

AP Networking | Unit 4

4.1 What Failure Costs

Solutions

Reference scenario

Translate a network incident into user impact before recommending resilience.

Clinic scheduling service: unavailable for 45 minutes

Patient records: no observed disclosure

Record contents: no observed alteration

4.1.1

A shared folder is online, but an unauthorized user changes appointment times. Which security goal is most directly affected?

Integrity is directly affected because the information was changed without authorization. Availability alone would not capture the problem; access controls and audit records are relevant.

4.1.2

Name two operational consequences of losing a school network during online registration.

Families may be unable to submit registrations and staff may be unable to verify submissions or allocate places. Connect recovery priorities to those disrupted tasks rather than merely naming failed equipment.

AP Networking | Unit 4

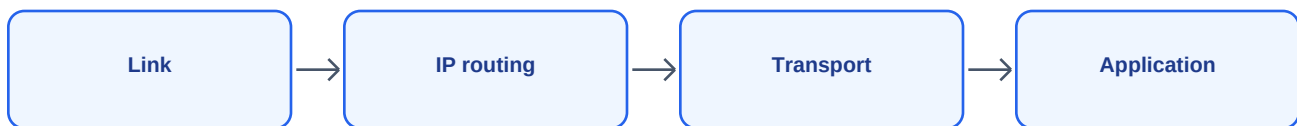
4.2 Two Models for One Network

Solutions

Reference scenario

Use layers to locate a fault without confusing the two common models.

Cable link: up
IP configuration: valid
Gateway: reachable
Web name resolution: fails



4.2.1

Match Ethernet framing, IP forwarding, TCP reliability, and DNS name lookup to OSI layer names.

Ethernet framing: data link. IP forwarding: network. TCP reliability: transport. DNS name lookup: application.
The mapping organizes diagnosis rather than proving a whole layer is fault-free.

4.2.2

Why does a successful gateway ping not prove that HTTPS and DNS both work?

It tests one form of IP reachability to one destination. Application services can fail independently through service configuration, name records, transport policy, or server problems.

AP Networking | Unit 4

4.3 The Protocols That Do the Work

Solutions

Reference scenario

Separate naming, addressing, and transport responsibilities in a web request.

Name: portal.example

DNS answer: 192.0.2.20

Application: HTTPS

Transport: TCP in this example

4.3.1

A service is reachable by its documented address but not its hostname. Which service is a leading suspect, and what check supports the diagnosis?

Name resolution is a leading suspect. Query the configured resolver for the exact hostname and compare its result with the documented address or a known working client.

4.3.2

Explain why a real-time media application might accept some loss rather than wait indefinitely for retransmission.

Late media data may no longer be useful for timely playback. The application may favor lower delay over complete delivery, while still needing appropriate congestion handling and security.

AP Networking | Unit 4

4.4 Working at the Command Line

Solutions

Reference scenario

Interpret example command output without running disruptive commands.

Address: 10.3.5.22/24

Gateway: 10.3.5.1

DNS query: timeout

HTTPS test by address: succeeds

4.4.1

What information would you collect before changing DNS settings after a timeout?

Record the configured resolver, the exact name queried, timestamps and error output, whether other clients are affected, and whether an approved alternate resolver answers. A timeout alone does not identify a unique cause.

4.4.2

Why should a technician preserve the original diagnostic output along with the interpretation?

Another technician can review the evidence, compare later results, and detect mistaken assumptions. The interpretation may change, but the original readings establish what was actually observed.

AP Networking | Unit 4

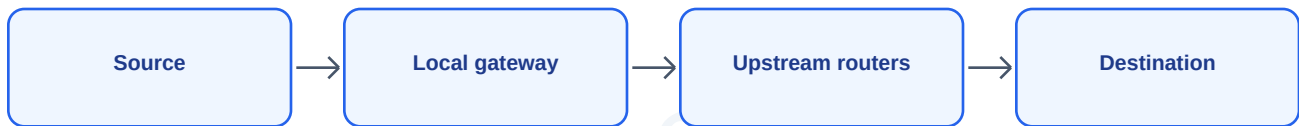
4.5 How Data Finds Its Way

Solutions

Reference scenario

Read end-to-end behavior in an example path trace.

Hop 1: 2 ms
Hop 2: * * *
Hop 3: 8 ms
Destination: 11 ms
Required application: works



4.5.1

A trace reports 90 ms at hop 3, 10 ms at hop 4, and 12 ms at the destination. Does the 90 ms response alone prove a persistent path delay?

No. The later responses are faster, so hop 3 may simply prioritize diagnostic replies differently. Evaluate repeated end-to-end measurements and the application behavior.

4.5.2

A trace becomes slow at hop 4 and remains slow to the destination, while the application also slows. What next action is justified?

Investigate the path around and beyond that transition using repeated tests and provider or device evidence. Treat it as a lead rather than proof of the exact failing router.

AP Networking | Unit 4

4.6 Reliability, Growth, and Newer Addressing

Solutions

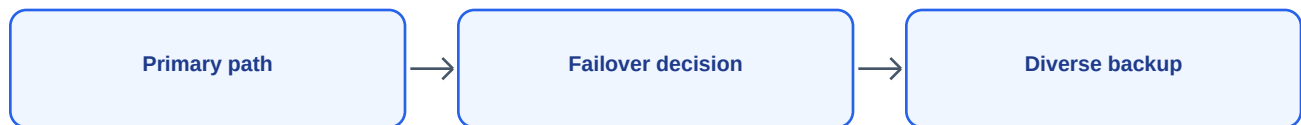
Reference scenario

Evaluate a redundancy proposal and newer addressing.

Primary uplink: conduit A

Backup uplink: conduit A

Addressing growth: additional device groups expected



4.6.1

Why can two routers connected to the same failed power strip both become unavailable?

They share the power strip as a common dependency. Device duplication alone does not remove the shared failure path; assess power diversity and recovery requirements.

4.6.2

What is the address bit length of IPv4 and IPv6, and why does migrating not eliminate the need for firewall rules?

IPv4 uses 32-bit addresses and IPv6 uses 128-bit addresses. Address capacity is separate from authorization; required traffic still needs an explicit, verified security policy.