



COMPUTER NETWORK SETUP

Teaching Notes

Unit code: 0612 351 03A | Level: 6 | Course: ICT Technician | College: Sample Technical Training Institute | Prepared by: A. Sample

LEARNING OUTCOME 1: TERMINATE COMPUTER NETWORK CABLES

1. Learning Outcome Statement

By the end of this outcome you will be able to select the correct devices, media and tools for a cabling job, and terminate UTP cable onto RJ-45 connectors, outlets and patch panels to TIA/EIA-568, testing every termination you make.

2. Key Concepts and Explanations

Network types and topologies

A network is classified first by the area it covers and then by the shape in which its nodes are joined. A LAN covers one building or site and is owned by the organisation; a WAN spans towns or countries and usually rides on a service provider's links; a MAN sits between the two, across a city. The topology is the arrangement of the nodes, and it decides how a fault spreads.

- Star — every node has its own cable back to a central switch. A single cable fault takes out one node only, which is why almost every modern LAN is wired as a star.
- Bus — all nodes tap one backbone terminated at both ends. Cheap in cable, but one break stops the whole segment. Now obsolete for data.
- Ring — nodes form a closed loop. Access is deterministic, so there are no collisions, but a break in the loop is serious unless the ring is dual.
- Mesh — multiple redundant paths between nodes. Expensive in cable and ports, so it is used between switches and sites rather than out to the desk.
- Hybrid — real installations are usually a star at each floor, joined into a tree by the backbone.
- A 24-user office: one switch in a floor cabinet, one cable per desk — a star.
- Three floors, each with its own switch, all uplinked to a core switch in the server room — a tree of stars.
- Two core switches cross-linked to both distribution switches so either can fail — a partial mesh.

Transmission media and when to use each

Media choice is decided by distance, the electrical environment and the bandwidth you must carry. Getting it wrong is expensive because the horizontal cable is buried in the fabric of the building and is not easily replaced.

- UTP — four unshielded twisted pairs. The twist itself rejects noise. Cheapest and easiest to terminate. Limited to 90 m of fixed horizontal cable plus 10 m of patch cords.
- STP/FTP — the same pairs with a foil or braid screen and a drain wire. Needs a bonded earth at both ends or the screen becomes an aerial. Use in workshops, near motors, or alongside heavy power runs.
- Fibre — light in a glass core. Immune to electromagnetic interference, no earth path between buildings, and good for hundreds of metres (multimode) to tens of kilometres (single mode). Used for backbones and inter-building links.
- Category matters: Cat 5e to 1 Gbps, Cat 6 to 10 Gbps over short runs, Cat 6A to 10 Gbps over the full 100 m. Connectors, patch panels and patch cords must all match the category or the link certifies at the lowest component.
- Desk outlets on all three floors: Cat 6 UTP.
- The run from the workshop, which passes a welding bay: screened Cat 6A, bonded at both ends.





- Between the main block and the hostel, 300 m apart: multimode fibre, which also avoids an earth loop between two buildings.

The T568A and T568B pin assignments

TIA/EIA-568 defines which conductor lands on which of the eight pins. Two schemes exist, and they differ only in that the orange and green pairs are swapped. Either is correct; mixing them on the two ends of one cable is what makes a crossover.

- T568B, pins 1 to 8: white/orange, orange, white/green, blue, white/blue, green, white/brown, brown.
- T568A, pins 1 to 8: white/green, green, white/orange, blue, white/blue, orange, white/brown, brown.
- Pins 4, 5, 7 and 8 are identical in both schemes — only pins 1, 2, 3 and 6 move.
- Both ends the same scheme = straight-through, used between unlike devices (PC to switch).
- One end A and the other B = crossover, used between like devices (switch to switch) on equipment without Auto-MDI/MDI-X.
- Pick one scheme for the whole site — usually T568B in this region — and write it on the documentation.

Illustration / worked example

```
T568B (pin : conductor)
1 : white/orange    5 : white/blue
2 : orange          6 : green
3 : white/green     7 : white/brown
4 : blue            8 : brown

T568A swaps the orange and green pairs:
1 : white/green     3 : white/orange
2 : green           6 : orange
(pins 4, 5, 7, 8 unchanged)
```

Terminating to standard — the four things that fail

Most terminations that fail certification fail for one of four reasons, and all four are workmanship rather than materials. Learn to spot them on your own work before the tester does.

- Excessive untwist. More than about 13 mm of untwisted pair at the connector raises near-end crosstalk. Untwist only as far as the connector needs.
- Split pairs. Each conductor is continuous end to end, but two conductors from different pairs are used as a pair. A continuity test passes; a wire-map test fails. This is why you test wire map, not just continuity.
- Conductors not fully seated. The IDC pin fails to pierce the insulation, giving an intermittent link that works on the bench and fails in service. Inspect the connector tip — all eight conductors must be visible at the end.
- Sheath not captured. If the outer sheath does not reach past the strain-relief point, any pull on the cable is taken by the conductors and the termination breaks.
- A link that shows a green light but drops under load: usually a split pair or a partly seated conductor.
- A patch cord that works until someone moves the desk: the sheath was not captured by the strain relief.

3. Practice Activities

- Identify and name every tool on the termination bench, and state what each one does.
- Strip a 300 mm offcut of Cat 6 and measure your strip length with a rule. Repeat until you can hit 12–13 mm consistently.
- Lay out the eight conductors in T568B order without looking at the chart, then check yourself.
- Terminate one end of a cord, then inspect the connector tip against the four failure modes above before you crimp.
- Swap cords with a partner and test each other's work on the cable tester. Write down every fault you find and what caused it.

4. Practical Task

Task. Make and prove three patch cords

The laboratory needs patch cords for a new bench. You are to make two straight-through cords and one crossover, and prove each one before it is issued.

1. Cut two 2 m lengths and one 1.5 m length of Cat 6 UTP.
2. Slide a strain-relief boot onto each end before you strip anything — it cannot be fitted after the connector is crimped.
3. Strip 12–13 mm of sheath from each end without nicking the conductors.
4. Terminate both 2 m cords T568B at both ends. Terminate the 1.5 m cord T568A at one end and T568B at the other.
5. Check the connector tip on every end: all eight conductors visible, sheath past the strain relief.
6. Crimp in one firm stroke, then slide the boot up over the connector.
7. Test all three cords and record the wire map result for each.
8. Label each cord with its type and your name.

Expected outputs

- Two straight-through cords that map pin 1 to pin 1 through to pin 8.
- One crossover cord showing the 1–3 and 2–6 transposition on the tester.
- A completed test record for all three cords.

5. Learning Checks

Oral

1. Which four pins differ between T568A and T568B?
2. Why does a split pair pass a continuity test but fail certification?
3. When would you specify screened cable instead of UTP?

Written

1. State four network topologies and give one advantage of each.
2. Explain why the untwist at a termination must be kept under 13 mm.
3. Differentiate between a straight-through and a crossover cable, and state where each is used.

Practical

1. Terminate an RJ-45 connector to T568B and have it pass a wire-map test first time.
2. Identify, from a set of pre-made cords, which is straight-through and which is crossover, using the tester.

6. Revision and Self-Check

Revise by making cords until you pass first time without checking the colour chart. Being able to recite the pin order is not the competency — producing a termination that certifies is. Keep every test record; the assessor will ask to see it.

Revision methods. Written test, Practical assessment, Direct observation, Oral questioning

LEARNING OUTCOME 2: CONNECT COMPUTER NETWORK CABLES

1. Learning Outcome Statement

By the end of this outcome you will be able to observe the required safety measures, mount and interconnect network devices to a design, route and dress cable to standard, apply an IP addressing scheme, and verify that the network you have built works.

2. Key Concepts and Explanations

Safety on a network installation

Cabling work puts you in ceilings, under floors and inside cabinets that may be live. The safety measures are not generic advice — they are performance criteria you will be assessed on, and the assessor will stop a practical for an unsafe act.

- Wear the PPE issued: dust coat, safety glasses when cutting or drilling, gloves when handling cable trays.
- Isolate and lock off power before working inside a cabinet or trunking that carries mains.
- Never look into the end of a fibre or a fibre port. Use a power meter, not your eye.
- Barrier and sign any open floor box, lifted tile or ladder. Keep fire exits and walkways clear of drums and tools.
- Use a tested ladder or platform. A chair is not a work platform.
- Report damaged tools and take them out of service rather than working round the fault.

Mounting and dressing — why it is marked

A cabinet that is neat is not just tidy; it is maintainable. Marks are awarded for the arrangement because the arrangement is what a technician has to work with three years later at two in the morning.

- Put patch panels immediately above or below the switch they serve, so patch cords are short and do not cross the cabinet.
- Heavy items — UPS, servers — go at the bottom, or the rack becomes unstable.
- Leave clearance for airflow, and respect the fan direction. A switch that draws front-to-back must not be boxed in.
- Keep power leads on one side and data cords on the other, crossing at right angles if they must cross.
- Support cables with hook-and-loop straps, not over-tightened cable ties — a tight tie deforms the pairs and shows up as a certification failure.
- Respect the bend radius, typically four times the cable diameter for UTP, and do not fill trunking beyond about 40 %.

IP addressing and subnetting

Every device on the network needs an address, a mask that tells it which addresses are local, and a gateway for everything else. Subnetting borrows host bits to create more, smaller networks — usually to separate departments, or to keep broadcast domains small.

- An IPv4 address is 32 bits, written as four octets. The mask separates the network part from the host part.
- Usable hosts in a subnet = $2^{(\text{host bits})} - 2$. The two subtracted are the network address.
- Borrowing n bits from the host part creates 2^n subnets. /24 !' /26 borrows 2 bits.
- Private ranges: 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16. These are not routed on the internet and are what you will use on a LAN.
- Give servers, printers and network devices static addresses; give workstations DHCP addresses from a pool that excludes the static range.
- Document the plan before you configure anything. Duplicate addresses are the most common self-inflicted fault on a new install.

Illustration / worked example

Worked example – divide 192.168.20.0/24 into four subnets

Borrow 2 host bits -> /26 mask 255.255.255.192

Subnets = $2^2 = 4$

Hosts = $2^6 - 2 = 62$ usable per subnet

Subnet 1 192.168.20.0/26 hosts .1 - .62 broadcast .63



Subnet 2	192.168.20.64/26	hosts .65 - .126	broadcast .127
Subnet 3	192.168.20.128/26	hosts .129 - .190	broadcast .191
Subnet 4	192.168.20.192/26	hosts .193 - .254	broadcast .255

Verifying the network you have built

You have not finished when the cables are in. You have finished when you can show, and record, that traffic passes. Work outwards from the node: prove each layer before moving to the next.

- Link light at the NIC and at the switch port — proves the physical link.
- ipconfig / ifconfig — proves the device has the address you intended, not an APIPA 169.254 address from a failed DHCP.
- ping the loopback (127.0.0.1) — proves the TCP/IP stack on the machine itself.
- ping a peer on the same subnet — proves local switching.
- ping the gateway — proves the route off the subnet.
- ping an external host by name — proves routing and DNS together. If the address works but the name does not, DNS is your fault, not routing.
- Record each result against the outlet label on the test schedule.
- Address is 169.254.x.x: the machine never reached a DHCP server — check the cable, the port and the VLAN before blaming the server.
- ping 8.8.8.8 works but ping google.com fails: routing is fine, DNS is not configured or unreachable.

3. Practice Activities

- Mount a patch panel and switch in a practice cabinet and dress six patch cords through the management bars.
- Given a floor plan and a user count, write an addressing plan before touching a device.
- Subnet 10.10.0.0/16 for six branches of up to 500 hosts each, and justify your choice of mask.
- Configure two workstations and prove connectivity through the full ping sequence, recording each step.
- Introduce a deliberate duplicate address on a partner's bench and watch what the symptom looks like.

4. Practical Task

Task. Build and prove a small office network

You are handed a switch, a router, two workstations, a patch panel and the cabling you terminated in Outcome

1. Build a working network and prove it.

1. Mount the patch panel and switch in the cabinet, observing position, airflow and cable management.
2. Patch the two horizontal runs to the switch and uplink the switch to the router's LAN port.
3. Write an addressing plan for both workstations, the switch management interface and the router from 192.168.50.0/24.
4. Configure the addressing on each device.
5. Run the verification sequence from each workstation: link light, ipconfig, loopback, peer, gateway, external host.
6. Record every result on the test schedule, then label the patch cords and update the patch record.

Expected outputs

- A written addressing plan with no duplicate addresses, produced before configuration.
- Both workstations reaching each other, the switch, the router and an external host.
- A completed test schedule and an updated patch record.

5. Learning Checks



Oral

1. Why do we subtract two when calculating usable hosts in a subnet?
2. What does a 169.254 address tell you?
3. Why are patch panels mounted next to the switch they serve?

Written

1. State five safety measures observed when working on a network installation in an occupied office.
2. Divide 192.168.20.0/24 into four subnets and give the mask, usable hosts and the four network addresses.
3. Explain four rules for routing and dressing cables in trunking, with a reason for each.

Practical

1. Build a star network from the components supplied and demonstrate connectivity to the assessor.
2. Apply a supplied addressing plan and prove there are no duplicates.

6. Revision and Self-Check

The verification sequence is what separates a pass from a fail here. Anyone can plug cables in; the competency is proving, in order, that each layer works and recording the evidence. Practise until the sequence is automatic.

Revision methods. Written test, Practical assessment, Direct observation, Project work

LEARNING OUTCOME 3: PERFORM COMPUTER NETWORK MAINTENANCE**1. Learning Outcome Statement**

By the end of this outcome you will be able to select and use network monitoring tools, monitor performance against a plan, diagnose faults using a structured procedure, repair or replace faulty components, and document the work to workplace standard.

2. Key Concepts and Explanations**Monitoring tools and what each one tells you**

Different tools answer different questions. Reaching for the wrong one wastes time; a protocol analyser will not tell you that a cable is broken, and a cable tester will not tell you that a link is congested.

- Cable tester / certifier — wire map, length, attenuation, crosstalk. Answers 'is the physical cable good?'
- Link lights and switch port statistics — CRC errors, discards, speed and duplex. Answers 'is this port healthy?'
- ping and traceroute — reachability and where in the path the loss starts. Answers 'can traffic get there, and how far does it get?'
- Protocol analyser (Wireshark) — the actual packets. Answers 'what is on the wire, and what is it doing wrong?'
- SNMP monitoring platform — utilisation, uptime and error counters over time. Answers 'is this getting worse, and since when?'
- Bandwidth monitor — throughput per link. Answers 'is the uplink the bottleneck?'

Monitoring against a plan

Monitoring only means something against a baseline. Take readings when the network is known-good, and the same readings later tell you what has changed.

- Baseline utilisation on each uplink at a typical busy hour, and record it.
- Watch error counters, not just utilisation — rising CRC errors on one port almost always mean a cable, connector or duplex mismatch on that port.

- Track latency to the gateway and to an external host. A jump in latency without a jump in utilisation points at a device, not congestion.
- Record device uptime. A switch that reboots on its own has a power or hardware fault, whatever else it is doing.
- Set thresholds and alert on them, so the first person to notice a problem is not the user.

A structured diagnostic procedure

Faults are found by narrowing the field, not by guessing. Work from the symptom outwards, and change one thing at a time so you know which change fixed it.

- Confirm the symptom yourself. 'The internet is down' from one desk is a different fault from the same report from every desk.
- Establish the scope: one node, one port, one switch, one floor, or everything. Scope points at the layer.
- Check the physical layer first: link lights at both ends, cable seated, patch cord not damaged.
- Substitute a known-good component — cord, port, workstation — to isolate the faulty one.
- Move up the stack: addressing (ipconfig), local reachability (ping peer), gateway, DNS.
- Once found, fix it, then prove the fix by repeating the test that failed.
- Document the fault, the diagnosis, the action and the verification. An undocumented fix is a fault that will be diagnosed from scratch next time.

Illustration / worked example

Symptom: one workstation has no access, its neighbours are fine

1	Link light at NIC and at the switch port?	no -> physical
2	Swap the patch cord for a known-good one	fixed -> cord
3	ipconfig -> 169.254.x.x ?	yes -> DHCP path
4	ping 127.0.0.1	fail -> local stack
5	ping peer on same subnet	fail -> switching / VLAN
6	ping gateway	fail -> routing / gateway
7	ping 8.8.8.8 then a hostname	name only fails -> DNS
8	Record fault, cause, fix and verification in the log	

Repair, replacement and the maintenance record

Replacing a component on a live network is a planned operation, not a reflex. The record you leave behind is part of the job.

- Schedule disruptive work in an agreed window and tell the users first.
- Back up the configuration and record the port assignments before you touch anything.
- Label every cord before disconnecting. An unlabelled cabinet takes hours to reassemble.
- Isolate power and observe ESD precautions when handling boards and modules.
- Restore the configuration, reconnect to the labelled ports, and verify every port comes up.
- Log it: date, fault reported, fault found, action taken, parts and serial numbers, verification result, technician, downtime.

3. Practice Activities

- Baseline the laboratory network: record utilisation and error counters on each uplink at a busy time.
- Work in pairs — one introduces a single fault, the other diagnoses it using the sequence above and times themselves.
- Read a switch's port statistics and identify the port with a physical problem from the error counters alone.
- Write a maintenance log entry for a fault you diagnosed, and have a partner check it is complete enough to act on.
- Draft a maintenance schedule for a 40-user office: what is checked daily, monthly and annually.

4. Practical Task

Task. Diagnose, repair and document an introduced fault

The assessor introduces one fault into the network you built in Outcome 2. You must find it, fix it, prove it and record it.

1. Confirm the symptom and establish its scope before touching anything.
2. Select the monitoring or test tool appropriate to the layer you suspect, and say why you chose it.
3. Work through the diagnostic sequence, explaining each step to the assessor as you carry it out.
4. State the fault and the evidence that led you to it.
5. Carry out the repair or replacement safely.
6. Repeat the test that originally failed and demonstrate the network is restored.
7. Complete a maintenance log entry covering the fault, diagnosis, action and verification.

Expected outputs

- A correct diagnosis supported by the evidence you gathered, not by guesswork.
- A restored network demonstrated to the assessor by the test that originally failed.
- A maintenance log entry a colleague could act on without asking you anything.

5. Learning Checks

Oral

1. Which tool would you reach for first if one port shows rising CRC errors, and why?
2. Why do we baseline a network when it is working?
3. What is the risk in changing two things at once while diagnosing?

Written

1. Identify four network monitoring tools and state what each one measures.
2. Set out a structured procedure for diagnosing a workstation with no network access.
3. State the information recorded in a network maintenance log and why each item is needed.

Practical

1. Diagnose an introduced fault within the time allowed, explaining each step.
2. Replace a faulty patch cord or switch port assignment and prove the link is restored.

6. Revision and Self-Check

You are marked on the procedure as much as on the answer. A candidate who finds the fault by luck, without a structured search, has not shown the competency. Talk the assessor through your reasoning as you work.

Revision methods. Written test, Practical assessment, Direct observation, Oral questioning, Case study

SMALL REVISION PRACTICE

Set up and hand over a small office network

A six-person office is moving into a new suite. It needs six data outlets, a floor cabinet with a patch panel and switch, a router to the ISP service, an addressing plan, and a documentation pack at handover.

Requirements

- Six horizontal runs terminated at outlets and on the patch panel, all to one scheme.
- Patch cords made by you, labelled and tested.
- Switch and patch panel mounted with correct positioning, airflow and cable management.
- An addressing plan from a private range, with static addresses for infrastructure and a DHCP pool for workstations.
- Every link tested, with the results recorded against the run labels.

**Expected outputs**

- A working network with all six outlets live and reaching the internet.
- A test schedule covering every run and cord.
- An as-built plan showing outlet positions and their labels.
- A patch record mapping outlet to panel port to switch port.
- An addressing plan and an equipment inventory with serial numbers.

Practice instructions

- Submit the documentation pack as one file, with your name and the date on the cover.
- Photograph the finished cabinet from the front and the rear and include both images.
- Demonstrate the working network to your trainer before you submit.

Self-check criteria

- Every termination passes a wire-map test first time.
- The cabinet is dressed so any single cord can be traced and replaced without disturbing others.
- The addressing plan contains no duplicates and matches what is actually configured.
- The documentation is complete enough for a different technician to support the site.

SELF-CHECK CHECKLIST

Task / Competency	I can check this	Yes	Not yet	Revision note
Select devices, media and tools	Correct category of cable, matching connectors, and serviceable tools selected for the specification.			
Terminate to TIA/EIA-568	Untwist within limits, correct colour sequence, all conductors seated, sheath captured.			
Route and dress cabling	Bend radius respected, trunking not overfilled, data separated from power, cables supported without deformation.			
Mount and interconnect devices	Panel and switch positioned for short patching and airflow; topology formed as designed.			
Apply an IP addressing scheme	Plan written before configuration; no duplicates; correct mask and gateway throughout.			
Verify connectivity	Full sequence demonstrated from link light through to an external host, each result recorded.			



Diagnose a fault	Structured search, one change at a time, conclusion supported by evidence.			
Document the work	Test schedule, patch record and maintenance log complete and legible.			

WRITTEN REVISION QUESTIONS

Short-answer questions

1. State four network topologies and give one advantage of each.
2. Differentiate between UTP, STP and fibre optic media.
3. List the T568B pin assignments from pin 1 to pin 8.
4. State four hand tools used to terminate UTP cable and the purpose of each.
5. Explain why the untwist at a termination must be kept under 13 mm.
6. State three items of information recorded in a network maintenance log.

Structured questions

1. Describe the T568A and T568B pin assignments and explain the consequence of mixing them on the two ends of a run.
2. Divide 192.168.20.0/24 into four subnets. Give the mask, the usable hosts per subnet and the four network addresses.
3. Explain four rules observed when routing and dressing cables in trunking, giving the reason for each.
4. Set out a structured procedure for diagnosing a workstation that has no network access while its neighbours work normally.
5. Describe the procedure for replacing a faulty switch in a live network, including the precautions taken.

ORAL REVISION QUESTIONS

1. Which four pins differ between T568A and T568B?
2. Why does a split pair pass a continuity test but fail a wire-map test?
3. What does a 169.254 address tell you about a workstation?
4. Why is a bend radius specified for UTP cable?
5. Which tool would you use first if one switch port shows rising CRC errors?

PRACTICAL REVISION TASK

Terminate two horizontal runs, connect them into a working network with two workstations and a router, apply an addressing plan, and diagnose a fault introduced by the assessor.

1. Select and check your tools and materials before starting.
2. Terminate both runs to T568B at outlet and patch panel.
3. Make the patch cords you need and test everything you terminate.
4. Mount and interconnect the devices, then apply the addressing plan.
5. Prove connectivity with the full verification sequence and record each result.
6. Diagnose, repair and document the fault the assessor introduces.

Practice evidence

- Terminated and tested runs and cords, labelled.
- A working network demonstrated to the assessor.
- Completed test schedule and addressing plan.
- A maintenance log entry for the introduced fault.

PRACTICE RECORD TEMPLATE

Network maintenance log entry

- Date and time of the work
- Site, cabinet and affected outlet or port
- Fault as reported by the user
- Fault as found, with the evidence
- Action taken, and any part replaced with its serial number
- Verification test carried out and its result
- Downtime incurred
- Technician's name and signature
- Next scheduled maintenance date

REFERENCES

- ANSI/TIA-568 series — Commercial Building Telecommunications Cabling Standard.
- ISO/IEC 11801 — Information technology: generic cabling for customer premises.
- Kenya Occupational Safety and Health Act, 2007 — duties when working at height and on electrical installations.
- Manufacturer's installation instructions for the connectors, outlets and patch panels in use on site.
- TVET CDACC curriculum for Computer Network Setup, unit code 0612 351 03A.