



Network+ Series Supplemental Information

Q: What are the characteristics of the following types of cables?

- 10Base5
- 10Base2
- 10Base-T
- 100Base-TX
- 100Base-T4
- 100Base-FX
- 1000Base-T

A: Refer to the table below

Common Name	Physical Layer Standard	Speed	Cable Type	Topology	Maximum Segment Length
Thick Ethernet	10Base5	10 Mbps	RG-8 coaxial	Bus	500 meters
Thin Ethernet	10Base2	10 Mbps	RG-58 coaxial	Bus	185 meters
Ethernet	10Base-T	10 Mbps	Cat 3 UTP	Star	100 meters
Fast Ethernet	100Base-TX	100 Mbps	Cat 5 UTP	Star	100 meters
Fast Ethernet	100Base-T4	100 Mbps	Cat 3 UTP	Star	100 meters
Fast Ethernet	100Base-FX	100 Mbps	62.5/125-multimode fiber optic	Star	412 meters
Gigabit Ethernet	1000Base-T	1,000 Mbps	Cat 5 UTP	Star	100 meters

* UTP – Unshielded twisted pair. Category 5 or 5e is most common type of UTP currently in use for data networks.

Q: What are ST and SC connectors used for?

A: ST and SC connectors are used to connect fiber optic cable (single-mode and multi-mode fiber).

- ST — Round with a bayonet or twist lock coupling connector.
- SC — Push/pull coupling connector similar to ST connector except the connector is square shaped.

Q: How do you choose the appropriate media type and connectors to add a client to an existing network?

A: When selecting an appropriate network medium for a LAN installation (connecting a client to a network), there are several factors you must take into consideration:

- **Segment length** – The distance between two devices has an effect on your cabling decision. In a thicknet or thinnet network (bus network), the issue is typically the distance between two PCs. In a star topology (e.g. 10baseT or 100baseT), the issue becomes the distance between each PC and the hub. The hub functions as a repeater so you'll also need to make sure hubs are positioned correctly and not chained excessively.
 - When cable distances exceed specifications the devices become so far apart electronically that they can not detect collisions properly.
- **Upgradeability** – Like momma always said, "When you fail to plan, you plan to fail", and network design is certainly no exception. When deciding a network configuration, factoring in future expansion will pay dividends in the long run. Cable installation, connectors and associated hardware (not to mention labor) comprise a major piece of an IT operating budget. By planning for future expansion, you can limit your future costs by buying equipment, cabling, etc., that will allow you to upgrade your network
 - (i.e. Installing Category 5e cable even though you are only implementing 10 Mbps Ethernet currently; you may want to upgrade to gigabit Ethernet in the future, which Cat 5 will handle the speed increase without having to install all new cabling)
- **Fault tolerance** – Understanding your risk tolerance plays a major factor in choosing the cabling and equipment for your network as well. Older style bus networks were problematic in that if a break in the cable occurred anywhere on the bus, the PC's attached to the bus were affected. Star networks, on the other hand, have increased fault tolerance. If a cable breaks to one PC, only that PC is affected. Not the entire network.
- **Security** – If your network requires a high degree of security, you may need to choose fiber optic cabling over copper. Fiber



optic is more expensive and harder to install, but can't be tapped like copper.

- **Ease of installation** – Copper cables are fairly straight forward (and forgiving) during the install process, although some types of copper cable are easier to install than others. UTP is the easiest to work with and most commonly found in star networks. Fiber optic is the hardest to install in that it requires specialized skills and tools to make the connections, polish the ends, and ensure breaks don't occur in the cable due to crimping, pinching or bending too sharply. As the installation complexity increases, so does the cost.
- **Environmental factors** – Your work environment will have an impact on your cabling decision as well. If there are electrical components that could interfere with your copper cabling (e.g. generators, fluorescent lighting, electrical wiring, etc) then you may need to go with fiber optic cable. Fiber is immune to EMI (Electromagnetic Interference) since it uses light, not electrical pulses to send data.

Each type of cabling will have an associated connector or connectors. For example, 10baseT networks use RJ45 connectors, whereas 10base2 uses BNC connectors.

Q: What is a Wireless Access Point?

A: A wireless access point is a piece of hardware that is typically used with networks implementing 802.11b (WiFi). They look much like a normal hub or switch, except they have antennas on the back or sides of the device.

In a wireless network, you can operate in one of two modes, infrastructure and ad-hoc.

- Infrastructure – in this mode, all traffic passes through the wireless access point
- Ad-hoc – devices talk directly to one another with no need for an access point

Wireless AP's provide a number of advantages, including NAT functionality and routing and bridging functions. A typical wireless AP for a DSL or cable network will allow a wired network to connect to a wireless network, and share an internet connection through one IP address (NAT – network address translation).

The Wireless AP can also provide security through WEP (wireless encryption protocol) as well as firewall functionality for the devices on the network.

Q: What is NTP?

A: Network Time Protocol is an Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. NTP synchronizes client workstation clocks to the U.S. Naval Observatory Master Clocks in Washington, DC and Colorado Springs CO. NTP can run continuously in the background of a client computer where it sends periodic time requests to keep its internal clock in synch with the atomic clock.

Q: What is RAS?

A: RAS stands for Remote Access Server, and is typically used to allow employees remote access to a corporate network. A RAS server is usually configured to allow users to either dial-in via modem or tunnel in via the internet so they can establish connectivity to their work LAN. RAS allows employees who travel frequently or work from home (telecommute) to have network access while still maintaining security (through various authentication and/or encryption methods).

Q: What is ICA?

A: ICA stands for Independent Computing Architecture, a protocol developed by Citrix. ICA is used in thin-client computing, allowing users to work on corporate systems remotely. In a thin-client environment, the user sees the application on their desktop, but all the actual processing takes place on the server.

ICA lets the server separate application logic from the user interface (UI) and send only the application's UI to the client. The application runs completely on the server. The only things transmitted over the network are keystrokes, mouse clicks, and screen updates. Applications you deploy with ICA consume as little as one-tenth of the network bandwidth they typically require; which results in an increase in performance due to the smaller of information being transmitted - about 10KB to 20KB per user

Q: Can a Macintosh computer connect to an existing network (Novell, Unix or Microsoft)?

A: Yes. Macintosh computers offer similar functionality to Microsoft-based PC's in a networked environment. They offer user authentication, file-sharing, web browsing and a wide variety of applications. Macintosh computers use Appletalk as their default protocol, but can use TCP/IP as well.



For additional functionality, a client can be installed for Microsoft or Novell networks that allows for enhanced user authentication, encryption, and browsing of the respective network.

In an all-Mac LAN, areas are divided into zones with each zone typically representing an Ethernet or Token Ring segment.

Q: What is NAS and what are its main characteristics?

A: NAS stands for Network Attached Storage and functions as the name implies. NAS devices are highly-reliable, scalable storage devices that can be attached anywhere in the network. They allow you to add storage by adding or increasing hard drives in a NAS device, or clustering devices together. Most units are fault-tolerant via RAID and redundant critical components (power supplies, fans, etc). NAS devices typically allow for hot-swapping of drives and allow you to increase storage, repair failed drives, etc., without taking down your main servers (domain controllers, e-mail servers, etc).

Most NAS devices are protocol independent and run on a variety of platforms (e.g. Microsoft, Unix/Linux, Novell, etc). NAS devices also range in price and functionality from small business/departmental level solutions to full enterprise class devices offering up to 50 TB or more of data connected via high-speed fiber-channel backbones.

Q: How can the following utilities be used in a troubleshooting situation?

A: Refer to following list:

▪ **ARP**

- Address Resolution Protocol – ARP resolves IP addresses to MAC addresses and is integral to the communication process. For two devices to communicate on an IP network, IP addresses must be resolved to their MAC address (hosts communicate via MAC address). ARP is the protocol that broadcasts for the recipient's physical (MAC) address. The host owning the IP address in question responds back with its physical address. Once a host obtains the destination host's MAC address, it will cache this information for a period of time so subsequent communication doesn't require the ARP broadcast. If the destination host is not on the local network, the source host will ARP for the MAC address of the default gateway and send the information there.
 - You can view the arp cache by typing "arp -a" from a command prompt. Communication errors would occur if the MAC address in cache is incorrect for a given IP address. This typically occurs when a duplicate IP address exists on a network, or an IP has been given to a different machine.
 - ARP can also be used to see who is communicating with your machine locally (all remote communication will only show the MAC address of the default gateway).

▪ **Ipconfig/Ifconfig**

- Ipconfig is TCP/IP utility used in MS Windows environments (NT, Windows 2000 and XP) that provides you with information about the interfaces on your machine. It will provide you with the IP address, subnet mask and default gateway for each interface. If you type ipconfig /all you'll see more detailed information, including DNS information, DHCP server address (if applicable) and node type.
 - From a troubleshooting perspective, ipconfig allows you to determine if TCP/IP is configured properly on your machine, as well as releasing and renewing a DHCP lease, by typing ipconfig /release or ipconfig /renew, respectively.
- Ifconfig command is similar to the ipconfig command found in the Windows world but it is used in Unix and Linux environments to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.
- If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only.

▪ **Winipcfg**

- For Windows 95/98/ME operating systems, using the **winipcfg** utility will provide the same type of information but in a graphical pop-up window. You can access winipcfg from a command prompt and typing "winipcfg". You can choose which interface to obtain information about by choosing it in the drop down window that appears in the pop-up.

Q: How do I configure a client to connect to a Macintosh server?

A: That depends on the operating system we're talking about.

If client computers are Macintosh, we have several options.

- Mac OS X Server allows what is called a "netboot" with Mac clients running OS 9.x or higher, booting them into a thin-client environment. All processing takes place on the server with the clients essentially seeing the GUI and passing



mouse clicks and keystrokes back to the server.

- To log into a Macintosh network with Macintosh clients, no configuration is necessary in this case since the Mac client is built into the OS
 - It may be necessary to update the Appleshare client from time to time as new versions become available.

If the clients are Windows-based PC, then we need to install the Appleshare client on the PC. Older versions utilized Apple's proprietary AppleTalk protocol, while newer versions of the client can utilize TCP/IP or AppleTalk to maintain backwards compatibility.

Q: What are some visual indicators that you can use to troubleshoot network problems?

A: Any time we troubleshoot, it's important to start simple. The little things are often overlooked and can cause us the most frustration. When dealing with loss of network connectivity, make sure to check the cables and connections to ensure power is getting to all devices and that all devices are connected to the network.

Also utilize the link lights and activity lights that are found on NIC cards, hubs, switches, etc. They can tell us a great deal of information at a glance, for example:

- 5 machines plugged into a hub, link lights are on for all except one connection. Immediately we know there is something wrong with the connection. The RJ45 may not be plugged all the way into the hub or NIC, the cable could be bad, the PC could be down, or perhaps the NIC itself has gone bad or come unseated in its slot on the motherboard.
 - Obviously this will take a little more investigation to narrow the problem down, but we know instantly from the link lights on the hub that the hub is working ok because the other connections are up and active.
- Network communication has slowed tremendously
 - Looking at our hub, we see that even though no machines are being used currently, there is a tremendous amount of activity on the network (as evidenced by the activity lights on the hub), and excessive collisions (again visible via collision detection lights on the hub).
 - Further investigation will be needed, but at first glance it seems we might have a defective NIC that is generating excessive traffic or broadcast storms (since no machines are actually being used, but excessive traffic is taking place).

Both scenarios require further investigation to determine the nature of the problem, but systematically approaching the problem and narrowing things down until the problem is solved is the most efficient method. Utilizing visual indicators like link or activity lights on a hub, switch or even modem can help to direct us to the nature of the problem.