

## Networking Basics - Architectures

### Network Architectures

This document will discuss three network architectures in exploring the basics of networking:

- Ethernet
- ARCnet
- Token Ring

These architectures are labeled as 'OPEN' since you can run a variety of network operating systems on them.

### Ethernet

Ethernet is by far and large the most common network architecture encountered today. Ethernet usually runs on 10BaseT (UTP) wiring but in older installation might be found on 10Base2 or 10Base5 (Coax cable). Ethernet can be deployed on either a star or linear-bus wiring topology.

#### Ethernet: Linear-bus (coax) topology

Ethernet can be run on a linear-bus topology using coax (RG-58) cabling. This type of network will employ a point-to-point structure where every node will speak over the same cabling segment. Basically there will exist a single string of cable that will 'touch' each node of the network. (A 'Node' is defined as any fileserver, workstation, or peripheral device attached to the network). Each end of the 'string' will be 'terminated' to form an electrical circuit for communications to travel over.

This topology is a simple two-wire circuit – the coax core and the wire mesh beneath the outer casing. A linear bus topology relies on the integrity of the entire length of its coax line. The major drawback to this structure is that if any point on the 'communications string' develops a fault, the entire network goes down. There are no communication 'Hubs' in this structure to use in isolating problems with specific segments of the network; the network is all one segment.

**Note:** Coax has a distance limitation of about 600 feet (before the signal degrades). Since a linear-bus topology treats the entire network as one segment, the distance between its two nodes furthest from each other cannot exceed 600 ft.

The way around this limitation is to compensate for signal degradation by installing repeaters along the network. Repeaters will 'boost' the signal and send it off ready to travel another 600 ft., if necessary. This changes the scenario to one where the node must be less than 600 ft. from the nearest repeater instead of the furthest node.

#### Ethernet: Star/Complex Star (UTP) topology

A star topology involves 'hubs'. Hubs come in various forms and, depending on their complexity/abilities, may be called 'concentrators', 'switches', or 'ethernet switches'. The hub serves as a central connection point for the population of the network. Nodes, (file servers, workstations, and shared network devices), will all 'plug-into' a hub to communicate with the other nodes on the network.

## Networking Basics – Architectures

Looking at the lines connecting the nodes to the hub from above you might see a star shape. That is, a picture similar to what you would get by drawing several lines through a single point to form a Christmas-card star.

Working with this star topology has many benefits in the areas of trouble shooting and fault tolerance. Instead of a single network segment touching each node, (linear-bus), each node has a separate cable segment that ‘touches’ the hub.

This segment will take form, at least in part, as a ‘patch cable’. Patch cables are lengths of network wire with connectors on both ends. Workstations will typically have a patch cable running between the computer and a wall outlet. Commercial/Industrial installations will also have ‘patch panels’ in the ‘computer room’. Patch Panels represent the other end of the cable running from the back of the node’s wall outlet. Yet another patch cable connects a node’s ‘port’ on the patch panel to a hub.

Because nodes have their own cable segment and speak to each other via a hub, any individual connection can be interrupted without affecting other nodes on the network. (The disconnected node will obviously be unable to reply to connected nodes but connected nodes can continue talking to each other). This is a significant advantage when trouble shooting network problems and ‘isolating’ traffic problems.

For example, network cards or connectors will sometimes become faulty. A faulty NIC or connector can cause normal data packets to become distorted and be broadcast as ‘garbage’.

In the case of a faulty NIC, it may continuously broadcast these garbage packets – flooding its own cabling segment (and probably those of its neighbors) to the point where normal traffic is unable to travel.

This condition is commonly known as ‘packet storm’ or ‘data storm’. Network administrators are often tipped off to this problem by finding that communication problems happen only at certain times of the day or only in certain departments.

Many administrators have stayed late or come in early to diagnose problems and found nothing. They later determine that the problem only occurs when Jack/Jill is at work (and their computer is on). (Its also a good idea to take note of who is on vacation and who doesn’t turn off their computer when they go home).

The advantage for star networks in this case is that nodes can be connected/disconnected one by one to find the offending node. Connecting/disconnecting nodes on a hub is as simple as unplugging a phone cord. The normal scenario here would be to have two stations connected in the problem area, generate traffic between them, and add stations until the communication problem is duplicated.

**Note:** While IP nodes may let you plug and unplug them at will, IPX/SPX (Ex. Novell) networks need you to re-boot the node after disconnecting it. This is because IP is a packet-oriented technology and IPX is a broadcast technology. In IP, the packet is more or less self-contained and addressed to a specific destination.

In broadcast technology, IPX, every node basically ‘listens’ to all traffic and only ‘pays attention’ to the traffic addressed to it.

## Networking Basics – Architectures

In ethernet, a ‘collision detection’ system ensures that if two nodes broadcast data at the same time and data ‘collides’, the data gets rebroadcast. IPX/SPX networks have several layers of ‘drivers’ loaded to establish this ‘listening’ environment. When the physical connection is disrupted in IPX, the drivers need to be reloaded to re-establish the ‘listening’ environment.

### Complex Star topologies

Complex Star topologies consist of multiple Star networks connected to each other. Complex Stars typically develop out of formerly isolated departmental networks. The consolidation of the individual star networks may be dictated or desired to provide one bigger/better central fileserver serving all departments in lieu of deploying smaller, less expensive, file servers for each department.

Consolidating networks also helps departments share information and physical resources (like printers). Individual stars of a complex star network are connected via a ‘backbone’.

Backbones are simply another cabling segment of the network. Backbones differ from other segments by the fact that they normally connect hub to hub instead of node to hub. Characteristically, backbones are often longer than other cabling segments since they might provide connectivity to stars that are hundreds or thousands of feet apart.

### Crossover

Before describing the common types of backbones, we should discuss ‘Crossover’. Most hubs will reserve their first port for backbones. This is significant because the first port will allow you to cancel the ‘cross over’ on that single port. Crossover is necessary for effective communications.

In ethernet, wires 1,2,3,6 are used for communications. Two of the wires or ‘pins’ are used to transmit data and two are used to receive. At some point, the transmissions of one node have to end up on the receiving pins of another node. This ‘crossover’ happens in the hub.

Hypothetically the crossover should happen only an odd number of times. In practice, it only happens once. For this reason, you cannot simply connect one hub to another without turning the crossover ‘off’ on one of the connecting ports. A backbone simply combines two hubs into one large hub – typically over some significant distance.

### Backbones

#### UTP:

For connecting networks IN THE SAME BUILDING, running 10BaseT is a nice, quick networking solution. However, the UTP cable should not be run through harsh environments, like extremely hot/cold warehouses or places where birds, squirrels, or pests might chew on or damage the cable. In short, UTP is very fragile. All an end user has to do to ruin a cable is run the wheels of a desk chair over it a few times. Signals will degrade after traveling over 300’ of UTP wire and become unreliable. Repeaters can be installed to compensate for the 300’ distance limitation.

**Note:** Although similar in appearance to hubs, repeaters serve a different function. Repeaters will take the fading signal from either side and ‘boost’ it to full strength, enabling it to travel potentially another 300’, over CAT5/UTP. A repeater used in a coax backbone would allow the signal to travel another 600’. This difference in distance is a property of the cable more than of the repeater.

## Networking Basics – Architectures

### Coax:

Coax backbones are quite common due to the greater lengths they can carry a signal before it degrades. In addition to having twice the range of UTP, they are less sensitive to their environments and fairly sturdy. Coax backbones can be buried, (preferably in metal conduit), or run in the open air between buildings, (ideally attached to a structure or rigid line).

Coax lines can also employ repeaters to cover distances greater than 600' but it's important to note that repeaters installed outdoors would have to live in a weatherproof workbox and be secured to a structure or tower. Its generally a bad idea to install a work box at ground level unless its immediately next to a building – vehicles tend to run over them otherwise.

Many hubs will have a BNC connector on the back to support coax backbones. In this case the 'crossover' mentioned above is not an issue. If a hub does not have a 'native' BNC connector, a balen may be used to convert the RJ45 port to a BNC connector, (of course, one is needed on each end of the backbone). As implied just now, a balen will translate an RJ45 connector to a BNC connector.

### Fiber-Optic Cable:

Fiber will connect sites that are miles apart but fiber is expensive. The expenses include hardware on both ends to connect to the fiber, paying the telco to lay the cable, if leaving the company grounds, and the fiber itself.

Fiber is fragile (its essentially just glass) and should be professionally installed if going any great distance. The cost of fiber usually prohibits its use for short distances. This leaves a local network administrator choosing professional installation for most fiber.

Its not uncommon, however, to connect hub/switches in wiring closets with fiber when convenient. A ten foot, prefabricated fiber patch cable might cost about \$35. Higher-end hubs will have slots that you can 'fill' with cards that support fiber cabling. The overall advantage of fiber is the high quality of the transmitted signal over great distances.

### Wireless backbones

There are means of connecting buildings with line-of sight wireless backbones. Wireless backbones are basically a radio-frequency link between 'hubs'. This type of backbone is reliable, until you have bad weather or a bird takes a liking to your transceiver or a tree grows a branch in your line-of-sight. Wireless backbones tend to need more technical support that standard backbones.

## ARCnet

ARCnet is an old, old networking architecture. It is coax-based but employs a specific type of coax. Where it follows linear-bus wiring topologies similar to ethernet it has intricate rules regarding its cabling. Cable segments in an ARCnet network can vary form 100' to 20,000 feet, if you follow the rules.

These rules, 'the Hierarchy of Hubs' involves both active and passive hubs. ARCnet is really much more trouble than it's worth considering that ARCnet is rated at about 2.5 mbps. vs. Ethernet at 10 or 100 mbps (megabits per second). In addition to the wiring rules, ARCnet uses 93 Ohm coax vs. the 50 Ohm coax of Ethernet. Currently there are few, if any, newusers of ARCnet. Those that do have it already are phasing it out.

## Networking Basics – Architectures

### Token Ring

Token Ring was a product for large companies, with deep pockets, that needed complicated networks. Basically there was one ‘token’. The token was passed from node to node. If you had the token you could talk to the other nodes. If someone else had the token, you just had to wait until the token got back to you.

This is the exact opposite of a ‘broadcast’ technology (Ex. IPX/SPX). Token Ring networks are built on the star topology. However, Token Ring networks use SHIELDED-twisted-pair (STP) vs. UTP (Unshielded Twisted Pair).

They also use hubs but not the same hubs found in Ethernet networks. Networks running Token Ring will have MAU’s (Multi-station Access Units). Token Ring still has a presence in the industry, but you won’t see many new Token Ring installations.

This goes hand in hand with all the AS400s still in use because of the software they run. Many AS400 systems can today be replaced with powerful PCs for a fraction of the cost. In short, they were the best in their time, but technology got smaller, faster, and cheaper.

### Differences between architectures

#### Bandwidth

The major difference of these architectures is in bandwidth. Please note that bandwidth is a measure of *potential* rate data can be transmitted over a network. There is always a bottleneck somewhere in a communication process. One of the two computers communicating may be slower than the other, have inferior resources compared to the other, or be performing more tasks than the other.

### Bandwidth vs. Throughput

Throughput is the actual speed data will transfer at from one point on the network to another. The actual speed, (throughput), of a network is often quite less than it’s Bandwidth, (potential speed). Bandwidth is more often quoted than Throughput since it is easier to calculate and not subject to changes in many variables. The hardware used to communicate, heavy/light traffic, etc...can effect throughput.

#### Ethernet

Ethernet comes in two flavors of bandwidth, 10 mbps and 100 mbps. Fortunately, for 10 mbps networks that are upgrading, CAT5/UTP cable is already rated for 100 mbps. Ethernet running on Coax is limited to 10 mbps.

#### ARCnet

ARCnet is limited to 2.5 Mbps and no longer in wide use. There once was an effort to produce ‘high-speed’ ARCnet. That effort met little success and it is hard to find a mention of it in ARCnet reference materials.

#### Token Ring

Token Ring comes in both a 4 mbps and 16 mbps version. The 16 mbps version requires STP, shielded twisted pair, which could easily cost two or three times the price of UTP. The, much older, 4 mbps version would allow the use of UTP – but it was only 4 mbps.

## Networking Basics – Architectures

The major drawback to running 16 mbps Token Ring over 10 mbps ethernet was the token passing. Each NIC is responsible for passing the token on to the next after its predefined turn is up. If just one card malfunctions and fails to do this, the token could be lost and all the other cards will sit there still waiting for the token. For this reason, Token Ring networks typically have large support staffs.

### Summary

Overall, running Ethernet in the 10 or 100 mbps flavor on a Star networking topology is the most flexible and reliable choice. However, in any information system, the software should drive the hardware decisions. If a company can not run without software that only works on some old Unix system, they will need hardware and, at least part of, a network that supports that Unix system. In this scenario, standard workstations can still be deployed using terminal emulation software to connect to the Unix system. The terminal emulation software ‘pretends’ to be a VT100 or ‘dumb tube’ station previously used to access the custom Unix software.

### Common Issues to all Architectures

#### Network connections (NICs)

The selection of NIC will be determined by your architecture; Token Ring networks require Token Ring cards, Ethernet networks require Ethernet cards and so on... Ethernet cards are the most common and we will discuss those in this section.

#### Bits

NICs evolved in many stages. There were 8-bit, 16-bit, 32-bit and now 64-bit cards available. Basically, the more bits the card would support in communications, the better the potential communications between processor and LAN/WAN. Here, ‘better’ is a mixture of both speed and quantity. It might often be the case that the data you transmit on a 32-bit card is no larger, at a given time, than you would transmit on a 16-bit card – but you have removed a potential bottleneck for times when traffic demands are higher.

#### Bus

Bus refers to the ‘pipe’ used to funnel data back and forth from the CPU of a node to the NIC. Common terms you might see are (listed roughly oldest to most recent):

- ISA: a.k.a. AT bus. (found in older 486s and lower speed machines)
- MCA: IBM’s own, and very proprietary, flavor of bus. (Currently not in wide use). MCA cards are bus-mastering card. Bus mastering cards were a somewhat successful attempt at increasing the efficiency of communications between the card's slot on the motherboard and the processor. Basically, read ‘bus-mastering’ as ‘proprietary hardware architecture’.
- EISA (Expanded Industry Standard Architecture): High speed interface still popular but usually found only in file servers, especially Novell file servers, due to a limited selection of cards on the market made for the EISA type motherboard slot. EISA cards are also bus-mastering cards. EISA offers 32-bit throughput and auto-reconfiguration. Both EISA and VESA incorporate principles of FLEX. FLEX was originally developed by Compaq Computer Corp. in an attempt to increase the efficiency of communications between peripheral components and the processor.

## Networking Basics – Architectures

- VESA Local Bus: This short-lived technology was essentially a direct line between peripheral slot on the motherboard and the processor (very similar to Macintosh bus technology). (Macintosh developed PDS, (processor direct slot), and NuBus both of which involve a direct connection between the processor and peripheral slot).
- PCI: Currently enjoying wide acceptance as the bus of choice in the PC industry. PCI slots are found in late model 486s and all Pentium systems.

### Memory access methods

There was a time, pre-windows95, when memory management played a greater role in installing network interface cards. In fact, it was only really in versions 6 and higher of MS Dos that we started to see memory management integrated into a PC's operating system. The NIC needs to communicate to the processor through a 'piece' of memory. Typical methods of this are:

- Shared memory – uses up memory that could be put to better use and often causes conflict with other hardware trying to talk to the processor.
- Direct Memory Access – a little better than the 'shared' method, but it uses up a DMA channel that other devices might need to talk to the processor.
- Programmed I/O – you might also call this a memory-mapping card – it has its own little piece of memory to add to the computer and gives the best overall performance of the lot.

#### The Network Interface Card

The NIC will come in three general types: internal, external, and PCMCIA:

- Internal: By far and large the most common. 8-bit, 16-bit, 32-bit, 64-bit, 10 mbps, 100 mbps, etc... These cards are simply another circuit board that lives in a 'peripheral slot' on a PC's motherboard. Peripheral slots may be filled by many items including: modems, video cards, and controller cards.
- External: External interface cards were big before PCMCIA slots hit the market. They are about the size of a package of two Swiss Rolls or a PC's mouse. External cards are very nice for technicians since you can install them temporarily without opening a computer case. It also saves time diagnosing hardware problems with internal network interface cards. If the network connection works with the external card but not the internal card, it really narrows down your search for the problem.
- PCMCIA: Personal Computer Modular Component Interface Adapter? Or how about 'People Can't Memorize Computer Industry Acronyms'. Maybe we should all call them credit card adapters since the shape and size are just about the same. PCMCIA slots are externally accessible peripheral slots. Available PCMCIA devices include: NICs, modems, controllers, hard drives, security access cards, etc... The advantage is that these devices can be added (and removed) without opening the computer's case and many times without even shutting it off. However, installing *certain* PCMCIA cards involve a complex process of driver loading.