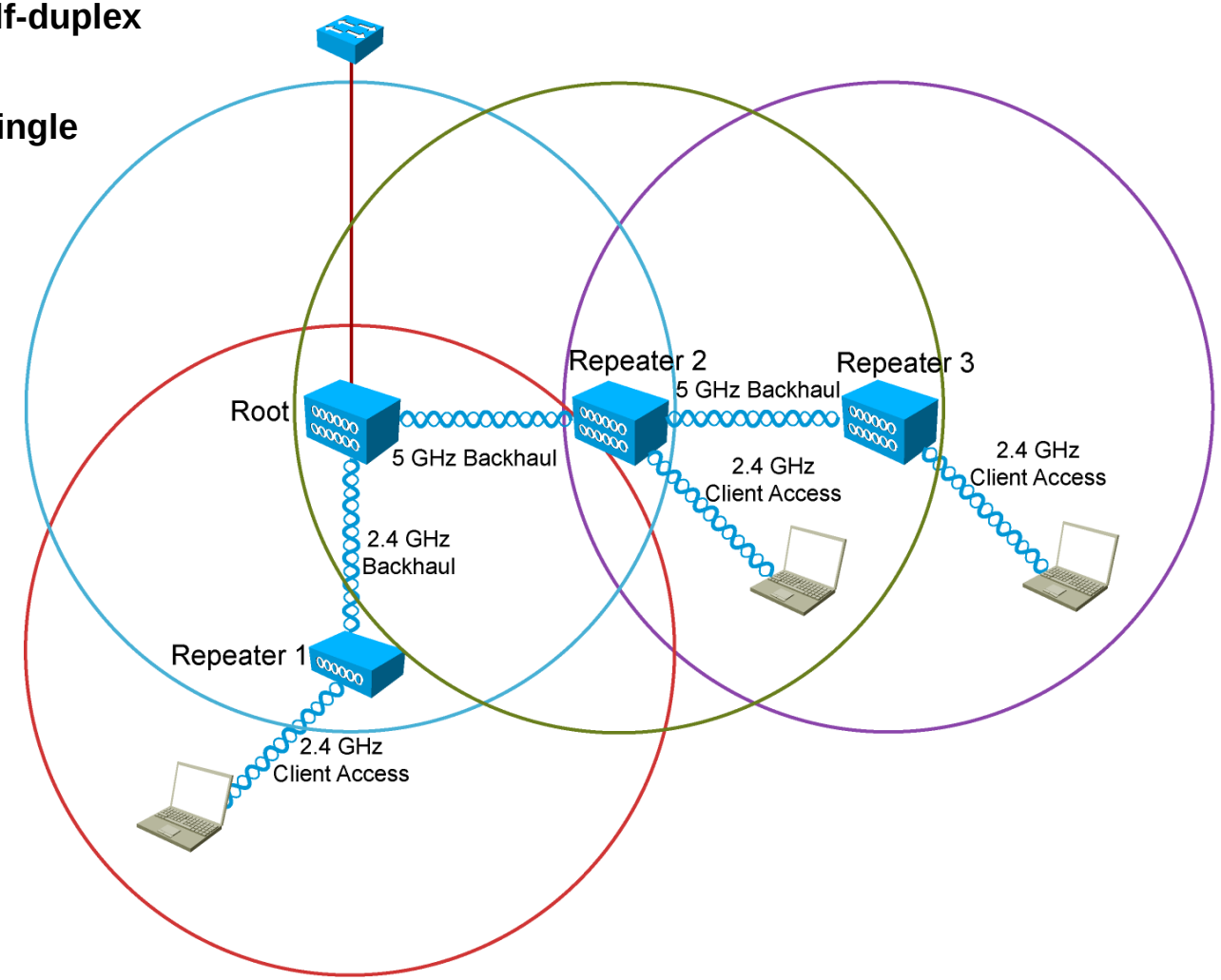


Service Set Identifier

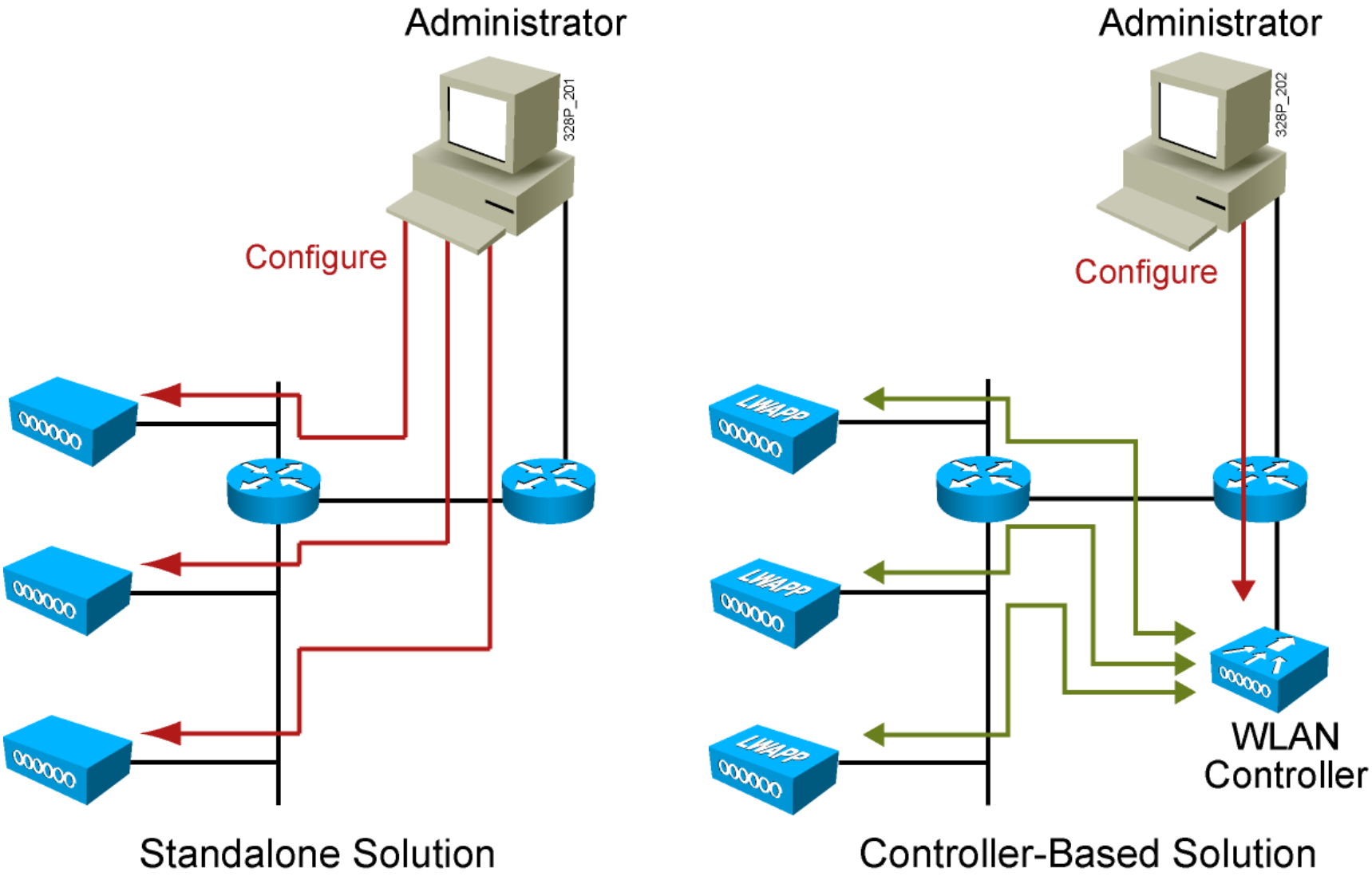


Repeaters

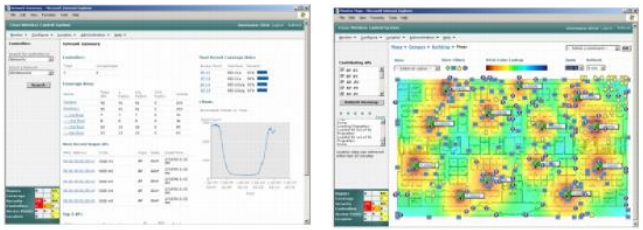
- Extends the AP coverage
- Dual radio can create dual half-duplex
- Overlap of 50% required
- Throughput impacted when single frequency used
- 2.4 GHz:
  - 802.11b/g/n
  - Large range
  - High levels of compatibility
  - More signal interference
  - 3 available channels
  - Lower bandwidth
- 5 GHz:
  - 802.11a/n/ac
  - Small range
  - Low levels of compatibility
  - Less signal interference
  - 23 available channels
  - Higher bandwidth



Standalone and Lightweight APs



Cisco Unified Controller-Based Solution



Cisco Wireless Control System

Location Server

Blade-Based Controllers

SNMP

4400 WLAN Controller

(Lightweight Access Point Protocol)

LWAPP

Access Points

WLAN Controller

Mobility Management

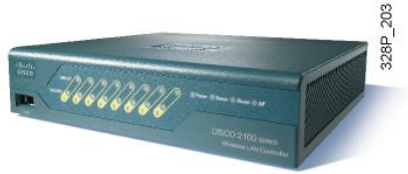
Location Services

Grouping & Redundancy

Security

Real-Time RF Management

3750G Integrated WLAN Controller



2106 WLAN Controller

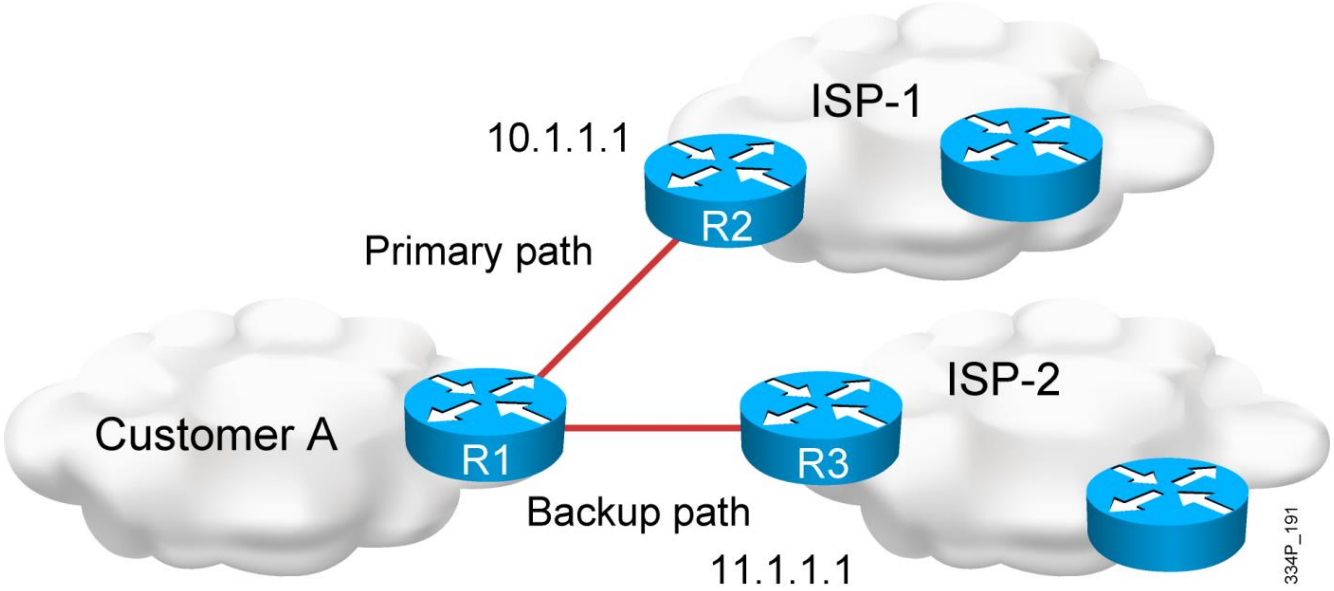
328P_203

Path Selection Process Using Filters

- **Manipulating path control by manipulating routing protocols and the routing table**
- **Tool availability is protocol-dependent:**
  - Route maps
  - Prefix lists
  - Distribute lists
  - Administrative distance
  - Route tagging
  - Offset lists
  - Cisco IOS IP SLA
  - PBR

Cisco IOS IP SLA Example

- **Customer A is multihoming to ISP-1 and ISP-2**
- **The link to ISP-1 is the primary link for all traffic**
- **Customer A is using the default routes to the ISPs**
- **A Cisco IOS IP SLA is used to conditionally announce the default route**



Using IP SLA for verifying Internet connection

```
A(config)#ip sla 1
A(config-ip-sla)#icmp-echo 10.1.1.1 source-ip 200.0.0.1
A(config-ip-sla-echo)#frequency 10
A(config-ip-sla-echo)#exit
A(config)#ip sla schedule 1 start-time now life forever
```

- Set the probe to send an ICMP packet every 10 seconds to IP address 10.1.1.1.
- Start sending packets now and continues forever.

```
A(config)#track 10 ip sla 1
```

- Define the tracking of object 1 linked to IP SLA 1.

```
A(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1 5 track 10
```

- Announces the default route with gateway IP 10.1.1.1 with administrative distance of 5 if tracking object 1 is true.


CISCO