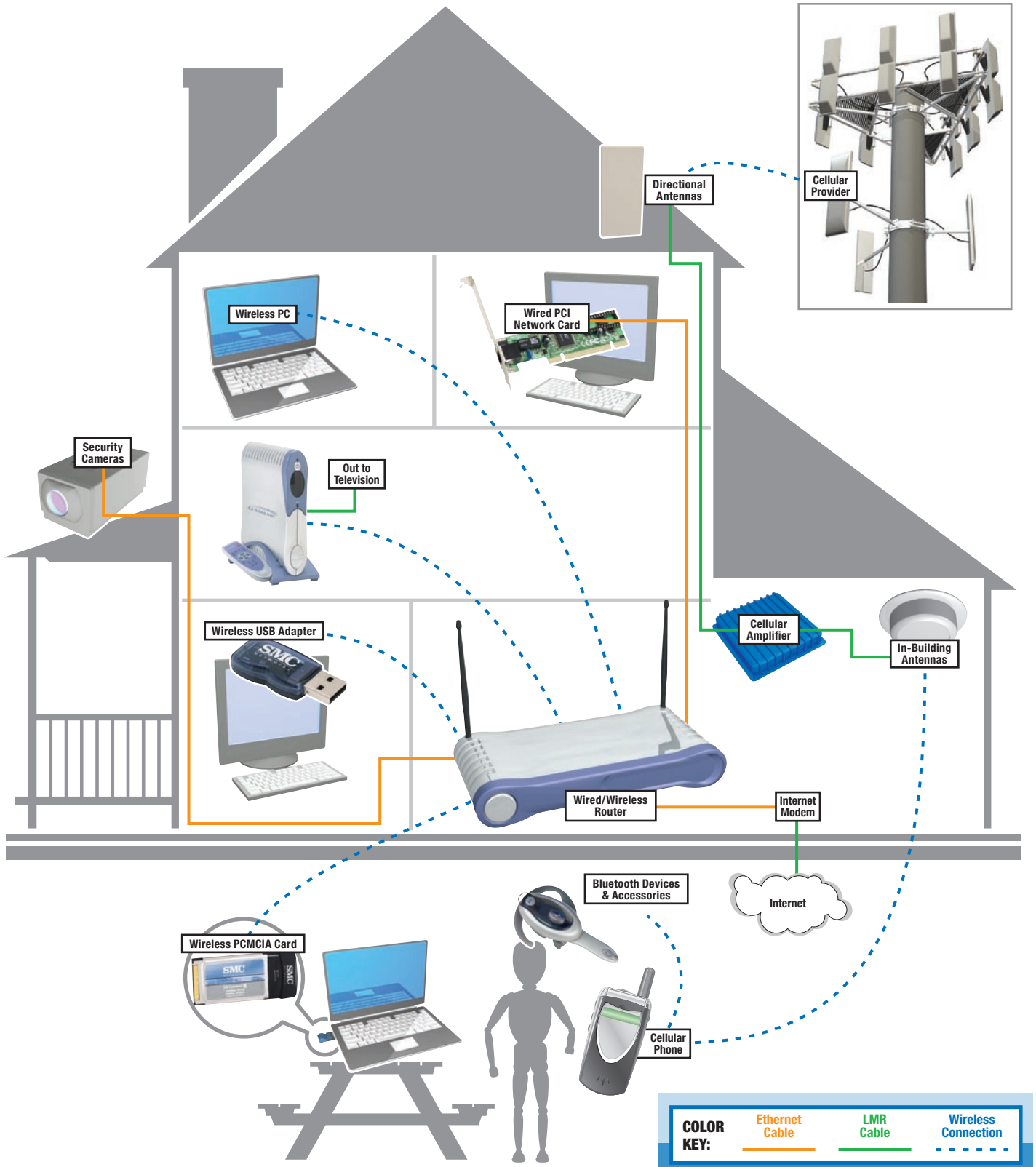
TESSCO

Solution: In-Building Networks

Application: SOHO Networking



TESSCO

Solution: In-Building Networks

Application: SOHO Networking

SUMMARY

As an increasing number of organizations push for a decentralized workforce, more and more people are working in remote small offices or home offices (SOHO). It is crucial that users have the same capabilities as on-site employees. This means providing them specially designed voice, data, and video communications solutions to allow them to connect computers, phones and peripherals to the corporate network.

FEATURES

- Data rates up to 54 Mbps
- Integrated and/or external antennas
- Unlicensed spectrum of 2.4 GHz and 5.8 GHz
- Power over Ethernet
- VoIP
- Video conferencing
- Indoor and outdoor use
- 802.11 a/b/g/n – standard access points
- 802.11n routers

BENEFITS

- Quick deployment time
- Portability
- Secure connectivity
- Ease-of-integration for guests onto the wireless network
- Scalability
- Compatibility with most wireless systems
- Compatibility with popular MP3 music services

REAL WORLD EXAMPLES

Situation: A company set up a branch office with 6 people onsite, 5 of whom will be telecommuting every other week.

Problem: The company needed an affordable way to provide its employees access to corporate servers from home or the branch office, while protecting confidential information such as student contact information and grade.

Solution: The company created a secure wireless network by installing wireless routers, switches, and Wi-Fi antennas and they supplied employees with wireless PCMCIA and PCI cards.

Situation: A mid-size college needed to set up a wireless network around campus in classrooms, sitting areas and the cafeteria to allow students and faculty to have network access on their laptops. Network access needed to be controlled so that data is secure and only authorized students and faculty have access.

Problem: The college had a limited budget.

Solution: The college was able to create a secure wireless network by installing wireless routers, switches, access points, and Wi-Fi antennas.

Situation: A hospital wanted to set up a wireless network to allow remote laptops and administrative equipment to access servers. Hospitals have numerous visitors on a daily basis, so they needed to have the network secure to prevent unauthorized users. They also wanted to install uninterrupted power supplies so that they would have access in the event of a power outage.

Problem: Security is vital in the medical field. HIPPA regulations require medical records to be kept confidential. Hospitals are a 24x7 operation so they need to keep systems running at all times.

Solution: The hospital was able to create a secure wireless network by installing wireless routers, switches, access points, Wi-Fi antennas, wireless PCMCIA cards, and PCI cards. They also installed uninterrupted power supplies (UPS) to ensure that systems would be running in the event of an outage.

ADDITIONAL CONSIDERATIONS

- How important is security?
- What are the bandwidth requirements?
- Are there any constraints for the location of products?
- Are there any environmental characteristics that could affect performance of the system?
- What is the estimated number of users?
- What type of traffic will use the connections?
- What is the size of the coverage area?
- Is there a current network diagram?

PRODUCTS

- Access points
- Enclosures
- Premise cable or wire
- Connectors
- Patch cords
- Antennas
- Wi-Fi and/or VoIP handsets
- Power solutions
- Test equipment
- Tools
- Network routers and switches