



Ahmadu Bello University – Zaria
Directorate of Information & Communications Technology

STANDARDS FOR NETWORK CABLING & INSTALLATION

Version 2.0 [2nd September 2007]

1.0 INTRODUCTION

The ICT Directorate of Ahmadu Bello University operates a computer network to support the university in its mission. Bandwidth on this network is a limited resource and is susceptible to misuse, abuse and attack. It must therefore be effectively managed. One way of ensuring this effective use is that network devices and infrastructure in departments, units and faculties be set up and operated according to well laid down standards. This document will serve as that reference for standards.

Adherence to these standards is for the common good and the Network Infrastructure & Security unit of the ICT Directorate shall disconnect or block access of any defaulting computer or network.

This policy applies to all faculty, staff, students and contractors who connect a Network device to the campus network either through wire or wireless. Whenever anyone is connected to the campus network, he or she is expected to comply with this Policy.

This document defines standards for the installation of voice and data networks in all departments or units of the university. It will be revised periodically and so every department/unit that wants to install and network must contact the ICT – Directorate for the latest version of this document. For technical inquiries relating to these standards contact one of the following Network Infrastructure & Security unit staff members.

Adedokun Adewale

wale@abu.edu.ng

Mukom A. Tamon

mukom.tamon@abu.edu.ng

2.0 LOGICAL NETWORK DESIGN

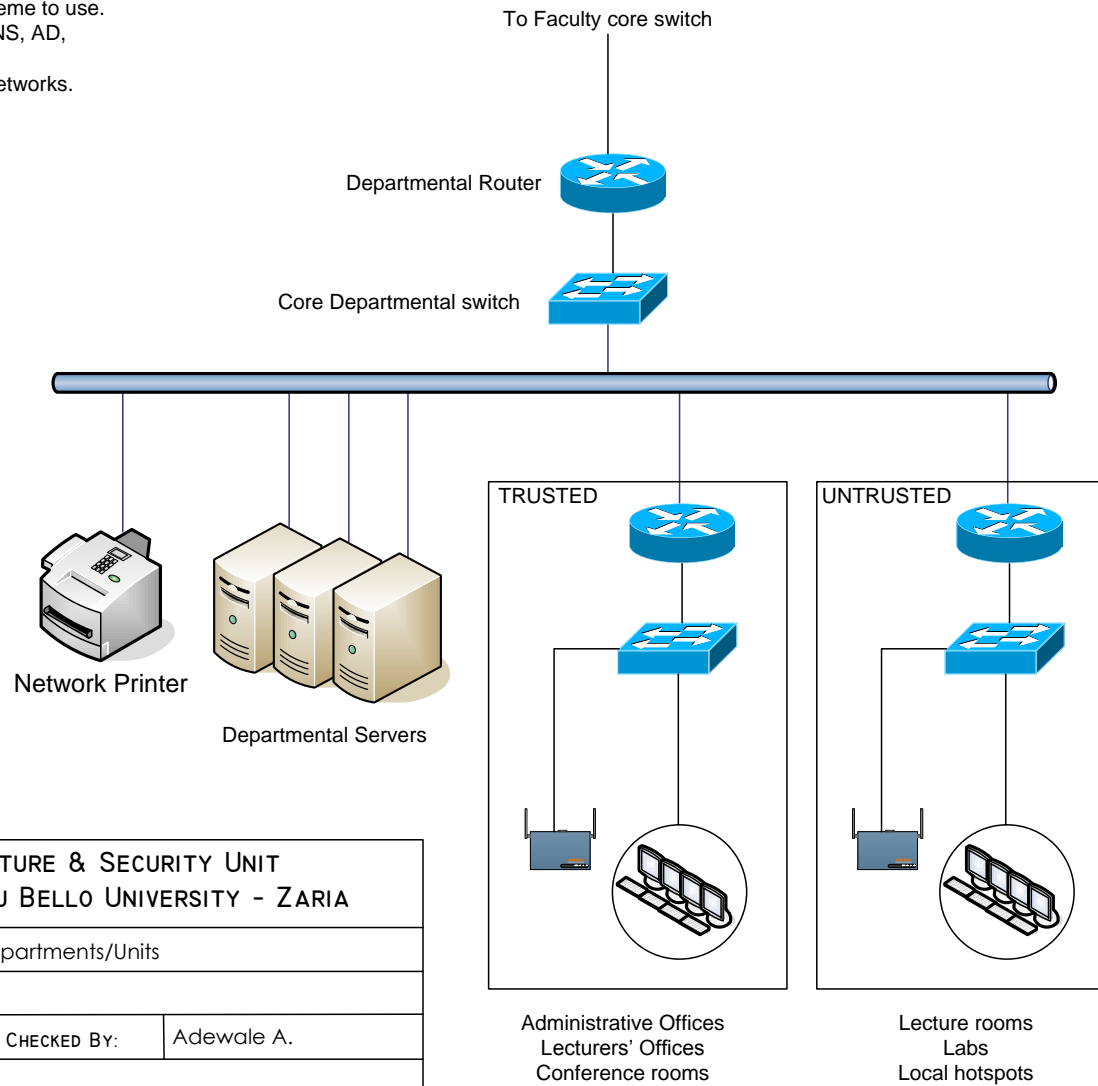
The diagram on the next page shows how every departmental network should be structured. Although implementation details may vary and all components may not be implemented at the same time – this design should generally be adhered to for purposes of efficient traffic engineering and security.

The following aspects from the diagram are to be noted:

1. Departmental servers could provide services like DHCP, File and print sharing, Directory services e.g. Active Directory etc. These will serve the department temporarily until at which time those services shall be provided at either the faculty or campus level.
2. Servers related to exam records should be placed in the trusted network and protected by host-based access lists.
3. The access points in the different networks (trusted and un-trusted) must have different SSIDs. Although shown here as two separate APs, these separate wireless LANs can be implemented in virtual APs.
4. Policies should be implemented to prevent any communications between the trusted and un-trusted network. Devices in the un-trusted network should only be able to access the Internet and selected services on the departmental servers.
5. The contractor shall contact Network Infrastructure & Security unit for the IP subnet to use in each department.
6. The faculty office shall be considered as a department and have its own separate network according to the same design.

NOTES

1. Contact Networks for IP addressing scheme to use.
2. Departmental servers will run DHCP, DNS, AD, Exams, File etc
3. Router configuration shall be done by Networks.



NETWORK INFRASTRUCTURE & SECURITY UNIT ICT DIRECTORATE AHMADU BELLO UNIVERSITY - ZARIA			
DRAWING TITLE:	Logical Design for all Departments/Units		
PAGE:	1 of 1		
DRAWN BY:	M.A. TAMON	CHECKED BY:	Adewale A.
DATE	Friday August 24 th 2007		

Fig 1.0: Prototype logical network diagram for all departments.

3.0 HORIZONTAL CABLING

3.1 GENERAL

All cable and cabling products (copper and fibre) that form part of a voice/data cable installation shall be specified and installed only with the approval of Network Infrastructure & Security unit. In multi storey installations, cables shall not be installed between floors except through an approved communications cabling riser or duct. All fire-rating materials removed for the installation of cables shall be replaced such that the original fire rating is preserved. All installed cables on University property shall be terminated at each end, properly labelled and documented. This applies to all permanently installed cable types.

3.2 NETWORK EQUIPMENT

The installation, removal or configuration of non-departmental LAN infrastructure equipment shall be carried out by Network Infrastructure & Security unit staff only. The connection of faculty or departmental switches to the core University network shall only be carried out by Network Infrastructure & Security unit staff. Departments/faculties purchasing network equipment for their own use shall ensure that the following requirements are met:

- ◆ A minimum of 100Mbps switched connectivity to the desktop.
- ◆ All servers must be connected at a minimum of switched 1Gbps.
- ◆ The departmental switch must support VLANs for user segmentation.

3.3 NETWORK CONFIGURATION CONSTRAINTS

Each basic link shall comprise of a four pair Category 5e cable and RJ45 connectors with following specifications.

- ◆ Maximum link length -90 metres
- ◆ Maximum channel length -100 metres
- ◆ Maximum number of stations per segment -1.

All new cabling installations shall meet the TIA/EIA-568B. The cabling system shall include all patch panels, horizontal cables, vertical cabling, modular jacks,

system cables, patch cables, drop-leads, cable management, and a comprehensive labelling system. The cable interconnecting a network outlet and a horizontal distribution panel/transition point or patch panel shall be of one continuous length with no inter-mediate joins, splices or taps.

Where horizontal cabling is part of an integrated voice and data installation, both voice and data cables shall be terminated on common patch panels. Additions/repairs to existing Cat 5 cabling shall be made using Cat 5e standard components and cable.

3.4 NUMBER OF OUTLETS PER WORKSPACE

A workspace is here defined as the space/seating that is occupied by a single individual in an office. The following information represents a minimum requirement for the number of UTP outlets that shall be installed in each type of workspace.

1. General staff, lecturers and graduate assistants' workspace: Two outlets (in a single dual-point RJ45 faceplate) shall be cabled to each workspace.
2. Departmental Student Computer Lab: Departmental computer labs shall have a minimum of one outlet allocated per seating space.
3. Lecture Theatre/Teaching Space: A minimum of three UTP outlets shall be provided to each standard lectern. A minimum of two outlets shall be provided for a "mini lectern". If a student seat in a teaching space is to be provided with a network outlet, one UTP outlet shall be installed per seat. Tutorial/Seminar rooms shall be provided with two outlets.
4. Information Kiosks: A minimum of one outlet shall be run to an information kiosk.

3.5 NETWORK OUTLET & LABELLING

The outlet shall be fitted with a clear and permanent label that depicts the unique outlet identifier. The identifier shall contain the following elements:

A switch or patch panel identifier prefixed with the letter S or P respectively. A switch port or patch panel jack identifier (1 – maximum number of patch panels)

For example an outlet having a label – 'S2-12' will be cabled back to the 12th port on the second switch that serves this floor. Similarly 'P2-7' will be cabled back to the 7th jack on the second patch panel. In the wiring close, the other ends of the links must be labelled to show where they terminate. This labelling shall use the floor (prefixed by F), room number (as is known in the department/unit) and a fixed number starting from 1 to the number of points in the room. The wall jacks must have these numbers written on them in indelible ink. For example F2-B9-2 means that this link goes to the second wall jack in the room known in this department as B9 which is on the second floor. On the schematic, each outlet's position shall be clearly indicated so that the room and position within the room can be identified.

3.6 CABLE INSTALLATION

Cable termination onto a horizontal distribution panel or patch panel shall be undertaken in a manner that permits additional cables to be terminated without unduly disturbing previously installed cables. One horizontal cable management (patch lead minder) panel shall be used for each patch panel. The horizontal cable management panel/s shall be dimensioned to accommodate a number of patch leads equal to the number of ports on the switch or patch panel. All field cables shall be led through the rear cable management duct prior to termination on the patch panel jack. No more than 24 cables shall be cable tied in a bunch.

A 2-metre loop of cable shall be left within or on the approach to each communications room/enclosure to facilitate future re-termination of the cable. Such cable slack shall be coiled and supported in a neat and practical manner. A 0.5-metre loop of cable shall be left in the trunking/ducting on the approach to each network outlet to facilitate future re-termination of the cable, should this be required.

Precautions shall be observed to eliminate cable stress caused by tension in suspended cable runs and tightly strapped bundles. Cable bundles shall not obstruct the installation and removal of equipment in equipment racks. As much as possible, running network cabling parallel to power cabling must be avoided or else a minimum separation of half a metre (50cm) is to be observed. Where UTP

cables are run in the proximity of electrical motors or transformers the minimum separation shall be 1 metre. In situations where the above minimum distances cannot be applied due to a lack of available space, data cables shall be enclosed in rigid and/or flexible PVC conduit.

3.7 PATCH PANEL & OUTLET SPECIFICATION

All patch and drop cables shall be certified to the category of cabling being installed. Handmade patch and drop cables shall not be permitted. Patch and drop cables from one category shall not be used in an installation cabled to a differing category. Two Velcro cable ties suitable for securing 24 UTP cables shall be supplied for each patch panel installed. The maximum length of a patch or drop-lead shall be 5 metres. - lead lengths greater than 5 metres shall be specifically approved by Network Infrastructure & Security unit.

Patch leads shall be colour coded according to the following convention:

Patch Cable Type	Colour
Straight through data cable	Blue
Crossover data cable	Green
Core network (campus backbone)	Purple
Voice outlet	Yellow
Power over Ethernet	Red

4.0 TESTING

Prior to handing over the job, all devices and systems installed must be tested by Network Infrastructure & Security unit to ensure that they meet the acceptable performance standards.

Cabling shall be tested using a high specification cable LAN tester. Testing shall be carried out with building electrical services operating (lighting, power, air-conditioning plant and lift services where applicable). Where this is not practical, cable testing shall be carried out on all installed cables within the project time frame. At the discretion of Networks, further testing shall then be carried out on not less than 10% of the total installed cable plant with all electrical services operating. This test shall be carried out within one month of the project schedule test. The cables selected for live condition testing shall be selected from all patch panels installed.

If this delayed testing is required, the cabling installation shall be deemed incomplete, and payment withheld pending the outcome of the delayed tests. Networks reserve the right to observe the test procedure at any time and to perform its own tests on the cable and other installation.

5.0 DOCUMENTATION

The contractor shall provide installation documentation at the completion of the structured cabling system or other network installation. This documentation shall be in both hard and soft copies (on CDs) and will be verified by Network Infrastructure & Security unit prior to accepting the job as completed. These documents must be provided to the unit at least one week prior the commissioning date for the project. Sample templates for network documentation are provided in the appendix and should guide the contractor in providing documentation. The documentation shall include the following:

- a. A logical diagram of the installed network showing all devices, their OSI layer 2 & 3 connectivity as well as any services running. Any security boundaries must also be shown.
- b. A building schematic in plan view (in AutoCAD .dwg format) illustrating devices, network outlets and their location within the building.
- c. All major cable routes with intermediary devices.
- d. RF coverage map showing for different wireless solutions installed.

Documentation shall be presented three sets, one each to the relevant Department Head, the Estate Department and the Network Infrastructure & Security unit of the ICT Directorate. Where networking equipment has been installed, their full configuration plus administrative passwords must also be provided prior to commissioning of the project.

All contractors are advised to contact Network Infrastructure & Security unit before and during contract execution so as to be abreast of any additional requirements and modifications.

6.0 WIRELESS LANs

Every departmental LAN must be a hybrid wired/wireless network. The WLAN shall be deployed to extend the LAN to mobile devices like laptops, palmtops and smart phones. As illustrated in Fig 1.0, just as for the wired LAN, there shall be two wireless LANs, a trusted one and a non-trusted WLAN. The former offers network connectivity exclusively within administrative offices, lecturers' offices and official meeting rooms. The non-trusted WLAN is that which offers coverage in classrooms, labs, libraries, general conference and tea rooms as well as outside the building.

All WLAN installations and/or connections shall be made according to the following conditions and standards.

6.1 OPERATING CHANNEL

The portions of the wireless spectrum designated for Wireless Network Infrastructure & Security unit are considered a University wide resource. All devices that use the spectrum shall be approved by Network Infrastructure & Security unit. Network Infrastructure & Security unit may require devices that cause interference to be switched off or reconfigured at its discretion. A proper RF site survey must be done to ascertain what frequencies are already being used so as not to cause interference to existing wireless LANs.

If necessary that channels be reallocated, the administrators of existing WLANs and networks shall be informed and will together agree on acceptable channel usage. Prior to any wireless installations especially around the faculty of medicine, veterinary medicine and teaching hospitals, an extensive equipment audit must be done to determine that there are no devices whose operation will be interfered with by the proposed WLAN.

All co-located access points must not cross-interfere with each other – this thus constraints all 2.4GHz APs to run any of channels 1, 6 and 11. 5GHz channels are all non-overlapping and so may used indiscriminately.

6.2 STANDARDS

All local area wireless access points or routers intended for WLAN extension shall conform to the 802.11g, 802.11n and optionally 802.11a standards. IEEE 802.11b-only access points and routers shall not be may be used. Use of base stations conforming to other standards shall be subject to approval by Network Infrastructure & Security unit.

6.3 ACCESS, SECURITY AND AUTHENTICATION

The trusted WLAN must future strong encryption based on WPA2 or IEEE 802.11i standard. Authentication must also be done to against the directory service in use – most like Active Directory using Extensible Authentication Protocol. Un-trusted WLANs shall be open access and authenticate via the Universal Access Method either to a local server or the university's hotspot.

6.4 BASE ASSOCIATION RATES & ROAMING

For all WLANs designed to extend wired LANs, the following apply:

- ◆ The base association rate for each 802.11g or 802.11a client is 36Mbps.
- ◆ The base association rate for 802.11b clients is 5.5 Mbps.

Within each administrative domain (department, institute, unit or faculty) the wireless LAN must be designed such that users can roam about without losing their connection.

7.0 CONDITIONS OF CONTRACT

All contractors who carry out horizontal cabling and network related work in any department, faculty or unit of the university shall adhere strictly to all the conditions and requirements laid down in this document. The following are to be noted.

1. Adherence to the Standards for Network Installation by cabling installation contractors is a condition of contract.
2. The Network Infrastructure & Security unit section of the ICT Directorate (hereafter referred to in this document as 'Network Infrastructure & Security unit') provides a network specification and design service. Contracts for structured cabling systems and/or other minor works shall be let and managed at the request of the relevant department or faculty.
3. **Approved LAN Designs:** All building LAN cabling designs shall be approved by the Network Infrastructure & Security unit. A copy of the proposal, tender specification, schematic and/or floor plan shall be submitted to the Network Infrastructure & Security unit for approval prior to the issuing of documents for tender or award of the contract. Any cabling installation that does not comply with the 'Standards for Network Installation' shall not be connected to the University network infrastructure.
4. **Workmanship:** All cabling installations, both external and internal, shall be made using the highest practical standard of workmanship and consideration for aesthetics. Such installations shall be commensurate with the enduring and world-class nature of the University. Any cabling installation that does not comply with the 'Standards for Network Installation' shall not be connected to the University network infrastructure.
5. **Aesthetics:** All cabling installations in General Access Areas (Theatres, Common Learning Spaces, Classrooms, Tutorial Rooms, offices, corridors/foyers and toilets) shall be concealed within wall and/or ceiling cavities wherever possible. In cases where such concealment is not possible, surface mounted duct/trunk fitted with a removable lid shall be supplied. Samples of the proposed duct

shall be submitted to the Project Coordinator for final approval prior to commencement of work on site.

6. **Documentation:** The contractor shall provide installation documentation at the completion of the any networking related work. Both hard and soft copies (on CDs) must be provided to Network Infrastructure & Security unit a minimum of one week prior to the commissioning date.

8.0 MINIMUM SECURITY STANDARDS FOR NETWORKING DEVICES

These minimum standards are intended to ensure the security of all devices connected to the campus network. Any device to be connected to the campus network must satisfy the following minimum standards.

8.1 SOFTWARE PATCH UPDATES

Devices to be connected to the campus network must run software for which critical security patches are made available in a timely fashion and must have all currently available security patches installed. For Windows-based computers, Automatic Updates must be turned on.

8.2 ANTI-VIRUS SOFTWARE

Anti-virus software for any particular type of operating system must be running and up-to-date on every device, including clients, file servers and mail servers. These antivirus software must also be configured to as follows:

- a. Automatically update their virus definition files at least once a day.
- b. Perform full systems scans at least once a week.

8.3 HOST-BASED FIREWALL SOFTWARE

This is software on a device that helps protect the device by controlling what network traffic is allowed to enter and leave the device. An example of this is the Windows Firewall that runs on Windows XP Service Pack 2.

System Administrators are responsible for ensuring that computers with native host-based firewall software included in the operating system have the firewall activated and properly configured.

8.4 PASSWORDS

Campus electronic communications systems or services that require users to be identified must identify and authorize users using secure authentication processes (e.g., digital certificates, biometrics, Smart Cards, one-time passwords or en-

encrypted password transactions). When reusable passwords are employed, they must meet the minimum password complexity standards below. In addition, shared-access systems must be configured to enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible devices must be modified. Passwords that may be used by System Administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

All passwords employed to authorize access to campus electronic communications systems or services must meet the following minimum password complexity standards. The password must:

- ◆ Contain six characters or more.
- ◆ Contain characters from at least two of the following three character classes:
 - ◆ Alphabetic (e.g.: a-z, A-Z)
 - ◆ Numeric (i.e. 0-9)
 - ◆ Punctuation and other characters (e.g.: !@#\$%^&*()_+|~-=\`{}[]:;';<>?.,/)

8.5 UNENCRYPTED AUTHENTICATION

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the campus network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. To prevent password harvesting, passwords must not be sent in the clear and all campus devices must use encrypted authentication mechanisms or otherwise secure authentication mechanisms. Passwords or protocols which provide no log on access to the system (e.g., anonymous FTP) are exempted from this requirement.

8.6 UNAUTHENTICATED EMAIL RELAYS

Campus devices must not provide an active SMTP (an Internet protocol for sending email between devices) service that allows unauthorized parties to relay email messages. Before transmitting email to a non-local address, the sender must authenticate with the SMTP service. Unless an unauthenticated relay service has been reviewed by Network Infrastructure & Security unit as to configuration and appropriate use, it may not operate on the campus network.

8.7 UNAUTHENTICATED PROXY SERVICES

Although properly configured unauthenticated proxy servers may be used for valid purposes, such services commonly exist only as a result of inappropriate device configuration.

Unauthenticated proxy servers may enable an attacker to execute malicious programs on the server in the context of an anonymous user account. Therefore, unless an unauthenticated proxy server has been reviewed by Network Infrastructure & Security unit as to configuration and appropriate use, it is not allowed on the campus network.

In particular, software program default settings in which proxy servers are automatically enabled must be identified by the System Administrator and re-configured to prevent unauthenticated proxy services.

8.8 PHYSICAL SECURITY

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to “lock” and require a user to re-authenticate if left unattended for more than 20 minutes.

System Administrators are responsible for maintaining the physical security of devices in their care.

8.9 UNNECESSARY SERVICES

If a service is not necessary for the intended purpose or operation of the device, that service shall not be running.

9.0 APPENDICES

9.1 EXISTING LANs

All departmental LANs already in existence that do not meet these standards are given up to 6 months from the date of publication of this document to upgrade their networks to standard or risk being cut off from the university's services.

9.2 DOCUMENTATION TEMPLATES

The following templates shall be used in aiding the contractors provide the documentation that is required by Network Infrastructure & Security unit for effective management.

Current Configuration

Please attach a copy of this router's configuration (show running-config)

Other Useful Information

Please specify any other useful information not already captured above.

DOCUMENTATION TEMPLATE FOR SERVERS

Device ID		
Device Name		
Model/Make		
Manufacturer		
Serial Number		
Location		
Purpose of this device		
Person Responsible		
Operating System	<input type="checkbox"/> Windows Server <input type="checkbox"/> Linux <input type="checkbox"/> Unix <input type="checkbox"/> Other (Specify) [_____]	
	Version/Type: Service Pack:	
Services being offered	<input type="checkbox"/> DHCP <input type="checkbox"/> Directory Services <input type="checkbox"/> Web Server <input type="checkbox"/> NAT <input type="checkbox"/> Other (Specify) [_____]	
Interface Description		
Interface 1	Type:	<input type="checkbox"/> FastEthernet <input type="checkbox"/> Gigabit Ethernet <input type="checkbox"/> Other (Specify) [_____]
	MAC Address	
	IP Address	
	Subnet Mask	
Interface 2	Type:	<input type="checkbox"/> FastEthernet <input type="checkbox"/> Gigabit Ethernet <input type="checkbox"/> Other (Specify) [_____]
	MAC Address	
	IP Address	
	Subnet Mask	
Interface 3	Type:	<input type="checkbox"/> FastEthernet <input type="checkbox"/> Gigabit Ethernet <input type="checkbox"/> Other (Specify) [_____]
	MAC Address	
	IP Address	
	Subnet Mask	

Procedure Information

Please describe the procedure for accessing and configuring this device. Provide sample screenshots

Other Useful Information

Please specify any other useful information not already captured above.

DOCUMENTATION TEMPLATE FOR SWITCHES

Device ID	
Device Name	
Model/Make	
Manufacturer	
Serial Number	
Location	
Purpose of this device	
Person Responsible	
Operating System	<input type="checkbox"/> Cisco IOS <input type="checkbox"/> CatOS <input type="checkbox"/> Other (Specify) [_____]
	Version/Type:
Manageability	<input type="checkbox"/> Command Line Interface <input type="checkbox"/> Web Interface <input type="checkbox"/> Other (Specify) [_____]
	Management IP Address & Mask: Management VLAN
Interfaces Description & Count	
Interface 1	Type: <input type="checkbox"/> Fast Ethernet <input type="checkbox"/> Gigabit Ethernet <input type="checkbox"/> Other (Specify) [_____]
	MAC Address
	Count
Interface 2	Type: <input type="checkbox"/> Fast Ethernet <input type="checkbox"/> Gigabit Ethernet <input type="checkbox"/> Other (Specify) [_____]
	MAC Address
	Count
VLANS in Use & Description	
<i>If VLANs are being used on this switch, please list out the vlan numbers here and their descriptions.</i>	

Current Configuration

Please attach a copy of this router's configuration (show running-config)

Other Useful Information

Please specify any other useful information not already captured above.

DOCUMENTATION TEMPLATE FOR WIRELESS DEVICES

Device ID			
Device Name			
Model		Manufacturer	
Serial Number			
Location			
Purpose of this device			
Person Responsible			
Operating System	<input type="checkbox"/> Linux-based <input type="checkbox"/> Proprietary(Specify) [_____]		
	Version/Type:		
Manageability	<input type="checkbox"/> Command Line Interface <input type="checkbox"/> Web Interface <input type="checkbox"/> Other (Specify) [_____]		
	Management IP Address & Mask: Management VLAN		
Operating Mode	<input type="checkbox"/> Access Point		<input type="checkbox"/> Bridge
	<input type="checkbox"/> Access Point Bridge		<input type="checkbox"/> Router
Interface Description			
Uplink Interface	Type:	<input type="checkbox"/> Fast Ethernet <input type="checkbox"/> Gigabit Ethernet <input type="checkbox"/> Other (Specify) [_____]	
	MAC Address		
	IP Address		
	Subnet Mask		
	Far end of link		
Wireless Interface 1	Wireless Protocol	<input type="checkbox"/> IEEE 802.11b <input type="checkbox"/> IEEE 802.11a	<input type="checkbox"/> IEEE 802.11g <input type="checkbox"/> IEEE 802.11n
	MAC Address		
	IP Address		
	Subnet Mask		
	RF Channel		SSID
	Antenna type		
	Connection	<input type="checkbox"/> Point-to-Point	<input type="checkbox"/> Point-to-Multipoint
	Far end of link		
Wireless Interface 2	Wireless Protocol	<input type="checkbox"/> IEEE 802.11b <input type="checkbox"/> IEEE 802.11a	<input type="checkbox"/> IEEE 802.11g <input type="checkbox"/> IEEE 802.11n
	MAC Address		
	IP Address		
	Subnet Mask		
	RF Channel		SSID
	Antenna type		
	Connection	<input type="checkbox"/> Point-to-Point	<input type="checkbox"/> Point-to-Multipoint
	Far end of link		

Wireless Interface 3	Wireless Protocol	<input type="checkbox"/> IEEE 802.11b	<input type="checkbox"/> IEEE 802.11g
		<input type="checkbox"/> IEEE 802.11a	<input type="checkbox"/> IEEE 802.11n
	MAC Address		
	IP Address		
	Subnet Mask		
	RF Channel		SSID
	Antenna type		
	Connection	<input type="checkbox"/> Point-to-Point	<input type="checkbox"/> Point-to-Multipoint
Far end of link			
Current Configuration			
<i>Please attach a copy of this router's configuration (show running-config)</i>			

Other Useful Information

Please specify any other useful information not already captured above.